T2184096

COUR DE CASSATION

RAPPORT DE MR PETIPREZ, CONSEILLER

Arrêt n° 772 du 12 juillet 2022 – Chambre criminelle

Pourvoi n° 21-84.096

Décision attaquée : Cour d'appel de Lyon du 20 mai 2021

M. [R] [K]
M. [S] [M]
C /

Rappel des faits et de la procédure

En septembre 2019, une enquête préliminaire a été ouverte à la suite de la réception par la brigade des stupéfiants de la sûreté départementale de [Localité 1] d'une carte de visite " Uber green ", assurant la promotion d'un service de livraison d'herbe de cannabis aux consommateurs de l'agglomération [Localité], sur appel à un numéro de téléphone indiqué sur cette carte.

Les vérifications entreprises par les enquêteurs à partir de ce numéro de téléphone ont permis de constater qu'un grand nombre de personnes faisait appel à ce réseau, organisé en plate-forme téléphonique répercutant les commandes à des équipes chargées des ventes.

Des vérifications ultérieures en matière de téléphonie ont permis d'identifier une nouvelle ligne " Uber green ", active depuis le 29 septembre 2019.

Les investigations se sont poursuivies dans le cadre d'une information judiciaire ouverte le 14 novembre 2019 au tribunal judiciaire de Lyon.

Les surveillances physiques et interceptions téléphoniques ont abouti notamment à l'identification de [S] [M], considéré comme l'un des principaux coursiers et de [R] [K] cité comme étant le responsable de l'approvisionnement des livreurs.

Dans le cadre de l'information, MM. [R] [K] et [S] [M] ont été mis en examen des chefs d'infractions à la législation sur les stupéfiants, association de malfaiteurs et, pour le premier, blanchiment.

Par requête en date du 14 décembre 2020, MM. [K] et [M] ont sollicité l'annulation de l'ensemble des réquisitions délivrées aux opérateurs téléphoniques, notamment celles visant les lignes dont ils étaient titulaires ou celles avec lesquelles ils avaient été en contact, ainsi que des actes subséquents.

Cette requête a été rejetée par arrêt de la chambre de l'instruction en date du vingt mai 2021.

C'est l'arrêt attaqué.
Il convient de remarquer, à titre liminaire, que pour déclarer recevable la requête en nullité présentée par M. [S] [M], après l'expiration du délai de forclusion édicté par l'article 173-1 du code de procédure pénale, la chambre de l'instruction s'est fondée sur les dispositions de l'article 4 de l'ordonnance n° 2020-303 du 25 mars 2020.

La chambre criminelle juge cependant que le délai de six mois imparti par l'article 173-1 du code de procédure pénale à la personne mise en examen pour faire état des moyens pris de la nullité des actes accomplis avant son interrogatoire de première comparution ou de cet interrogatoire lui-même, à compter de la notification de sa mise en examen, ne s'interprète pas comme un délai de recours et n'entre pas dans les prévisions de l'article 4 de l'ordonnance n° 2020-303 du 25 mars 2020 [1].

La personne mise en examen, irrecevable à soulever un moyen de nullité devant la chambre de l'instruction en raison de l'expiration du délai de forclusion prévu par l'article 173-1 du code de procédure pénale, ne saurait être admise à invoquer ce

[1] Crim. 9 février 2021, n° 20-84.852 et n° 20-84.915

moyen devant la Cour de cassation, y compris pour faire grief à ladite chambre de l'instruction de l'avoir rejeté [2].

Dès lors, le moyen unique de cassation sera déclaré irrecevable en tant qu'il est proposé par M. [M].

M. [R] [K] ayant été mis en examen le 12 juin 2020, le délai de forclusion qui expirait le samedi 12 décembre 2020, a été prorogé jusqu'au premier jour ouvrable suivant, soit le lundi 14 décembre 2020, jour du dépôt de la requête.

La chambre de l'instruction a donc déclaré à juste titre sa requête recevable.

Analyse succincte du moyen

M. [R] [K] propose un moyen unique de cassation, décomposé en quatre branches tendant à faire juger que le droit de l'Union européenne s'oppose à la conservation généralisée et indifférenciée des données de trafic et de localisation, que le ministère public n'est pas une autorité indépendante compétente pour autoriser l'accès d'une autorité publique aux données de connexion et, subsidiairement, que le juge pénal doit écarter les éléments de preuve obtenu par une telle conservation dès lors que les personnes mises en cause ne sont pas en mesure de les commenter efficacement et que ces éléments sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

La chambre de l'instruction aurait méconnu l'article 15, § 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, lu à la lumière des articles 7, 8, 11 et 52, § 1er, de la charte des droits fondamentaux de l'Union européenne en estimant que le droit de l'Union européenne ne s'opposait pas à cette conservation généralisée des données et se serait prononcée par des motifs impropres et inopérants en jugeant d'une part que la conservation de l'ensemble des données de M. [K] ne portait pas une atteinte disproportionnée à son droit au respect de la vie privée ou à la protection de ses données personnelles et d'autre part, que l'accès à ces données a été effectué sous le contrôle de l'autorité judiciaire qui comprend à la fois les magistrats du siège et du parquet. Enfin, elle se serait abstenue de rechercher si l'intéressé était en mesure de commenter efficacement les informations et les éléments de preuve recueillis à son encontre.

Discussion

1°) La directive 2002/58/CE et son interprétation par la CJUE

[2] Crim. 25 mai 2016, n° 16-80.379, Bull. n° 159

La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, “vie privée et communications électroniques”, énonce dans son préambule qu’elle vise à respecter les droits fondamentaux et à garantir le plein respect des droits exposés aux articles 7 et 8 de la charte des droits fondamentaux de l’Union européenne [3].

L’article 15 §1 de cette directive prévoit que les Etats membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes « *lorsqu’une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d’une société démocratique, pour sauvegarder la sécurité nationale — c’est-à-dire la sûreté de l’État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d’infractions pénales ou d’utilisations non autorisées du système de communications électroniques* ». Concernant la préservation des données, l’article 15 § 1 prescrit que leur conservation n’ait lieu que « *pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* ».

La portée de cet article a été précisée par la Cour de justice de l’Union européenne dans sa décision préjudicielle Tele2 Sverige (2016), puis dans les arrêts Minesterio Fiscal (2018) et, plus récemment, Quadrature du net (2020), Prokuuratur (2021) et Commissioner of An Garda Siochana (2022).

L’arrêt Tele 2 Sverige [4]

Selon la CJUE, le droit de l’Union européenne « *s’oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l’ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* ». L’article 15, paragraphe 1 de la directive 2002/58/CE du 12 juillet 2002, lu à la lumière des articles 7, 8 , 11 et 52 de la Charte des droits fondamentaux, fait également obstacle à une réglementation qui donne aux autorités nationales un accès aux données conservées sans le limiter « *aux seules fins de lutte contre la criminalité grave* ».

[3] Ces articles affirment le droit de toute personne au respect de sa vie privée et familale, de son domicile et de ses communications (art. 7), ainsi que le droit à la protection de ses données à caractère personnel (art. 8).

[4] CJUE, 11 grande chambre, 21 décembre 2016, Tele 2 Sverige AB c. Post-och telestyrelsen, Secretary of State for the Home Department c. T. Watson et a., affaires jointes C-203/15 et C-698/15

la CJUE reprend, pour l'essentiel, le raisonnement tenu dans l'arrêt Digital Rights[5] quant aux risques pour la vie privée d'une telle conservation généralisée des données de connexion. Les Etats membres ne peuvent prévoir qu'une conservation « *ciblée* » des données à condition qu'elle soit, « *en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire* ». Elle subordonne enfin l'accès des autorités nationales compétentes aux données conservées, sauf cas d'urgence « *à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante* ».

L'arrêt Minesterio Fiscal [6]

Dans un arrêt du 2 octobre 2018, la Cour de Justice de l'Union Européenne a reconnu que les infractions pénales sans particulière gravité peuvent justifier un accès aux données personnelles conservées par les fournisseurs de services de communications électroniques, lorsqu'un tel accès ne porte pas une atteinte injustifiée à la vie privée.

En l'occurrence, elle considère que le recueil des noms et coordonnées des titulaires des cartes SIM insérées dans un téléphone volé, ne constitue pas une atteinte grave à la vie privée.

Comme le rappelle l'avocat général dans ses conclusions, faisant référence à l'arrêt Tele2 , « *c'est uniquement lorsque l'ingérence subie est d'une particulière gravité [...] que les infractions susceptibles de justifier une telle ingérence doivent elles-mêmes être d'une particulière gravité* ». En d'autres termes, c'est le critère de la gravité de l'ingérence qui détermine les conditions d'accès par les autorités publiques aux données conservées par les fournisseurs de services de communications électroniques, seules les infractions graves pouvant légitimer une ingérence grave.

L'arrêt Quadrature du net [7]

La CJUE était saisi de questions préjudicielles transmises par le Conseil d'Etat [8] et par la Cour constitutionnelle belge [9].

---

[5] CJUE, grande chambre, 8 avril 2014, n° C-293/12, Digital Rights Ireland Ltd

[6] CJUE, grande chambre, 2 octobre 2018, n° C-207/16, Ministerio Fiscal

[7] CJUE, gr.ch., 6 oct. 2020, aff. jtes C-511/18, La Quadrature du Net e.a., aff. C-512/18, French Data Network e.a., aff. C-520/18, Ordre des barreaux francophones et germanophones.

[8] Arrêts du 26 juillet 2018 (Quadrature du Net et French Data Network)

La Cour réitère le principe dégagé dans sa jurisprudence antérieure d'interdiction d'une conservation généralisée des données de connexion mais y apporte des exceptions.

Elle considère que l'importance de l'objectif de sauvegarde de la sécurité nationale peut justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier les autres objectifs que sont la lutte contre la criminalité, même grave, ainsi que la sauvegarde de la sécurité publique (§ 136).

Ainsi, l'article 15 paragraphe 1 de la directive 2002/58 « *ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave... pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* ».

La Cour ajoute que la décision de recourir à une telle mesure doit pouvoir faire l'objet d'un contrôle effectif par une juridiction ou une entité administrative indépendante (§ 139).

S'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation (§ 140).

C'est pourquoi « *une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* » (§ 141).

Reprenant les mêmes considérations que dans l'arrêt Tele 2, la Cour défend l'idée d'une « *conservation ciblée* » des données de connexion, en fonction des catégories de personnes concernées, préalablement identifiées comme présentant une menace pour la sécurité publique ou nationale, ou de critères géographiques (zones exposées à la

[9] Demande présentée le 2 août 2018

criminalité grave, lieux stratégiques tels que gares, aéroports et péages routiers) (§ 148 à 150).

En ce qui concerne la conservation préventive des adresses IP, la Cour estime que seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation (§ 151).

Elle confirme par ailleurs sa jurisprudence Ministerio Fiscal, en estimant que la conservation des données relatives à l'identité des utilisateurs des moyens de communications électroniques ne constitue pas une ingérence grave et qu'il peut être imposé aux fournisseurs d'accès de les conserver, sans condition de délai, aux fins de prévention, recherche, détection et poursuite d'infractions pénales (§ 157 à 159).

La Cour admet néanmoins que durant la période où les données de connexion sont traitées et stockés par les fournisseurs d'accès, peuvent se présenter des situations dans lesquelles il importe de conserver ces données aux fins d'élucidation d'infractions pénales graves déjà constatées ou dont l'existence peut être raisonnablement soupçonnée (§ 160 et 161). Dans de telles situations, « *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* » (§ 161). La Cour précise que seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier une telle conservation rapide et que cette conservation, décidée par l'autorité compétente soumise à un contrôle juridictionnel effectif, ne doit porter que sur les seules données utiles à l'élucidation de l'infraction grave ou de l'atteinte à la sécurité nationale concernée, sans être limitée aux données des personnes soupçonnées (§ 163 à 165).

La Cour précise enfin le régime des preuves obtenues en violation du droit de l'Union : L'article 15 de la directive, interprété à la lumière du principe d'effectivité, impose au juge national d'écarter des informations ou éléments de preuve obtenus par une conservation généralisée et indifférenciée incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si les personnes soupçonnées ne sont pas en mesure de prendre efficacement position sur 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 (§ 227) [10].

[10] Les conditions posées sont cumulatives.

Commentant cet arrêt, le professeur Dominique Berlin constate que « *compte tenu de l'importance des objectifs poursuivis par certaines législations nationales en la matière, notamment la lutte contre la criminalité grave et la préservation de la sécurité publique, la Cour accepte un infléchissement de sa jurisprudence pour légitimer, sous condition, ces législations nationales afin de mieux en encadrer l'exercice. Parmi ces conditions, dont le non-respect est susceptible d'entraîner l'inapplicabilité, on notera les objectifs seuls susceptibles de légitimer les atteintes aux droits garantis, le principe de proportionnalité et le nécessaire contrôle administratif et/ou judiciaire des mesures d'application ».*

S'agissant de l'impact de cet arrêt, le même auteur relève que « *la victime d'une atteinte à ses droits en la matière devra donc désormais se concentrer sur la démonstration du caractère disproportionné des mesures dont elle a dû subir les effets. D'autant plus que le caractère trop général de celles-ci fragilisera leur licéité. Le contrôle de la cohérence des moyens utilisés au regard de l'objectif légitime poursuivi ajoute un autre angle d'attaque devant le juge. À l'inverse les États retrouvent une marge de manœuvre nécessaire à la lutte contre le terrorisme* » [11].

[11] Dominique Berlin « La Cour de justice revient sur l'interdiction absolue des mesures générales de conservation et de traitement des données à caractère personnel, pour finalement en dresser le régime dérogatoire », La Semaine du droit, Ed. Générale - N° 48 - 23 novembre 2020

Etant observé que la CJUE refuse expressément au juge national la faculté de moduler les effets dans le temps de la déclaration de non-conformité au droit de l'Union, M. Galland s'interroge sur ce qu'il advient « *de l'admissibilité et de l'exploitation, dans des procédures nationales ouvertes, d'informations ou d'éléments de preuves de téléphonie conservés dans des conditions déclarées incompatibles avec le droit de l'Union* ». Il note que « *de manière très explicite, le juge européen refuse toute modulation des effets dans le temps de sa décision. En revanche, il reconnaît la possibilité au juge national de ne pas vicier l'entière procédure en appréciant in concreto si l'admissibilité et l'exploitation des éléments de preuve obtenues en contravention au droit de l'Union sont néanmoins rendues envisageables par un exercice effectif des droits garantissant un procès équitable avant tout jugement définitif* [...] *À cette occasion et en vertu du principe d'équivalence, le juge national saisi au fond de la validité de la preuve de téléphonie devra être en mesure de l'écarter ou de l'annuler s'il considère que, en appliquant la norme nationale, le suspect ne bénéficiera pas d'une protection analogue à celle conférée par l'état du droit de l'Union* » [12].

L'arrêt Quadrature du net n'offre aucune réponse immédiate aux questions liées à l'utilisation des données de connexion en matière de lutte contre les abus de marché. Dans le cadre de questions préjudicielles transmises par la chambre criminelle de la Cour de cassation [13], la CJUE est invitée à se prononcer sur l'articulation entre la directive vie privée et le droit dérivé du règlement 596/2014/UE appelant les Etats membres à mettre en place des dispositifs de conservation de données de connexion permettant aux autorités administratives d'apporter la preuve d'opérations d'initiés ou de manipulations de marché et d'en identifier les auteurs.

Cette demande est actuellement pendante devant la Cour [14].

L'arrêt Prokuratuur [15]

Sur une demande de question préjudicielle introduite par la Cour suprême d'Estonie, la cour était appelée notamment à se prononcer sur l'accès des autorités nationales compétentes aux données conservées.

Elle juge « *essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction soit par*

---

[12] Maxime Galland, « Le droit de l'Union applicable à la conservation des données de connexion », Bulletin Joly Bourse du 1er janvier 2021 - n°01 - page 16

[13] Crim. 1er avril 2020, n° 19-80.908 et Crim. 1er avril 2020, n° 19-82.223

[14] Affaires jointes C-339/20 et C-397/20

[15] CJUE, gr. ch., 2 mars 2021, aff. C-746/18, H. K. c/ Prokuratuur

une entité administrative indépendante » (§ 51) et que « *l'exigence d'indépendance implique... que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale. Tel n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique* » (§ 54 et 55).

L'arrêt GD, Commissioner of An Garda Siochana [16]

La Cour suprême d'Irlande a posé, le 25 mars 2020, la question de savoir si un régime général/universel de conservation des données, même assorti de restrictions strictes en matière de conservation et d'accès, est en soi, contraire aux dispositions de l'article 15 de la directive 2002/58/CE 1 , interprétées à la lumière de la Charte.

La CJUE maintient entièrement sa jurisprudence Quadrature du Net selon laquelle la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques n'est autorisée qu'en cas de menace grave pour la sécurité nationale, en apportant un certain nombre de précisions.

Ainsi, elle rejette l'argumentation selon laquelle la criminalité particulièrement grave pourrait être assimilée à une menace pour la sécurité nationale. Elle estime, en effet, qu' « *une telle menace se distingue..., par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent, du risque général et permanent qu'est celui de survenance de tensions ou de troubles, même graves, à la sécurité publique ou celui d'infractions pénales graves* » (§ 62).

En revanche, elle entre plus explicitement dans le détail des mesures législatives que peuvent adopter les Etats, afin de lutter contre la criminalité grave et de prévenir des menaces graves contre la sécurité publique, dont elle indique qu'elles peuvent être combinées entre elles et doivent en tout état de cause respecter les exigences de nécessité et de proportionnalité par rapport à l'objectif poursuivi (§ 67, 92 et 93).

En ce qui concerne la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, la Cour indique que « *ni cette directive* [vie privée et communications électroniques] *ni aucun autre acte du droit de l'Union ne s'opposent à une législation nationale, ayant pour objet la lutte contre la criminalité grave, en vertu de laquelle* ***l'acquisition d'un moyen de communication électronique, tel qu'une carte SIM prépayée, est subordonnée à la vérification de documents officiels établissant l'identité de l'acheteur et à***

[16] CJUE Gr. Ch. 5 avril 2022, aff. C-140/20, GD, Commissioner of An Garda Siochana (Chef de la police nationale d'Irlande)

l'enregistrement, par le vendeur, des informations en résultant*, le vendeur étant le cas échéant tenu de donner accès à ces informations aux autorités nationales compétentes* » (§ 72).

Les mesures de conservation ciblée peuvent quant à elle être prises sur des critères géographiques, tel que notamment le taux moyen de criminalité dans une zone déterminée ou le caractère sensible ou particulièrement fréquenté de certains lieux comme les infrastructures aéroportuaires, ferroviaires, portuaires, autoroutières etc. (§ 81) ou encore viser des personnes faisant l'objet de mesures de surveillance ou de condamnations inscrites au casier judiciaire (§ 78).

S'agissant des mesures législatives prévoyant une conservation rapide des données de trafic et de localisation, la Cour précise que « ***la directive n'exige pas que l'injonction imposant une conservation rapide soit limitée à des suspects identifiés préalablement à une telle injonction*** » (§ 75).

L'injonction de conservation rapide vise les données dont les opérateurs disposent encore pendant le temps nécessaire à leur traitement et leur stockage s'il est nécessaire de les conserver au delà des délais légaux d'effacement, aux fins d'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, qu'il s'agisse d'infractions ou d'atteintes déjà constatées ou pouvant être raisonnablement soupçonnées et sous réserve que la mesure soit limitée dans le temps et soumise à un contrôle juridictionnel effectif (§ 85).

Reprenant le point 164 de l'arrêt Quadrature du Net, la Cour spécifie que « *dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement... les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu* » et que seules la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier l'ingérence dans les droits fondamentaux qu'est susceptible de comporter une telle conservation (§ 87).

Une telle mesure peut être étendue à des personnes autres que celles soupçonnées, si elles peuvent contribuer à l'élucidation d'une infraction pénale grave ou d'une atteinte à la sécurité nationale, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel ou plus généralement des personnes avec lesquelles la victime a été en contact antérieurement à la survenance d'une menace grave pour la sécurité publique ou d'un acte de criminalité grave (§ 88).

La conservation rapide peut être ordonnée « ***dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique ou 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* » (§ 91).

La Cour rejette également l'argumentation selon laquelle « *les autorités nationales compétentes devraient pouvoir accéder, aux fins de la lutte contre la criminalité grave, aux données relatives au trafic et aux données de localisation qui ont été conservées de manière généralisée et indifférenciée, conformément à sa jurisprudence..., pour faire face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* ». En effet, cette argumentation fait dépendre cet accès de circonstances étrangères à l'objectif de lutte contre la criminalité grave. En outre, selon ladite argumentation, l'accès pourrait être justifié par un objectif d'une importance moindre que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale, ce qui irait à l'encontre de la hiérarchie des objectifs d'intérêt général dans le cadre de laquelle doit s'apprécier la proportionnalité d'une mesure de conservation. Par ailleurs, autoriser un tel accès risquerait de priver de tout effet utile l'interdiction de procéder à une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave (§ 96 à 100).

S'agissant de l'accès des autorités nationales compétentes aux données conservées la Cour, confirmant sa jurisprudence ProKuratuur, impose qu'il soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante. Cette juridiction ou entité doit pouvoir assurer un juste équilibre entre les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et les droits fondamentaux au respect de la vie privée et à la protection des personnes concernées (§ 107). Elle précise que lorsque ce contrôle est effectué non par une juridiction, mais par une entité administrative indépendante, cette entité doit disposer d'un statut d'indépendance garantissant qu'elle ne soit pas impliquée dans la conduite de l'enquête pénale en cause et qu'elle ait une position de neutralité à l'égard des parties (§ 108).

La Cour rappelle enfin que l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité (§ 128).

Cette décision fait notamment ressortir les éléments suivants, utiles à l'examen du présent pourvoi :

S'agissant de la conservation des données aux fins de lutte contre la criminalité grave, la CJUE admet la possibilité de recourir, sous certaines conditions, à une injonction faite aux opérateurs de procéder à la conservation dite " rapide " des données relatives au trafic et des données de localisation dont ils disposent.

Ce mécanisme, sorte de " gel des lieux numérique ", concerne au premier chef les données techniques conservées dans un but commercial, comme le rappelle l'avocat général au point 46 de ses conclusions en indiquant que « *s'agissant des données que les opérateurs stockent à des fins commerciales, la Cour, dans l'arrêt Quadrature du Net,*

les lie à l'objectif pour lequel elles ont été collectées et autorise uniquement leur éventuelle conservation rapide ».

Mais en énonçant au paragraphe 87 de l'arrêt que les Etats membres doivent spécifier dans leur législation la finalité de cette conservation rapide, dès lors qu'elle ne correspond plus à « *celles pour lesquelles les données ont été collectées et conservées initialement* », la Cour admet nécessairement, comme elle l'avait déjà fait dans l'arrêt Quadrature du Net, que la collecte des données peut répondre à plusieurs objectifs et qu'ainsi toutes les données disponibles peuvent être temporairement gelées, qu'il s'agisse de celles recueillies à des fins commerciales ou pour faire face à un menace grave pour la sécurité nationale.

On voit mal, d'ailleurs, comment un tri pourrait être opéré dans les données stockées en fonction de la finalité pour laquelle elles ont été conservées initialement.

Ajoutons que cette faculté de conservation rapide, subordonnée au respect de conditions matérielles et procédurales n'est pas en contradiction avec l'interdiction posée par la Cour au paragraphe 100 de l'arrêt d'accéder, sans autre formalité, dans le cadre d'enquêtes et de poursuites pénales, aux données relatives au trafic et aux données de localisation qui ont été conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale.

Il convient de consacrer quelques développements au mécanisme de conservation rapide des données, auquel se réfère la CJUE.

La référence au mécanisme dit de « conservation rapide »

La conservation dite « rapide » est un mécanisme autonome, issu de la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité, ratifiée par la France, qui consiste à permettre aux autorités étatiques de requérir d'un opérateur le gel temporaire du traitement des données relatives à une personne.

Plus précisément, l'article 16 de la Convention 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 de la Convention 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.

Le rapport explicatif de cette Convention [17] indique, à propos de la conservation rapide de données stockées que « *les mesures mentionnées dans les articles 16 et 17 s'appliquent aux* ***données stockées qui ont déjà été collectées et archivées par les détenteurs de données****, tels que les fournisseurs de services. Elles ne s'appliquent pas à la collecte en temps réel et à la conservation de futures données relatives au trafic ni à l'accès en temps réel au contenu des communications* » (§ 149). Ces mesures « *ne sont applicables que lorsque* ***les données informatiques existent déjà et sont en cours de stockage*** » (§ 150).

Dans une approche globale de la notion de conservation rapide, le rapport distingue ensuite le ‟ gel ” des données de leur ‟ divulgation ” (§ 152), c'est à dire les deux étapes, consistant, pour la première, à ‟ fixer ” les données et, pour la seconde, à en prendre connaissance.

Le rapport spécifie que l'article 16 de la Convention « *vise à donner aux autorités nationales compétentes la possibilité d'ordonner ou d'obtenir par un moyen similaire la conservation rapide de données électroniques stockées spécifiées dans le cadre d'une enquête ou d'une procédure pénale spécifique* » (§ 158). La Convention introduit une certaine souplesse puisque « *la mention ‟ ordonner ou ... obtenir par un moyen similaire ” vise à* ***autoriser la mise en œuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative ou une instruction*** *(de la police ou du parquet, par exemple). Dans certains États, le droit de procédure ne prévoit pas d'injonctions de conservation; les données ne peuvent alors être conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire* [...] *Toutefois, il est recommandé aux États 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* »

La Convention **n'impose donc pas aux États de prévoir impérieusement dans le droit interne une phase de gel des données**, elle leur conseille simplement d'y recourir dès lors qu'ils ne disposent d'aucun autre moyen juridique de le faire.

Si le mécanisme de la conservation rapide est, en tant que tel, inconnu en droit interne, le code pénal, en imposant à tout un chacun de répondre aux réquisitions des autorités judiciaires instaure un pouvoir de réquisition qui peut être parfaitement assimilé à une injonction de conservation rapide.

Ainsi le code de procédure pénale autorise de nombreuses réquisitions spécifiques et notamment celles des articles 60-2, 77-1-2, et 99-4 que l'on peut qualifier de ‟ réquisitions informatiques ". Celles-ci permettent aux enquêteurs **de se faire transmettre les informations** contenues dans un système informatique mais

[17] Rapport explicatif de la Convention sur la cybercriminalité, site du Conseil de l'Europe

également de **préserver le contenu des informations** consultées par les utilisateurs d'un système informatique.

L'article 60-2 alinéa 2 du code de procédure pénale prévoit en effet , depuis sa création par la loi n° 2004-204 du 9 mars 2004 que les opérateurs de télécommunications peuvent être requis « *de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs* ».

La procédure pénale française offre donc une double possibilité :

- La réquisition aux fins de transmission directe et immédiate des données de connexion;

- la réquisition aux fins de " préservation " des données de connexion qui est celle qui se rapproche le plus de la conservation rapide.

Eléments de droit comparé

En **Belgique**, un projet de loi déposé par le gouvernement [18] vise à rétablir un cadre juridique conforme à la jurisprudence européenne, en matière de conservation des "métadonnées" ou "données de trafic et de localisation" par les opérateurs.

Une conservation généralisée et indifférenciée des données est prévue en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

Le projet de loi envisage par ailleurs une conservation ciblée sur des personnes, sur base géographique, en fonction des statistiques de criminalité grave, ou encore fondée sur des lieux stratégiques.

Ces mesures viennent compléter d'autres dispositifs, le « quick freeze » consistant à demander une conservation rapide de données existantes, qui figure déjà dans la procédure pénale belge, par transposition de la Convention de Budapest, et le « future freeze », autrement dit un gel en temps réel des données générées ou traitées par les opérateurs qui serait ordonné à l'égard d'une personne ou d'un groupe de personnes, d'un lieu ou d'un moyen de communication. Il pourrait également s'agir de données que les opérateurs conserveraient pour leurs propres besoins.

De telles mesures seraient accompagnées de garanties procédurales importantes (demande du procureur du Roi ou d'un juge d'instruction, application des principes

[18] Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, 17 mars 2022

essentiels : droit de consulter le dossier, d'en prendre copie, de contester la régularité de la procédure, exercice de voies de recours...).

En **Allemagne**, les dispositions en vigueur distinguent d'une part l'accès aux données de trafic conservées par les opérateurs à des fins commerciales et d'autre part l'accès aux données conservées par ces mêmes opérateurs en application de la loi sur les télécommunications (article 176 TKG) qui leur impose une minimale de stockage de six semaines pour les données de trafic à l'exception des données de géolocalisation et de quatre semaines pour les données de géolocalisation.

L'accès aux données de trafic conservées en application de l'article 176 TKG n'est possible, sous certaines conditions, que pour des infractions graves, et sur autorisation d'un juge ou validation postérieure par ce dernier en cas d'urgence.

De fait, dans l'attente d'une décision de la CJUE sur la conformité de l'article 176 TKG au droit de l'Union, les autorités judiciaires et les enquêteurs n'ont accès qu'aux données conservées à des fins commerciales. Le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne) a en effet transmis le 29 octobre 2019 des questions préjudicielles portant à nouveau sur le stockage des données de connexion et l'accès à ces données, en faisant valoir que la législation nationale applicable avait substantiellement réduit le type de données conservées, ainsi que la durée de l'obligation de les conserver et offrait désormais une protection efficace de ces données contre les risques d'abus et d'accès illicite [19].

L'**Autriche** a adopté en 2017, dans un souci de conformité avec la jurisprudence européenne un système de « quick freeze » qui comporte deux étapes : une étape de rétention des données, sur injonction délivrée aux opérateurs, pour durée maximale d'un an (ces données, normalement supprimées après la facturation, sont les données de trafic, d'accès et de localisation conservées à des fins commerciales) et une étape d'autorisation des autorités d'enquête à accéder à ces données (sur autorisation d'un juge et soumise à l'existence de preuves d'une infraction grave).

Aux **Pays-Bas**, depuis l'arrêt de la CJUE Digital Rights de 2014, le droit néerlandais n'impose plus aux fournisseurs d'un service de télécommunications l'obligation de conserver des données.

L'**Estonie** a adapté une partie de sa législation, l'accès aux métadonnées relevant largement du contrôle du juge, mais ce pays reste, comme l'Autriche, l'Allemagne et les Pays-Bas, et pour l'instant la Belgique, sans réglementation d'obligation de conservation des données en vue d'investigations judiciaires.

Enfin, malgré une conservation toujours généralisée des données, l'**Espagne** et l'**Italie** paraissent considérer que leur législation est conforme au droit européen.

---

[19] Affaires jointes C-793/19 et C-794/19

2°) La jurisprudence de la Cour européenne des droits de l'homme

Si la Cour européenne des droits de l'homme a eu à examiner la compatibilité, sous l'angle de l'article 8 de la Convention, d'un régime prévoyant la possibilité pour une autorité publique d'acquérir des données de communications auprès d'un fournisseur de services de communication, il ne semble pas qu'elle ait été amenée à se prononcer sur la question de la conservation des données auprès de tels opérateurs économiques.

Dans l'affaire Malone c. Royaume Uni [20], la Cour a estimé que l'exploitation d'informations enregistrées par un bureau de poste concernant la date et la durée des appels téléphoniques, ainsi que les numéros composés pouvait poser problème au regard de l'article 8, dans la mesure où l'abonné n'avait pas consenti à ce qu'elles soient révélées à la police. Cette atteinte ne pouvait donc être justifiée que si elle était « *prévue par la loi* » et « *nécessaire dans une société démocratique* ». Or, la Cour européenne a relevé l'absence de cadre juridique régissant l'acquisition des données auprès de la Poste, constatant ainsi la violation de cette disposition conventionnelle, sans qu'il soit nécessaire d'examiner sa nécessité.

[20] CEDH 2 août 1984, Malone c. Royaume Uni, n° 8691/79

Dans l'affaire Ben Faiza c. France [21], la Cour a conclu à l'absence de violation de l'article 8 concernant la réquisition judiciaire adressée à un opérateur de téléphonie mobile pour obtenir la liste des bornes déclenchées par la ligne téléphonique du requérant afin de retracer a posteriori ses déplacements. Elle a relevé à cet égard que la réquisition judiciaire avait constitué une ingérence dans la vie privée du requérant mais que celle-ci était prévue par la loi. Visant en outre à permettre la manifestation de la vérité dans le cadre d'une procédure pénale relative à des faits d'importation de stupéfiants en bande organisée, d'association de malfaiteurs et de blanchiment, la réquisition judiciaire avait poursuivi un but légitime, à savoir la défense de l'ordre, la prévention des infractions pénales ainsi que la protection de la santé publique. La Cour a également estimé que cette mesure avait été nécessaire dans une société démocratique car elle avait visé à démanteler un trafic de stupéfiants de grande ampleur.

Dans l'affaire Big Brother Watch et autres c. Royaume-Uni, la Cour européenne des droits de l'homme , à propos de la décision des autorités britanniques de recourir à un régime d'interception massive de communications, s'est prononcée à nouveau sur l'obtention de données de communication auprès de fournisseurs de services de communication [22]. Elle a jugé que les dispositions internes issues du "Regulation of Investigatory Powers Act" ne pouvaient être conformes à la loi au sens de l'article 8 de la Convention européenne : « *Il est donc clair que le droit interne, tel qu'interprété par les autorités internes à la lumière des derniers arrêts de la CJUE, commande que tout régime permettant aux autorités d'accéder aux données conservées par un fournisseur de services de communication limite cet accès au but de lutter contre les « infractions graves » et le soumette au contrôle préalable d'un tribunal ou d'une instance administrative indépendante. Dès lors que le régime découlant du chapitre II permet d'accéder aux données dans le but de lutter contre les infractions (et non spécifiquement contre les « infractions graves ») et n'est pas soumis au contrôle préalable d'un tribunal ou d'une instance administrative indépendante sauf lorsqu'il s'agit d'accéder aux données pour déterminer la source d'un journaliste, il ne peut être considéré comme prévu par la loi au sens de l'article 8 de la Convention* » (§ 467).

Par un arrêt du 25 mai 2021 [23] , la Grande chambre, devant laquelle l'affaire avait été renvoyée, a estimé pour les mêmes raisons que le régime britannique d'obtention de données de communication auprès des fournisseurs de services de communication était contraire aux articles 8 et 10.

---

[21] CEDH, 8 mai 2018, Ben Faiza c. France, n° 31446/12

[22] CEDH 13 sept. 2018, Big Brother Watch et a. c. Royaume-Uni, nos 58170/13, 62322/14 et 24960/15

[23] CEDH 25 mai 2021, Big Brother Watch et autres c. Royaume-Uni, req. nos 58170/13, 62322/14 et 24960/15

Il convient de mentionner que si la Convention garantit en son article 6 le droit à un procès équitable , elle ne réglemente pas pour autant l' admissibilité des preuves en tant que telle, matière qui dès lors relève au premier chef du droit interne.

Dès lors, « *il n'appartient pas à la Cour de se prononcer, par principe, sur la recevabilité de certaines sortes d'éléments de preuve, par exemple des éléments obtenus de manière illégale, ou encore sur la culpabilité du requérant. Il y a lieu d'examiner si la procédure, y compris la manière dont les éléments de preuve ont été obtenus, fut équitable dans son ensemble, ce qui implique l'examen de l'« illégalité » en question et, dans les cas où se trouve en cause la violation d'un autre droit protégé par la Convention, de la nature de cette violation* » [24].

La Cour considère que « *pour déterminer si la procédure dans son ensemble a été équitable, il faut aussi se demander si les droits de la défense ont été respectés. Il faut rechercher notamment si le requérant s'est vu offrir la possibilité de remettre en question l'authenticité de l'élément de preuve et de s'opposer à son utilisation. Il faut prendre également en compte la qualité de l'élément de preuve, y compris le point de savoir si les circonstances dans lesquelles il a été recueilli font douter de sa fiabilité ou de son exactitude. Si un problème d'équité ne se pose pas nécessairement lorsque la preuve obtenue n'est pas corroborée par d'autres éléments, il faut noter que lorsqu'elle est très solide et ne prête à aucun doute, le besoin d'autres éléments à l'appui devient moindre* » [25].

À cet égard, la Cour attache aussi de l'importance au point de savoir si l'élément de preuve en question était ou non déterminant pour l'issue du procès pénal [26].

On relève ainsi des similitudes entre la jurisprudence de la CEDH et celle de la CJUE s'agissant de l'admissibilité des moyens de preuve.

3°) L'évolution du dispositif français de collecte et de consultation des données

Les dispositions antérieures prévoyant le principe de conservation généralisée

L'article L. 34-1 paragraphe III du code des postes et communications électroniques (CPCE), dans sa version ancienne (applicable du 20 décembre 2013 au 31 juillet

[24] CEDH 12 mai 2000, req. n° 35394/97, Khan c. Royaume-Uni, § 34. Voir également CEDH 25 sept. 2001, P.G. ET J.H. c. Royaume-Uni, CEDH 5 nov. 2002, Allan c. Royaume-Uni.

[25] CEDH 10 mars 2009, req. n° 4378/02, Bykov c. Russie, § 89, CEDH 11 juillet 2006, req. n° 54810/00, Jalloh c. Allemagne, § 96

[26] CEDH 1er juin 2010, Gäfgen c. Allemagne, req. no 22978/05

2021), faisait obligation aux opérateurs de communications électroniques de conserver de façon généralisée et indifférenciée, pour une durée d'un an, les données de trafic et de localisation de l'ensemble de leurs utilisateurs, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

L'article R. 10-3 du même code énumérait les catégories de données relevant de ce régime : informations permettant d'identifier l'utilisateur, données relatives aux équipements terminaux de communication utilisés, caractéristiques techniques ainsi que date, horaire et durée de chaque communication, données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs et, enfin, données permettant d'identifier le ou les destinataires de la communication.

Ce dispositif s'est ajouté à celui figurant désormais au II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, qui fait obligation aux fournisseurs d'accès à internet et aux hébergeurs de conserver les données nécessaires à l'identification des personnes créant, modifiant ou supprimant des contenus en ligne, données dont l'autorité judiciaire peut requérir communication.

Le contenu des données de connexion mérite d'être précisé, en reprenant quelques éléments de définition : « *Les données de connexion, également appelées "métadonnées" ou encore "données relatives au trafic et données de localisation"portent, non pas sur le contenu des messages, mais sur les conditions dans lesquelles ces derniers sont consultés ou échangés. Elles sont relatives à l'identité et à la localisation de l'auteur et du destinataire de communications, à la date et à la durée de celles-ci, aux matériel, numéros de téléphone et adresses IP utilisés. L'exploitation de ces données repose sur leur conservation généralisée, indifférenciée, pendant un certain temps, par les opérateurs de communications électroniques, qui sont tenus d'y procéder par la loi* [27]*. Elle permet, dans une certaine mesure, de "lire le passé" en retraçant les activités auxquelles un individu s'est livré sur le réseau avant même d'être soupçonné d'activités criminelles [...] mais [aussi] à "lire le présent" : il s'agit de la géo-localisation en temps réel, à partir des données de connexion, d'un terminal téléphonique ou informatique* » [28].

Les données d'activité communiquées par la Direction des affaires criminelles et des grâces font apparaître un recours massif par les officiers de police judiciaire agissant sur instructions du parquet ou commission rogatoire d'un juge, aux réquisitions tendant à la communication par les opérateurs de données de connexion et leur progression constante depuis 2019. Ainsi le nombre de réquisitions délivrées dans le cadre des enquêtes préliminaires ou de flagrance est passé en trois ans (2019 - 2021) de 1 052 000 à 1 221 000. Les réquisitions établies sur commission rogatoire du juge

[27] Il est fait référence ici à l'article L. 34-1 du CPCE dans sa version ancienne

[28] « L'avenir incertain d'un instrument de lutte contre le terrorisme : l'exploitation des données de connexion », étude par Caroline Grossholz, magistrat administratif, La Semaine Juridique Administrations et Collectivités territoriales n° 27, 10 Juillet 2017, 2177.

d'instruction, au nombre 480 000 en 2019, ont été de 505 000 en 2021. Dans tous les cas, les données fournies ne prennent pas en compte les réquisitions aux fins d'identification de l'abonné.

L'arrêt du Conseil d'Etat du 21 avril 2021, « **French Data network »**

À la suite des précisions apportées par la CJUE dans l'arrêt Quadrature du net, le Conseil d'État, statuant en Assemblée du contentieux, a examiné la conformité au droit européen du régime juridique français de conservation et d'accès aux données de connexion.

La Conseil d'Etat a d'abord refusé d'accéder à la demande du gouvernement, qui l'invitait, en défense, à s'engager dans la voie du contrôle dit " ultra vires " permettant au juge national de faire obstacle à l'application d'une norme du droit de l'Union qui outrepasserait les compétences attribuées à l'Union européenne. Ainsi, « *il n'appartient pas au juge administratif de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la CJUE elle-même, de la répartition des compétences entre l'Union européenne et les Etats membres* » (§ 8).

En revanche, le Conseil d'Etat s'est inspiré d'un autre mécanisme permettant de s'assurer que la transposition d'une directive européenne ne va pas à l'encontre d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France.

Précisant le cadre de son contrôle, il rappelle la place de la Constitution, au sommet de la hiérarchie des normes, ce qui impose de vérifier que l'application du droit européen, tel que précisé par la CJUE, ne compromet pas des exigences constitutionnelles qui ne sont pas garanties de façon équivalente par le droit européen (§ 5). A cet égard, il constate que les objectifs de valeur constitutionnelle que sont la sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, la lutte contre le terrorisme et la recherche des auteurs d'infractions pénale, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des Etats membres, ne bénéficient pas, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution (§ 10).

Le Conseil d'État relève ensuite que la conservation généralisée imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, condition requise par la CJUE. Conformément aux exigences de la Cour, il impose au Gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace.

En revanche, il juge contraire au droit de l'Union l'obligation de conservation généralisée des données (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins autres que ceux de la sécurité nationale, notamment la recherche, la constatation et la poursuite des infractions pénales.

Pour ces infractions, les solutions préconisées par la CJUE de conservation « ciblée » des données de connexion selon des critères géographiques et de conservation « rapide » de ces données se heurtent à des obstacles techniques et juridiques et à des considérations d'efficacité. Toutefois, dans la mesure où les données doivent être conservées aux fins de sauvegarde de la sécurité nationale, « *l'autorité judiciaire est en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie* » (§ 57).

Le Conseil d'Etat justifie sa position en se référant au point 164 de l'arrêt de la CJUE « Quadrature du net » précédemment évoqué.

En d'autres termes, comme l'observe également le Conseil d'Etat, « *lorsqu'est en cause une infraction suffisamment grave pour justifier l'ingérence dans la vie privée induite par la conservation des données de connexion, dans le respect du principe de proportionnalité..., l'autorité judiciaire peut, sans méconnaître ni la directive du 12 juillet 2002, ni le RGPD, enjoindre aux opérateurs de communications électroniques, aux fournisseurs d'accès à intemet et aux hébergeurs de sites intemet de procéder à la conservation rapide des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale* ».

Enfin, tirant les conséquences des illégalités constatées, le Conseil d'Etat constate qu'à la date de publication des dispositions réglementaires critiquées la France était confrontée à une menace grave, réelle et actuelle pour sa sécurité nationale et le demeure à la date de sa décision, si bien que les opérateurs pouvaient se voir imposer la conservation généralisée et indifférenciée des données de trafic et de localisation aux fins de sauvegarde de la sécurité nationale (§ 96).

Dans ses conclusions, M. Alexandre Lallet, rapporteur public, avait également soutenu que les données conservées de manière généralisée et indifférenciée pour les besoins de la sauvegarde de la sécurité nationale devenaient également disponibles pour les services d'enquête :

« *L'arrêt du 6 octobre 2020 n'exclut pas, et même envisage à notre avis, que la conservation rapide à des fins de lutte contre la criminalité grave puisse se greffer sur ce lac de données " sécurité nationale ". Elle* [la Cour de Justice de l'Union] *indique en effet au point 164 de l'arrêt du 6 octobre que la finalité de la conservation rapide doit être précisée dans la loi " dans la mesure où [elle] ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement ". Elle semble ainsi admettre une forme de " déclassement " du motif de conservation, qui apparaît justifié dès l'instant que la conservation rapide n'est pas elle-même généralisée et indifférenciée, mais porte sur des personnes ou des infractions bien identifiées - c'est la logique du bassin de rétention. Ainsi articulée avec le régime de conservation pour les besoins de la sécurité nationale, la conservation rapide pourra porter non seulement sur les données futures, mais aussi sur les données passées, avec la même profondeur d'un an, et avec le champ d'application large admis par la Cour qui permet de geler les données des suspects, des victimes ou*

des tiers dès l'instant qu'elles peuvent contribuer à l'élucidation de l'infraction, mais aussi de sanctuariser les données se rapportant à telle ou telle zone géographique - par exemple la liste des numéros de téléphone ayant " borné " dans un secteur » [29].

L'arrêt du Conseil d'Etat a donné lieu à de nombreux commentaires, dont on ne peut donner ici qu'un bref aperçu.

La plupart des commentateurs approuvent la solution retenue. Ainsi, MM. Malverti et Beaufils considèrent que « *la démarche retenue par le Conseil d'Etat, parce qu'elle parvient à maintenir les divergences avec la CJUE dans un cadre qui leur est commun, s'avère pertinente dans le contexte de pluralisme juridique qui caractérise la construction européenne.*

En refusant de s'engager dans un contrôle ultra vires, en évitant de faire un usage positif des contre-limites constitutionnelles et en leur préférant une utilisation maximale des possibilités ouvertes par la CJUE allant parfois jusqu'à déplacer de quelques pas les bornes posées par celle-ci, l'assemblée du contentieux a en effet choisi, en substance, de confronter à l'interprétation du droit de l'Union retenue par la Cour sa propre interprétation plutôt que de lui opposer le droit national » [30].

Le professeur Roux évoque une « *solution ingénieuse* » qui « *procède d'une lecture volontariste mais plausible de l'arrêt préjudiciel* » et qui « *a le mérite de sauvegarder l'effectivité de la lutte contre la criminalité, sans risque supplémentaire pour le respect de la vie privée* » [31].

---

[29] Alexandre Lallet, « Données personnelles : droit de l'Union européenne et Constitution », RFDA 2021 p. 421

[30] Clément Malverti, Cyrille Beaufils, L'instinct de conservation, AJDA 2021 p.1194

[31] Jérôme Roux, « La lucidité d'une fermeté ajustée », Recueil Dalloz 2021 p.1247

M. Bartolucci insiste néanmoins sur le caractère temporaire de la solution retenue : « *la gravité de la menace terroriste offre en quelque sorte une porte de sortie aux conseillers d'État. Tant que durent dans le temps les menaces qui pèsent sur la sécurité nationale, alors l'obligation de conservation de toutes les données de connexion est régulière, et donc les garanties constitutionnelles (qui couvrent la criminalité ordinaire et la criminalité grave) demeurent protégées. Toute la fragilité du raisonnement tient dans son caractère momentané et éphémère : lorsque le risque terroriste diminuera, ce que l'on espère rapidement, l'équation tombera à l'eau. Étant donné que seule une menace particulièrement élevée autorise la conservation générale des données, qui est à son tour seule à même d'assurer les exigences constitutionnelles, l'absence de menace sérieuse mettra mécaniquement en péril lesdites exigences* » [32].

Enfin, certains commentateurs se montrent plus critiques en estimant que « *loin de se conformer pleinement au droit de l'Union, le Conseil d'État le réinterprète en partie sous couvert de conciliation avec la sauvegarde des objectifs de valeur constitutionnelle* » [33].

La législation actuelle sur la conservation des données de connexion

Pour faire suite à l'arrêt du Conseil d'Etat « French Data network », L. 34-1 du code des postes et télécommunications a été modifié par la loi n° 2021-998 du 30 juillet 2021.

Dans sa nouvelle rédaction, cet article fixe les modalités selon lesquelles les opérateurs de communications électroniques sont tenus de conserver et d'anonymiser certaines données. Par renvoi de l'article 6 II de la loi n° 575-2004 du 21 juin 2004, cet article s'impose également aux fournisseurs d'accès à internet.

Désormais, cet article institue une obligation de conservation indifférenciée et généralisée de trois catégories de données : identité civile de l'utilisateur, informations liées au contrat, au compte et au paiement, adresse IP et ce, quelles que soient les circonstances (II bis de l'article L. 34-1).

Seul un impératif de sauvegarde de la sécurité nationale, en cas de menace grave, actuelle ou prévisible, permet, sur injonction du Premier ministre et pour une durée maximale d'un an renouvelable, la conservation généralisée et indifférenciée de certaines données de trafic et de localisation (art. L. 34-1 III).

Dans le cadre de la criminalité et de la délinquance grave, la faculté est ouverte à l'autorité judiciaire d'accéder à ces données de connexion, via une **injonction de conservation rapide** (art. L. 34-1 III bis).

---

[32] Mattéo Bartolucci, Semaine juridique éd. Administrations et collectivités territoriales, n° 28, 12 juil. 2021

[33] Thibault Douville, « Un arrêt sous le signe de l'exceptionnel », Recueil Dalloz 2021 p.1268

Trois décrets d'application ont été publiés le 20 octobre 2021, dont le décret annuel pris par le premier ministre 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, à savoir les données de trafic et de localisation [34].

Le critère de gravité des infractions justifiant l'accès de l'autorité judiciaire aux données disponibles n'est pas précisé par la loi, laquelle se réfère de manière générale à la « *criminalité* » et à la « *délinquance grave* », mais a été discuté à l'occasion des travaux parlementaires qui ont précédé l'adoption de la loi du 30 juillet 2021.

[34] Décret n° 2021-1363 du 20 octobre 2021

Les rapporteurs de la commission des lois du Sénat [35] reprennent l'analyse du Conseil d'Etat selon laquelle l'arrêt de la Cour de justice de l'Union européenne n'impose pas au législateur d'énumérer les infractions relevant du champ de la criminalité grave en se référant à des catégories strictement prédéfinies en droit interne. Le rattachement d'une infraction pénale à la criminalité grave aurait donc vocation à s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce. Il relèvent par ailleurs que « *la notion de criminalité grave est une notion que l'on retrouve dans divers actes du droit dérivé européen. La directive du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR 53) fixe le niveau de gravité par référence à une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans. Le règlement européen Eurojust du 14 novembre 2018 ne fait pas référence à la peine encourue, mais intègre dans le périmètre de la criminalité grave les infractions commises en amont ou en aval : infractions pénales commises pour se procurer les moyens de perpétrer les formes graves de criminalité, pour faciliter l'exécution de formes graves de criminalité et pour assurer l'impunité de ceux qui commettent les formes graves de criminalité. S'il semble évident que les contraventions ne peuvent être comprises dans cette notion de criminalité grave, il conviendrait pour l'application du dispositif prévu par l'article L. 34-1 du code des postes et des communications électroniques d'y intégrer a minima les délits punis de trois ans d'emprisonnement ou les infractions connexes à la criminalité grave* ».

Lors des débats devant le Sénat en première lecture [36], l'un des deux rapporteurs a indiqué que « *lors des auditions, une difficulté réelle est apparue pour les enquêtes de police judiciaire diligentées par les procureurs de la République. Ces derniers ne pourront plus recourir à des réquisitions de données de connexion dans le cadre d'enquêtes liées à la criminalité ordinaire. En effet, le dispositif mis en place par l'article 15 se limite à la criminalité grave.*

C'est la raison pour laquelle il nous a paru important de mieux définir la notion de criminalité grave et d'étendre les dispositions de cet article à la délinquance grave. Tel est le sens de l'amendement que je vous propose ».

C'est ce qui explique, après adoption de cet amendement, l'ajout dans le texte de loi de la référence à la délinquance grave, outre la criminalité (l'adjectif grave étant resté au singulier).

Cette précision ne paraît pas de nature à faire entrer l'ensemble des délits dans le champ de l'article L. 34-1 du code des postes et des postes et des communications électroniques, mais seulement ceux punis d'au moins trois ans d'emprisonnement, comme le suggérait les rapporteurs de la commission des lois du Sénat.

---

[35] Cf. Rapport au Sénat n° 694 (2020-2021) de M. Marc-Philippe Daubresse et Mme Agnès Canayer, fait au nom de la commission des lois, déposé le 16 juin 2021, article 15

[36] Séance du 29 juin 2021

La loi n° 2022-299 du 2 mars 2022, dont il sera question plus loin impose effectivement de respecter le seuil de trois ans, s'agissant du recours à des réquisitions de données de connexion.

Le nouvel encadrement de l'accès aux données de connexion

Dans sa décision n° 2021-930 QPC du 23 septembre 2021, le Conseil constitutionnel a déclaré conforme à la Constitution la première phrase du 1° de l'article 230-33 du code de procédure pénale, dans sa rédaction résultant de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

Il s'agit des dispositions permettant au procureur de la République d'autoriser le recours à une opération de géolocalisation en temps réel dans le cadre de l'enquête qu'il dirige.

Le Conseil a estimé que le législateur avait entouré la mise en œuvre des mesures de géolocalisation de garanties de nature à assurer, dans le respect des prérogatives de l'autorité judiciaire, une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée.

Le Conseil constitutionnel a été saisi le 23 septembre 2021 par la Cour de cassation d'une question prioritaire de constitutionnalité relative à la conformité aux droits et libertés que la Constitution garantit des articles 77-1-1 et 77-1-2 du code de procédure pénale.

L'article 77-1-1 de ce code permet au procureur de la République ou, sur son autorisation, à un officier ou à un agent de police judiciaire, dans le cadre d'une enquête préliminaire, de requérir, par tout moyen, la remise d'informations détenues par toute personne publique ou privée, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel.

L'article 77-1-2 du même code prévoit quant à lui que, sur autorisation du procureur de la République, l'officier ou l'agent de police judiciaire peut requérir d'un organisme public ou de certaines personnes morales de droit privé, par voie télématique ou informatique, la mise à disposition d'informations non protégées par un secret prévu par la loi, contenues dans un système informatique ou un traitement de données nominatives.

Dans sa décision n° 2021-952 QPC du 3 décembre 2021, le Conseil constitutionnel a relevé qu'en permettant de requérir des informations issues d'un système informatique ou d'un traitement de données nominatives, les dispositions contestées autorisent le

procureur de la République et les officiers et agents de police judiciaire à se faire communiquer des données de connexion ou à y avoir accès.

Il a constaté, d'une part, que les données de connexion comportent des données qui fournissent sur les personnes concernées des informations nombreuses et précises, particulièrement attentatoires à leur vie privée et, d'autre part, que la réquisition de ces données est autorisée dans le cadre d'une enquête préliminaire qui peut porter sur tout type d'infraction et qui n'est pas justifiée par l'urgence ni limitée dans le temps.

Il a relevé enfin que si ces réquisitions sont soumises à l'autorisation du procureur de la République, magistrat de l'ordre judiciaire auquel il revient, en application de l'article 39-3 du code de procédure pénale, de contrôler la légalité des moyens mis en œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits, le législateur n'a assorti le recours aux réquisitions de données de connexion d'aucune autre garantie.

Le Conseil en déduit que dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la recherche des auteurs d'infractions.

Il a donc déclaré contraires à la Constitution les mots «*, y compris celles issues d'un système informatique ou d'un traitement de données nominatives,* » figurant à la première phrase du premier alinéa de l'article 77-1-1 du code de procédure pénale et les mots « *aux réquisitions prévues par le premier alinéa de l'article 60-2* » figurant au premier alinéa de l'article 77-1-2 du même code, en reportant l'abrogation de ces dispositions au 31 décembre 2022.

La doctrine relève que le Conseil constitutionnel analyse l'autorisation délivrée par le procureur comme une garantie essentielle et que seule l'absence d'autres garanties entourant la mesure motive le prononcé de la censure. Il en résulte une appréciation divergente entre le juge constitutionnel et la Cour de justice sur les pouvoirs du parquet en matière d'accès aux données relatives au trafic et à celles de localisation [37].

La loi n° 2022-299 du 2 mars 2022, tirant les conséquences de cette décision, a limité le recours aux réquisitions de données de connexion aux hypothèses prévues par le nouvel article 60-1-2 du code de procédure pénale. Il en résulte notamment que les réquisitions portant sur les données de trafic et de localisation mentionnées au III de l''article L. 34-1 du code des postes et des communications électroniques ne sont possibles, si les nécessités de la procédure l'exigent, que si la procédure porte sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement.

---

[37] Philippe Collet « La censure des réquisitions de données informatiques en enquête préliminaire ! », La Semaine Juridique Edition Générale n° 4, 31 Janvier 2022, 133

Le choix opéré par le législateur a donc été de fixer un quantum de gravité des infractions pour lesquelles le parquet est habilité à autoriser l'accès aux données de connexion.

Néanmoins, la question de la compétence du ministère public pour autoriser l'accès à ces données s'est à nouveau posée.

Par arrêts du 7 décembre 2021[38], la chambre criminelle a renvoyé au Conseil constitutionnel une nouvelle question prioritaire de constitutionnalité portant sur la conformité à la Constitution de l'article L. 34-1 du code des postes et communications électroniques, dans sa version en vigueur jusqu'au 30 juillet 2021, en ce qu'il ne réserve pas la conservation des données de connexion et leur accès aux infractions les plus graves et ne les soumet pas à l'autorisation ou au contrôle d'une juridiction ou d'une autorité indépendante.

Par décision n° 2021-976/977 QPC du 25 février 2022, le Conseil constitutionnel a jugé qu'en autorisant la conservation générale et indifférenciée des données de connexion, les dispositions contestées [article L. 34-1 du CPCE dans sa version ancienne] portent une atteinte disproportionnée au droit au respect de la vie privée et doivent être, par conséquent déclarées contraires à la Constitution. Il a constaté que ces dispositions n'étaient plus en vigueur et a décidé que les mesures ayant été prises sur le fondement des dispositions déclarées contraires à la Constitution en pouvaient être contestées sur le fondement de cette inconstitutionnalité, sauf à méconnaître les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions, ce qui aurait des conséquences manifestement excessives.

Il est à noter que la question soumise au Conseil constitutionnel, circonscrite aux dispositions de l'article L. 34-1 du code des postes et communications électroniques, ne concernait que le régime de la conservation des données de connexion, la question de l'accès à ces données ayant fait l'objet de la décision du 3 décembre 2021 rappelée ci-dessus.

Ajoutons que si, à l'avenir, le juge des libertés et de la détention devait intervenir systématiquement dans le cadre de la mise en œuvre, au stade de l'enquête, de mesures d'investigations telles que la géolocalisation et la communication de données de connexion, une étude d'impact réalisée par la Direction des Services Judiciaires fait apparaître que les effectifs de ces magistrats localisés au sein des tribunaux judiciaires, soit 256 postes à l'heure actuelle, devraient être triplés, voire quadruplés.

Réponse au moyen

[38] n° 21-83.710 et 21-83.729

Dans sa requête en nullité, M. [R] [K] sollicitait l'annulation de l'ensemble des réquisitions visant les lignes téléphoniques, notamment celles dont il avait l'usage ou avec lesquelles il avait pu être en contact et des actes subséquents, au motif de la non conformité au droit de l'Union européenne du régime français de conservation des données de connexion résultant des articles R. 10-13 et L. 34-1 III du code des postes et des communications électroniques, ainsi que des dispositions de l'article 77-1-1 du code de procédure pénale encadrant l'accès des autorités à ces mêmes données.

Plus précisément, le requérant se disait « *directement concerné par plusieurs réquisitions ordonnées durant l'enquête préliminaire puis l'instruction, dès lors qu'il a reconnu avoir été titulaire des lignes téléphoniques objet des réquisitions, notamment des lignes* [XXXXX 01] *ou* [XXXXX02] *(D1625)* ».

Comme le relève la chambre de l'instruction (page 21 de l'arrêt attaqué), il ne résulte pas de la procédure que la ligne [XXXXX03] ait fait l'objet de réquisitions tendant à obtenir d'un opérateur téléphonique des facturations détaillées.

En revanche, la ligne [XXXXX04] apparaît en cours d'information, à la faveur d'un appel passé le 1er juin 2020, en direction de ce numéro, depuis le numéro attribué à la " plate-forme de distribution Uber Green " et placé sous surveillance. Les enquêteurs agissant sur commission rogatoire, obtiennent alors, sur réquisition délivrée le 2 juin suivant, la facturation détaillée et géolocalisée de cette ligne sur une période d'un mois débutant le 1er mai 2020. On relèvera qu'il s'agit d'une ligne prépayée, sans identification possible du client, ouverte le 8 avril 2020 soit postérieurement à la date d'ouverture d'information. L'exploitation des données recueillies permet de conclure que M. [K] est l'utilisateur de cette ligne compte tenu de ce que les relais déclenchés le soir ou la nuit sont proches de son domicile de [Localité 1] ou de l'adresse à laquelle il se rend quotidiennement à [Localité 2] (D 940). L'adresse en question est celle d'un appartement servant de lieu de stockage de produits stupéfiants comme l'ont établi d'autres investigations et notamment la captation d'images autorisée le 19 mai 2020 par le magistrat instructeur (D 1012).

Une seule autre réquisition concernant la même ligne figure au dossier. L'opérateur SFR est requis, le 8 juin 2020 à 3 heures 50 de fournir le détail géolocalisé de cette ligne afin de déterminer si à cet instant M. [K] se trouve au domicile de sa mère, ce qui ne donne aucun résultat (D 978).

M. [K] est interpellé le jour même à son domicile (D 1606).

Pour rejeter la requête conjointe de MM. [M] et [K], la chambre de l'instruction commence par rappeler les circonstances dans lesquelles les intéressés ont été identifiés : Les enquêteurs ont d'abord obtenu, début octobre 2019, les éléments d'identification et la facture détaillée de la ligne téléphonique mentionnée sur la carte de visite " Uber green ". Puis ils ont requis les opérateurs téléphoniques de leur communiquer le détail des communications des dix contacts privilégiés de cette ligne,

ce qui leur a permis de constater qu'ils avaient en commun une ligne récente identifiée dès lors comme le nouveau numéro d'appel du réseau, après abandon de la ligne initiale et dont le détail géolocalisé de l'utilisation a été recueilli pour la période du 29 septembre au 9 octobre 2019.

Agissant désormais sur commission rogatoire du juge d'instruction, les enquêteurs ont identifié en décembre 2019 une ligne téléphonique dédiée aux relations entre la plate-forme de commande et les coursiers et ont obtenu les factures détaillées géolocalisées de cette ligne pour la période du 1er octobre au 17 décembre 2019.

L'exploitation de ces données et l'interception des conversations échangées sur la ligne en question, outre les surveillances physiques, ont permis d'identifier M. [S] [M] et de lui attribuer une ligne téléphonique dont la facture détaillée géolocalisée leur a été communiquée pour la période du 16 au 24 décembre 2019.

En juin 2020, les enquêteurs ont matérialisé un contact entre une ligne placée sous surveillance, utilisée par la plate-forme de commande et une des deux lignes utilisées par M. [R] [K] pour laquelle ils ont obtenu la transmission de factures détaillées géolocalisées, en ce qui concerne les périodes du 1er mai au 2 juin 2020 (et non 2019 comme mentionné par erreur dans l'arrêt) puis du 7 au 8 juin 2020.

La chambre de l'instruction considère que la jurisprudence de la CJUE n'exclut nullement la conservation et l'accès aux données de connexion par les enquêteurs agissant dans le cadre des dispositions du code de procédure pénale. Elle affirme que la Cour admet l'ingérence dans les droits fondamentaux sous réserve du respect du principe de proportionnalité. Elle énonce ensuite que la procédure est relative à des faits de criminalité grave, au sens du droit de l'Union européenne, que les enquêteurs ont conduit des investigations ciblées sur les lignes utilisées par MM. [R] et [M], ont agi sous le contrôle du procureur de la République puis du juge d'instruction et ont employé des moyens proportionnés au regard du but poursuivi de démantèlement d'un important trafic de stupéfiants. Elle considère enfin que par le biais du dépôt d'une requête en nullité, les mis en examen sont en mesure dans le cadre d'un recours juridictionnel effectif de commenter efficacement les éléments de preuve ainsi obtenus.

Sur la conservation des données de connexion (deux premières branches du moyen)

Le moyen se fonde sur le caractère prohibé de la conservation générale et indifférenciée des données de trafic et de localisation et soutient que la chambre de l'instruction ne pouvait pas considérer que l'atteinte portée à la vie privée était proportionnée à l'objectif poursuivi.

Le raisonnement de la chambre de l'instruction repose sur une lecture erronée de l'arrêt de la CJUE Quadrature du Net, dont elle tire inexactement la conclusion que la

lutte contre la criminalité grave justifie l'ingérence dans les droits fondamentaux que constitue une législation nationale autorisant la conservation des données, sous réserve du principe de proportionnalité, sans d'ailleurs préciser de quels types de données il s'agit.

On a vu que la CJUE interprétait l'article 15, paragraphe 1, de la directive 2002/58 comme s'opposant à des mesures législatives prévoyant, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Or les dispositions de l'article L. 34-1 du CPCE, dans sa version ancienne, instauraient une obligation de conservation généralisée des données (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins de la poursuite des infractions pénales et ces normes de conservation étaient manifestement contraires au droit européen, tel qu'interprétées par la CJUE.

Un tel constat ne conduit pas nécessairement à en déduire que les données auxquelles les enquêteurs ont eu accès ont été conservées illicitement.

Dans sa décision French Data Network » le Conseil d'Etat a rappelé que la jurisprudence européenne autorisait la conservation généralisée et indifférenciée des données de connexion pour des motifs de sauvegarde de la sécurité nationale. Il a considéré que cette condition était remplie pour la France et que dès lors, les opérateurs de télécommunications pouvaient se voir imposer cette conservation.

Il s'est fondé ensuite sur le paragraphe 164 de l'arrêt de la CJUE Quadrature du Net, pour admettre que lorsqu'est en cause une infraction grave, l'autorité judiciaire est en mesure d'accéder, par le biais de la conservation rapide, aux données de connexion dont disposent les opérateurs, y compris lorsque cette conservation rapide porte sur des données initialement conservées au titre de la sauvegarde de la sécurité nationale.

Cette interprétation demeure parfaitement valide après l'arrêt de la CJUE Commissioner of An Garda Síochána (§ 87) confirmant la faculté de recourir au mécanisme de la conservation rapide de toutes les données disponibles.

Précisons qu'il est clair que le dispositif législatif français permettait, à la date des faits, la conservation générale et indifférenciée des données de connexion aux fins de sauvegarde de la sécurité nationale, l'objectif de lutte contre le terrorisme et, plus généralement, contre les atteintes aux intérêts fondamentaux de la nation étant évidemment inclus dans celui, plus général, de lutte contre la criminalité.

La chambre de l'instruction ne s'est pas prononcée sur ce point de savoir si au moment des faits reprochés à l'intéressé, soit entre le 1er janvier 2019 et le 8 juin 2020, l'ampleur de la menace terroriste justifiait une collecte généralisée et indifférenciée des données. Il paraît hasardeux de considérer qu'il s'agit là d'une question de pur fait qui

relèverait de l'appréciation des juges, sauf à s'exposer au risque d'appréciations divergentes des juridictions du fond sur l'état de la menace pour la sécurité nationale, selon le moment, le lieu et les circonstances.

A cet égard, la Cour de cassation, dont le rôle est d'assurer l'application uniforme du droit est en mesure de s'appuyer sur le constat du Conseil d'Etat selon lequel le motif de sécurité nationale, qui permet de justifier la conservation générale des données de trafic et de localisation, était présent sur toute la période couverte par les dispositions critiquées et le demeure aujourd'hui (§ 96 de l'arrêt French Data Network) [39].

Au besoin, la chambre criminelle pourra se reporter à la longue liste des attentats djihadistes commis sur le sol français durant la période considérée [40].

A propos du mécanisme de la conservation dite « rapide », il a été souligné que la Convention de Budapest permettait de s'affranchir d'un certain formalisme en se dispensant de l'étape du gel des données et que leur conservation pouvait être opérée par d'autres moyens juridiques que l'injonction judiciaire.

Dans le cas présent, les réquisitions délivrées par les enquêteurs, tendant à obtenir des opérateurs les facturations détaillées et les données de géolocalisation de la ligne prépayée utilisée par M. [R] [K] sont parfaitement assimilables à une injonction de conservation rapide des données.

---

[39] Le Conseil d'Etat fonde notamment ce constat sur la menace terroriste, que révèlent les attentats commis ou déjoués depuis 2015 (§ 66 de l'arrêt) mais également sur des menaces plus persistantes et diffuses, telles que l'espionnage et " l'activité de groupes radicaux et extrémistes " (§ 44), ce qui laisse à penser que la justification de la conservation générale n'est pas près de disparaître.

[40] Voir, en pièce jointe au dossier, la liste fournie par le parquet général de Paris (Cette liste ne recense pas les attentats déjoués par les services de renseignement ou de police)

On a vu, par ailleurs, que la notion de criminalité grave, « *dont les contours doivent être laissés à la main des États membres, dans le cadre de leur compétence de principe en matière pénale* » [41] relevait de l'appréciation concrète du juge pénal, par référence à la nature de l'infraction et à l'ensemble des faits de l'espèce. Nul doute que les infractions relevant de la grande délinquance organisée et notamment les crimes et délits de trafic de stupéfiants pour lesquels la loi donne compétence aux juridictions interrégionales spécialisées [42] entrent par hypothèse dans le champ de la criminalité grave.

En l'espèce, la chambre de l'instruction a caractérisé toutes les circonstances permettant de retenir que les infractions reprochées à M. [R] [K] entraient dans le champ de la criminalité grave.

On peut donc conclure que les données de trafic et de localisation auxquelles les enquêteurs ont eu accès ont été stockées dans des conditions licites, ce qui conduira à écarter les deux premières branches du moyen.

Sur l'accès aux données de connexion (3e branche du moyen)

Le mémoire ampliatif, se référant à l'arrêt Prokuratuur de la CJUE, fait valoir que « *le 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, n'est pas une autorité indépendante compétente pour autoriser l'accès aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale. En jugeant le contraire pour rejeter leurs exceptions de nullité, aux motifs que « l'autorité judiciaire (…) comprend à la fois les magistrats du siège et du parquet » (arrêt attaqué, p. 22, §. 3), la cour d'appel s'est fondée sur des motifs impropres et inopérants à justifier son arrêt* ».

Il est permis de se demander si l'arrêt Prokuratuur, qui concerne le ministère public estonien, est transposable au ministère public français.

Dans sa décision n° 2021-952 QPC du 3 décembre 2021, le Conseil constitutionnel n'a pas eu à se prononcer sur la question de la compétence du parquet pour autoriser les réquisitions de données de connexion mais il semble admettre implicitement cette compétence en analysant l'autorisation délivrée par le procureur comme une garantie essentielle, à l'instar de la géolocalisation [43].

---

[41] Conclusions des avocats généraux de la CJUE dans les affaires Ministerio fiscal et Prokuratuur

[42] Article 706-73, 3° du code de procédure pénale

[43] Décision n° 2021-930 QPC du 23 septembre 2021 : La conseil a jugé qu'eu égard à sa nature et aux garanties qui entourent son prononcé, une mesure de géolocalisation pouvait être ordonnée par le procureur de la République dans le cadre d'une enquête de police.

Il rappelle que « *le procureur de la République* [est] *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* » [44].

En l'espèce, la chambre de l'instruction tient un raisonnement voisin en se référant au principe de l'unité du corps judiciaire et donc à l'appartenance des magistrats du ministère public à l'autorité judiciaire.

Mais en tout état de cause, les données techniques recueillies par les enquêteurs concernant la ligne prépayée utilisée par M. [K], qui ont permis d'orienter les investigations et, en partie, de le mettre en cause dans la présente procédure, ont toutes été diligentées sur commission rogatoire du juge d'instruction et sous le contrôle de ce magistrat.

Pour les raisons qui seront exposées plus loin, M. [K] n'a aucune qualité à agir pour invoquer la nullité de toutes les autres réquisitions de données de connexion y compris celles délivrées en enquête préliminaire.

Dès lors, le moyen qui soutient que le ministère public n'est pas une autorité indépendante compétente pour autoriser l'accès aux données de trafic et de localisation paraît totalement inopérant.

La troisième branche du moyen ne peut donc sérieusement prospérer.

Sur la sanction de la méconnaissance éventuelle du droit européen (4e branche du moyen)

A supposer que les données de connexion aient conservées ou obtenues dans des conditions irrégulières, le problème se pose de savoir quelles conséquences devraient en être tirées en termes de procédure.

Il résulte des arrêts de la CJUE « Quadrature du net » et « Prokuratuur », qu'il appartient au seul juge 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 conservation de données contraire au droit de l'Union. Selon une jurisprudence constante, cette latitude est toutefois conditionnée : l'application des règles nationales ne doit pas être moins favorable (principe d'équivalence) et rendre impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité).

---

[44] § 13 de la décision n° 2021-952 QPC du 3 décembre 2021

L'application stricte du principe d'équivalence conduit à examiner les moyens pris de la violation du droit européen selon la méthodologie précisée par la chambre criminelle dans sa jurisprudence récente en matière de nullités [45] :

« *Hors les cas de nullité d'ordre public, qui touchent à la bonne administration de la justice, la chambre de l'instruction, saisie d'une requête en nullité, doit successivement d'abord rechercher si le requérant a intérêt à demander l'annulation de l'acte, puis, s'il a qualité pour la demander et, enfin, si l'irrégularité alléguée lui a causé un grief.*

Le requérant a intérêt à agir s'il a un intérêt à obtenir l'annulation de l'acte.

Pour déterminer si le requérant a qualité pour agir en nullité, la chambre de l'instruction doit rechercher si la formalité substantielle ou prescrite à peine de nullité, dont la méconnaissance est alléguée, a pour objet de préserver un droit ou un intérêt qui lui est propre.

L'existence d'un grief est établie lorsque l'irrégularité elle-même a occasionné un préjudice au requérant, lequel ne peut résulter de la seule mise en cause de celui-ci par l'acte critiqué ».

Nullité d'ordre public ou d'ordre privé ?

La chambre criminelle a estimé dans un premier temps que les dispositions de l'article 77-1-1 prévoyant l'autorisation du procureur de la République en vue des réquisitions de données informatiques étaient édictées dans l'intérêt d'une bonne administration de la justice [46]. Mais dans le dernier état de sa jurisprudence, elle exclut que l'on soit en présence d'une nullité d'ordre public [47].

S'agissant des dispositions du droit de l'Union européenne dont la violation est invoquée, la CJUE énonce elle même que « *la directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données* ». Elle considère que les données relatives au trafic et les données de localisation peuvent non seulement révéler des informations sensibles concernant la vie privée des personnes concernées, mais permettre de tirer des conclusions précises concernant leurs

[45] Crim. 7 septembre 2021, n° 21-80.642 et 20-97.191

[46] Crim. 1 septembre 2005, n° 05-84.061, Bull. n° 211

[47] Crim. 6 février 2018, n° 17-84.380, Bull. n° 30

habitudes, leurs déplacements, leurs relations et fournir, en particulier, les moyens d'établir le profil de ces personnes.

Il en résulte que les exigences européennes en matière de conservation des données de connexion et d'accès à ces données sont manifestement d'ordre privé et non d'ordre public comme le demandeur l'a affirmé devant la chambre de l'instruction.

Qualité à agir du demandeur

La chambre de l'instruction ne s'est pas prononcée sur qualité à agir du demandeur, étant rappelé que dans sa requête en nullité, l'intéressé sollicitait indistinctement l'annulation de « *l'ensemble des réquisitions portant sur les données à caractère personnel conservées par les opérateurs de communications électroniques, particulièrement celles ayant concerné M. [K]* ».

Pour apprécier si le requérant est concerné par l'irrégularité qu'il invoque, la chambre criminelle tient compte des finalités poursuivies par la formalité violée [48]. Ce n'est que si la formalité a pour objet d'authentifier les éléments de preuve, que sa méconnaissance peut être invoquée par toute partie [49].

En l'espèce, M. [R] [K] ne justifie d'aucun intérêt propre à invoquer la nullité de toutes les réquisitions délivrées aux opérateurs téléphoniques par les officiers de police judiciaire, agissant en enquête préliminaire puis sur commission rogatoire et tendant à obtenir les facturations détaillées et géolocalisées de lignes téléphoniques, y compris celles dont il n'est ni le titulaire ni l'utilisateur. Il n'établit pas non plus en quoi il a été porté atteinte à sa vie privée à l'occasion de telles investigations.

Il faut en conclure que l'intéressé n'est recevable à invoquer l'éventuelle violation du droit de l'Union européenne, en matière de conservation des données de connexion et d'accès à ces données, qu'en ce qui concerne la ligne téléphonique dont il était l'utilisateur.

Existence d'un grief

[48] Outre les arrêts précités du 7 septembre 2021, voir Crim., 21 février 2017, n° 16-85.542 : « Le demandeur, qui ne se prévaut d'aucun droit sur les véhicules géolocalisés ni sur le parking souterrain d'immeuble dans lequel l'un des dispositifs de géolocalisation a été posé, est irrecevable à invoquer une irrégularité affectant cette mesure, dès lors qu'il n'établit pas qu'à cette occasion il aurait été porté atteinte à un autre intérêt qui lui serait propre ».

[49] Voir Crim. 9 novembre 2021, n° 21-83.095, à propos de la pesée de produits stupéfiants

Ce grief paraît devoir être analysé au seul regard du principe du procès équitable en se référant aux exigences posées par la CJUE s'agissant de l'admissibilité des éléments de preuve fournis par l'exploitation des données de connexion dans des conditions contraires au droit de l'Union.

La CJUE estime que les États membres n'ont pas nécessairement à écarter les preuves collectées de manière contraire au droit de l'Union, dès lors que les personnes soupçonnées sont en mesure de les « *commenter efficacement* ». La notion de « *commentaire efficace* » suggère que la Cour entend subordonner l'admissibilité et l'exploitation des données de connexion à la possibilité pour la personne poursuivie de les discuter de manière contradictoire.

Dans le présent dossier, on peut douter que le dépôt d'une requête en nullité soit le moyen le plus efficient de contester les éléments de preuve ainsi recueillis, comme l'affirme la chambre de l'instruction.

Il suffit de constater qu'en tout état de cause M. [K] est en mesure de prendre position utilement sur les éléments issus de la téléphonie, voire de solliciter des actes, notamment une expertise technique sur la validité des conclusions tirées par les enquêteurs de l'exploitation des données de connexion.

<u>Inopposabilité des données de connexion</u>

Rappelons que pour la CJUE, les données collectées doivent exercer une influence prépondérante sur l'appréciation des faits, ce qui revient à dire qu'une décision de condamnation ne pourrait se fonder ni exclusivement, ni même essentiellement sur des éléments recueillis dans des conditions irrégulières.

La réponse à la question de savoir si les données recueillies ont exercé ou non une influence prépondérante sur l'issue de la procédure paraît cependant devoir être réservée à la juridiction de jugement, si elle est ultérieurement saisie.

Plus généralement, il n'est pas certain que la nullité des actes irréguliers soit en l'état la seule sanction envisageable. On peut se demander en effet si les exigences de sécurité juridique et de prévisibilité des règles de procédure ne doivent pas conduire à moduler dans le temps la nature de la sanction de la violation du droit européen.

La CJUE semble exclure, a priori, une telle faculté, en décidant « *qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article*

15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte » [50].

Mais il ne s'agit pas ici de refuser de tirer les conséquences d'une méconnaissance des exigences européennes mais d'adapter dans le temps la nature de la sanction qui doit y être apportée.

Saisie de moyens invoquant l'irrégularité d'auditions en garde à vue, sans l'assistance d'un avocat et sans notification du droit de se taire, pratiquées à une date bien antérieure aux arrêts Salduz c/ Turquie et Dayanan c/ Turquie, rendus les 27 novembre 2008 et 13 octobre 2009 par la Cour européenne des droits de l'homme, la chambre criminelle a jugé en 2018 « *qu'en l'absence, à la date des mesures critiquées, de jurisprudence établie ayant déduit de l'article 6, § 1 de la Convention européenne des droits de l'homme le droit pour la personne gardée à vue d'être assistée par un avocat lors de ses auditions et l'obligation de lui notifier le droit de garder le silence, l'exigence de prévisibilité de la loi et l'objectif de bonne administration de la justice* [faisait] *obstacle à ce que les auditions réalisées à cette date, sans que la personne gardée à vue ait été assistée d'un avocat pendant leur déroulement ou sans qu'elle se soit vue notifier le droit de se taire, soient annulées pour ces motifs* ». Elle a précisé toutefois que « *les déclarations incriminantes faites lors de ces auditions ne* [pouvaient]*, sans que soit portée une atteinte irrémédiable aux droits de la défense, fonder une décision de renvoi devant la juridiction de jugement ou une déclaration de culpabilité* » [51].

En l'espèce c'est antérieurement à l'arrêt Quadrature du Net que les enquêteurs ont eu accès aux données de connexion récentes concernant M. [K].

On peut considérer qu'à la date des opérations litigieuses, la jurisprudence de la CJUE sur la conservation et l'accès aux donnéeMs de connexion dans le cadre de la lutte contre la criminalité grave n'était pas encore consolidée, étant observé que demeuraient de nombreuses incertitudes sur l'interprétation de cette jurisprudence, ce qui explique d'ailleurs que plusieurs Etats membres aient saisi la Cour de questions préjudicielles.

Une telle solution reviendrait alors à écarter à titre transitoire les informations obtenues dans des conditions irrégulières au regard des engagements conventionnels.

il est proposé en définitive de rejeter le pourvoi.

Proposition

Avis de REJET.

---

[50] § 228 de l'arrêt Quadrature du Net.

[51] Crim. 11 décembre 2018, n° 18-82.854, Bull. n° 209