REVUE JURIDIQUE DE LA SORBONNE

SORBONNE LAW REVIEW

Décembre 2022 - N° 6

IRJS Editions

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Revue Juridique de la Sorbonne – *Sorbonne Law Review*

Revue semestrielle (2 numéros/an ; juin et décembre)
Revue gratuite, en open access
Disponible sur : https://irjs.pantheonsorbonne.fr/revue-juridique-sorbonne
Langues de publication : français, anglais.

IRJS éditions – Université Paris 1 Panthéon-Sorbonne
12 place du Panthéon
75005 PARIS (France)
@ : irjs-editions@univ-paris1.fr / Tel : 01 44 07 78 21I
SSN : 2739-6649
Dépôt légal : décembre 2022, mise en ligne janvier 2023.

TABLE DES MATIÈRES

4. Conservation généralisée et indifférenciée des données de connexion : pas d'infléchissement de la jurisprudence de la Cour de Justice en matière d'abus de marché

CJUE, Gde ch., 20 septembre 2022, *VD et SR*, aff. jointes C-339/20 et C-397/20

Commentaire rédigé par les étudiants du Master 2 Droit des affaires de l'École de Droit de la Sorbonne[1]
Sous la direction du professeur Anne-Claire Rouaud

L'Union européenne a fait de la protection du droit au respect de la vie privée et des données à caractère personnel un de ses fers de lance. À ce titre, plusieurs textes sont venus renforcer la protection de ces droits fondamentaux, tout particulièrement la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite *e-Privacy*. Par l'arrêt *VD et SR* du 20 septembre 2022[2], la Cour de justice de l'Union européenne (CJUE) s'inscrit dans la continuité de sa jurisprudence antérieure, notamment des arrêts *Digital Rights*[3], *Tele 2 Sverige*[4] et *La Quadrature du Net*[5], mais se prononce pour la première fois sur la conservation généralisée et indifférenciée, à titre préventif, de données de trafic en matière de lutte contre les abus de marché.

Deux personnes étaient poursuivies pénalement notamment pour des délits d'initiés et de blanchiment. Les deux prévenus ont contesté la transmission, à l'occasion de ces poursuites, de données relatives au trafic afférentes à des appels téléphoniques, par l'Autorité des marchés financiers (AMF) à l'autorité judiciaire. Ils faisaient valoir que les dispositions nationales concernant la conservation des

1 Bienheureux Abelam Edanga-Mette ; Marc Alexandrov ; Charlotte Allegre ; Ketibe Ayadi ; Alia Azizi ; Amel Belaid ; Yanis Benyahia ; Arthur Bernhard ; Brunet Blaise ; Edouard Bonnin ; Zoe Bordas ; Eloïse Boutan ; Julia Brusson ; Defne Caglar ; Ibrahim Camara ; Emine Celik ; Laura Da Costa ; Clothilde François De Valence ; Cyril Frestel ; Noémie Gondy ; Victor Goudallier ; Eléonore Grandjean ; Esther Grégoire ; Chloé Gruaz ; Clémence Hoerner ; Noémie Jacquot ; Margot Lescuras ; Solène Marquier ; Hasnia Moulessehoul ; Camilia Ounnar ; Laura Perigaud ; Mathilde Piraux ; Clara Pradel ; Isabelle Puren ; Victoire Roussel ; Mathis Sougy ; Alexandra Soulhiol Chabrier ; Shannon Stioui ; Yara Torbey ; Sacha Vidal ; Lucas Vincent.

2 CJUE, Gde ch., 20 sept. 2022, *VD et SR*, aff. jointes C-339/20 et C-397/20 ; *Banque & droit* n° 206, nov.- déc. 2022, p. 60, note A.-C. Rouaud.

3 CJUE, Gde ch., 8 avril 2014, *Digital Rights Ireland Ltd*, C-293/12 et C-594/12

4 CJUE, Gde ch., 21 décembre 2016, *Tele 2 Sverige AB*, C-203/18 et C-698/15

5 CJUE, Gde ch., 6 octobre 2020, *La Quadrature du Net e.a.*, aff. jointes C511/18, C512/18 et C520/18 ; *D.* 2021, p. 406, note M. Lassalle *; ibid.* 2020, p. 2262, obs. J. Larrieu, C. Le Stanc et P. Tréfigny *; D.* 2022, p. 2002, note W. Maxwell et C. Zolynski *; BJB* janv. 2021, n° 119p3, p. 16, note M. Galland.

données et l'accès à ces données par l'AMF, ne seraient pas conformes au droit de l'Union européenne.

Leurs recours ont été rejetés par deux arrêts de la cour d'appel de Paris en date du 20 décembre 2018 et du 7 mars 2019, laquelle retient qu'il existait des motifs de suspicion d'opérations d'initiés, pour lesquelles les données concernées étaient essentielles à l'enquête. Les personnes poursuivies décident alors de se pourvoir en cassation. Selon les moyens du pourvoi, le droit français serait contraire au droit de l'Union européenne à la fois en ce qu'il prévoit, à l'article L. 34-1 du Code des postes et communications électroniques dans sa rédaction alors applicable, la conservation généralisée et indifférenciée des données de connexion aux fins de lutte contre la criminalité et en ce qu'il n'entoure pas de suffisamment de garanties le pouvoir de l'AMF, prévu par les anciennes dispositions de l'article L. 621-10 du Code monétaire et financier, d'accéder à ces données.

Trois questions préjudicielles sont posées à la Cour de Justice de l'Union européenne par la chambre criminelle de la Cour de cassation[6]. D'une part, elle est interrogée sur le point de savoir si les dispositions des textes européens en matière d'abus de marché « *n'impliquent* [...] *pas, compte tenu du caractère occulte des informations échangées et de la généralité du public susceptible d'être mis en cause, la possibilité, pour le législateur national, d'imposer aux opérateurs de communications électroniques une conservation temporaire mais généralisée des données de connexion* », pour permettre à l'autorité administrative compétente d'obtenir des preuves antérieures aux soupçons visant certaines personnes. D'autre part, les deux autres questions portent sur la possibilité de maintenir provisoirement les effets d'une législation contraire au droit de l'Union.

La directive *e-Privacy*, tout en posant le principe d'effacement ou d'anonymisation des données de connexion, autorise les États membres à imposer, par exception, une obligation de conservation dans certains cas. Dans l'arrêt *La Quadrature du Net* rendu le 6 octobre 2020, la Cour de justice de l'Union européenne s'est prononcée sur la portée de ces dispositions et sur les modalités encadrant l'obligation faite aux fournisseurs de services de communication de conserver, de manière généralisée et indifférenciée, des données relatives au trafic et à la localisation sur le fondement d'une mesure nationale d'un État membre. Dans le cadre de son contrôle de proportionnalité entre la protection de la vie privée et la préservation de la sécurité nationale, la Cour accorde, au regard de l'article 15 de la directive *e-Privacy*, une importance de principe à la protection de la vie privée et à l'interdiction de la conservation de données de trafic et de localisation, du fait des informations précises susceptibles d'être déduites relativement à la vie privée des utilisateurs à partir de ces données (lesquelles incluent notamment l'identification du destinataire de la communication, la date et la durée de la correspondance). Toutefois, elle dégage

6 Cass. crim. 1er avril 2020, n°19-82.223 ; *Banque & Droit* n° 193 sept.-oct. 2020, p. 44, note A.-C. Rouaud *; BJB* Mai 2020, p. 21 note A. Pietrancosta.

trois niveaux de gravité qui auront une influence sur le régime de conservation des données, posant ainsi une série d'exceptions à ce principe. En haut de la hiérarchie se trouve la protection de la sécurité nationale, avec en particulier la lutte contre le terrorisme, qui permet une conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation à condition d'être limitée dans le temps et soumise au contrôle d'une autorité judiciaire. Puis, vient la lutte contre la criminalité grave ; à cette fin, la conservation ne peut être que ciblée, en fonction de catégories de personnes ou de critères géographiques, ou prendre la forme d'une injonction de conservation rapide justifiée par un lien avec un crime grave et restant limitée au « strict nécessaire ». Enfin, les autres formes de criminalité ne sauraient justifier la conservation de telles données, à l'exception de celles relatives à l'identité civile des utilisateurs.

L'arrêt commenté ne peut être parfaitement compris qu'à la lumière de l'interprétation faite par l'Assemblée du Conseil d'État, dans son arrêt du 21 avril 2021[7], de la jurisprudence de la Cour de Justice de l'Union européenne. Dans cet arrêt, la Haute Juridiction administrative reçoit en droit interne la réponse apportée par la Cour de Justice de l'Union européenne dans l'arrêt *La Quadrature du net*[8] à des questions préjudicielles. Elle valide pour l'essentiel, au terme d'une interprétation audacieuse du droit de l'Union européenne, les dispositions de l'article R.10-13 du Code des postes et des communications électroniques dans sa rédaction alors applicable. Le Conseil d'État justifie sa décision par la protection effective de la sécurité nationale, principe de valeur constitutionnelle fondant une réserve de constitutionnalité. Si l'arrêt enjoint au Premier ministre d'abroger certaines dispositions faute de garanties suffisantes pour préserver les droits et libertés fondamentaux, il accepte cependant que les autorités utilisent, aux fins de lutter contre la criminalité grave et grâce à la conservation rapide, les données conservées de façon généralisée et indifférenciée aux fins de sauvegarde de la sécurité nationale. En effet, la conservation rapide des données n'aurait pas, à elle seule, d'intérêt pour la recherche des infractions passées, mais seulement une utilité pour la prévention d'infractions à venir.

Pour aboutir à cette conclusion, le Conseil d'État « *s'engouffre dans une brèche ouverte dans la jurisprudence Tele 2 par l'arrêt Quadrature du Net* »[9] en affirmant qu'« *aussi longtemps que l'existence d'une menace grave sur la sécurité nationale justifie la conservation généralisée et indifférenciée des données de connexion, l'application du droit de l'Union européenne, en conduisant à écarter le droit national, ne prive pas de garanties effectives les objectifs de valeur constitutionnelle invoqués par le Premier ministre en défense*[10] ». Pour certains auteurs, le Conseil d'État « *réduit*

7 Conseil d'État, Assemblée, 21 avr. 2021, n°393099 ; F.-X. Bréchot, « De l'art de concilier l'inconciliable », *RTD eur*. 2021. 637 ; L. Azoulai, D. Ritleng, « « L'État, c'est moi ». Le Conseil d'État, la sécurité et la conservation des données », *RTD Eur*. 2021 p. 349 ; *BJB* juill. 2021, p. 14, note M. Galland ; *JCP G* 14 Juin 2021, 659, note A. Iliopoulou-Penot.

8 CJUE, Gde ch., 6 octobre 2020, préc.

9 F.-X. Bréchot, « De l'art de concilier l'inconciliable », préc.

10 Conseil d'État, 21 avr. 2021, préc., pt 58.

considérablement les termes de l'équation posée par la Cour de justice » en posant une exigence « *largement insuffisante* » du point de vue des droits protégés par le droit de l'Union[11]. La décision commentée semble permettre, dans une certaine mesure, de confirmer les critiques en ce sens.

En effet, dans l'arrêt *VD et SR* du 20 septembre 2022, la Cour considère que ni la Directive Abus de marché du 28 janvier 2003[12], ni le règlement Abus de marché du 16 avril 2014[13] « *ne sauraient être interprétés comme pouvant constituer le fondement juridique d'une obligation générale de conservation des enregistrements de données relatives au trafic détenus par les opérateurs de services de communications électroniques aux fins de l'exercice des pouvoirs conférés à l'autorité compétente en matière financière au titre de la directive 2003/6 et du règlement n° 596/2014* ». Elle ajoute que « *la directive 2002/58 constitue l'acte de référence en matière de conservation et, de manière plus générale, de traitement des données à caractère personnel dans le secteur des communications électroniques* ». Ce faisant, la Cour opère une lecture du droit de l'Union opposée à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, à moins d'être en présence d'un cas de menace grave pour la sécurité nationale. Néanmoins, et à condition de respecter les principes d'équivalence et d'effectivité, il revient au droit national de chaque État membre de trancher sur l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation.

Bien que les dispositions litigieuses ne soient plus en vigueur – elles ont, en effet, été réécrites, qu'il s'agisse de celles du Code monétaire et financier, à la suite de leur invalidation par le Conseil constitutionnel[14], ou de celles du Code des postes et communications électroniques, à la suite de l'arrêt *La Quadrature du Net* de la CJUE et de l'arrêt *French Data Network* du Conseil d'État[15] – et que la directive *e-Privacy* soit en cours de révision, l'arrêt *VD et SR* présente un intérêt certain en ce qu'il vient confirmer la jurisprudence de la Cour en la matière tout en en faisant application, pour la première fois, en matière d'abus de marché.

Dans un premier temps, la Cour écarte la directive et le règlement Abus de marché comme fondant juridiquement une obligation générale de conservation des données de trafic détenues par les opérateurs de services de communications électroniques aux fins de la lutte contre les infractions d'abus de marché (I). Dans un second temps, elle exclut la possibilité de maintenir provisoirement une législation contraire au droit de l'UE, tout en rappelant qu'il appartient au droit national de

11 L. Azoulai, D. Ritleng, préc.
12 Dir. 2003/6/CE 28 Janvier 2003 sur les opérations d'initiés et les manipulations de marché (abus de marché).
13 Règl. 596/2014 du Parlement européen et du Conseil du 16 avril 12014 sur les abus de marché.
14 Cons. Constit., 21 Juillet 2017, n°2017-646/647 QPC, M. Alexis K et autre ; *Revue des sociétés* 2017, p. 582 note N. Martial-Braz ; Loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude.
15 Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

chaque État membre de déterminer l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation (II).

I.- L'incompatibilité du droit français avec le droit de l'Union européenne

La Cour de justice de l'Union européenne répond à la première question préjudicielle qui lui est posée par la Cour de cassation en examinant les dispositions de droit de l'Union relatives aux abus de marché (A). Constatant que celles-ci n'habilitent pas le législateur national à instituer une obligation de conservation généralisée et indifférenciée des données, la Cour se réfère à la directive *e-Privacy* et à sa jurisprudence constante en la matière (B).

A.- Les textes en matière d'abus de marché et leur interprétation par la CJUE

Saisie de la question de la compatibilité avec le droit de l'Union de la loi nationale prévoyant un régime de conservation généralisée et indifférenciée des données pour lutter contre les abus de marché, la Cour de justice se penche sur les textes communautaires en la matière. La question préjudicielle dont elle était saisie visait plus précisément « *L'article 12, paragraphe 2, sous a) et d), de la directive 2003/6 et l'article 23, paragraphe 2, sous g) et h), du règlement n° 596/2014*[16] ». La CJUE se livre donc à une interprétation de ces textes, afin de savoir s'ils permettent une telle conservation des données.

Le règlement Abus de marché du 16 avril 2014[17] renforce le dispositif en matière de lutte contre les abus de marché découlant de la directive sur les opérations d'initiés et les manipulations de marché du 28 janvier 2003[18]. C'est l'article 23 de ce règlement qui détaille les pouvoirs des autorités nationales dans la recherche des infractions d'abus de marché. Ce texte, à l'instar de l'article 12 de la directive 2003/6, exige que celles-ci puissent se faire remettre non seulement les enregistrements des conversations téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic détenus par des entreprises d'investissement, des établissements de crédit ou des institutions financières (art. 23 (1) sous g), mais aussi, « *dans la mesure où le droit national l'autorise, les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications, lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler pertinents pour l'enquête* » (art. 23 (1) sous h).

En l'espèce, deux interprétations de ces articles se confrontaient. Selon certains gouvernements, dont le gouvernement français, ces dispositions habilitent implicitement le législateur national à instituer une obligation de conservation généralisée

16 Décision commentée, pt 65.
17 Règlement (UE) n° 596/2014, préc.
18 Directive 2003/6/CE, préc.

et indifférenciée des données, tandis que selon les requérants ces dispositions ne régissent que la question de l'accès aux données[19].

Il revenait donc à la CJUE de décider quelle est la bonne interprétation. Pour cela, la Cour se réfère aux termes de ces dispositions, à leur contexte, ainsi qu'aux objectifs poursuivis. Sur le premier critère, la juridiction européenne affirme qu'« *il ressort sans ambiguïté du libellé de ces dispositions que celles-ci se bornent à encadrer le pouvoir de ladite autorité d'*« *exiger* », *ou encore, de* « *se faire remettre* » *les données dont disposent ces opérateurs, ce qui correspond à un accès à ces données. En outre, la référence faite aux enregistrements* « *existants* », *tels que* « *détenus* » *par lesdits opérateurs, laisse entendre que le législateur de l'Union n'a pas entendu régir la possibilité, pour le législateur national, d'instaurer une obligation de conservation de tels enregistrements* »[20]. Sur le deuxième critère, relatif au contexte, la Cour arrive à la même conclusion. Le souhait du législateur européen n'était pas d'instituer une telle obligation de conservation à la charge des opérateurs de communications électroniques, mais simplement de doter les autorités compétentes de certains pouvoirs leur permettant de réaliser efficacement leurs missions d'enquête et de surveillance. Enfin, sur le troisième critère, tenant aux objectifs poursuivis, la Cour relève que la finalité de la réglementation relative aux abus de marché est d'assurer l'intégrité des marchés financiers de l'Union européenne et la confiance dans ces marchés, ce qui passe par la répression des abus de marché. Sur ce point, un doute était permis au regard du considérant 65 du règlement n° 596/2014, qui rappelle que les enregistrements des données sont parfois l'unique preuve permettant de détecter des opérations d'initié. En effet, ces opérations sont essentiellement secrètes, ce qui pose des difficultés probatoires.

Toutefois, la CJUE maintient son interprétation et affirme que « *ni la directive 2003/6 ni le règlement n° 596/2014 ne sauraient être interprétés comme pouvant constituer le fondement juridique d'une obligation générale de conservation des enregistrements de données relatives au trafic détenus par les opérateurs de services de communications électroniques aux fins de l'exercice des pouvoirs conférés à l'autorité compétente en matière financière au titre de la directive 2003/6 et du règlement n° 596/2014* »[21]. Ces textes ne régissent donc que la question de l'accès aux données par les autorités compétentes.

La conservation des données relève d'un autre texte communautaire, à savoir la directive *e-Privacy* du 12 juillet 2002.

19 Décision commentée, pts 66 et 67.
20 Décision commentée, pt 70.
21 Décision commentée, pt 78.

B.- L'application en matière d'abus de marché de la jurisprudence européenne interprétant la directive e-Privacy

La directive *e-Privacy* constitue selon les termes de la Cour « *l'acte de référence en matière de conservation des données* » au niveau européen[22]. C'est donc naturellement sur cette directive que se fonde la Cour dans l'arrêt *VD et SR*, pour juger non conforme le droit français de la conservation des données en matière d'abus de marché. Si cette inconventionnalité du droit français était prévisible (1), une question reste en suspens car la juridiction européenne ne se prononce pas sur le seuil de gravité des abus de marché (2).

1.- Une jurisprudence européenne constante en matière de conservation généralisée

La première question préjudicielle posée à la Cour de justice par la Cour de cassation[23] portait sur le point de savoir si le législateur national pouvait imposer, aux fins de la lutte contre les infractions d'abus de marché, une conservation temporaire mais généralisée et indifférenciée des données de trafic, et permettre à l'autorité chargée de la lutte contre les abus de marché de se faire remettre de telles données. De manière prévisible, la Cour estime « *qu'une réglementation nationale, telle que celle en cause au principal, imposant aux opérateurs de services de communications électroniques de procéder, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés, une conservation généralisée et indifférenciée des données de trafic de l'ensemble des utilisateurs des moyens de communications électroniques, sans qu'aucune différenciation soit faite à cet égard ou que des exceptions soient prévues et sans que les rapports requis, au titre de la jurisprudence mentionnée au point précédent, entre les données à conserver et l'objectif poursuivi, soit établi, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige 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*[24] ». C'est une fois de plus le droit des États à instaurer une conservation généralisée et indifférenciée des données qui est refusé par la juridiction européenne.

Cette décision n'est pas surprenante, elle s'inscrit pleinement dans la jurisprudence constante de la CJUE et ses arrêts *Digital Rights* de 2014[25], *Tele 2 Sverige* de 2016[26] et *La Quadrature du net* de 2020[27]. En effet, dès 2014, la Cour de justice de l'Union européenne invalidait la directive 2006/24/CE sur la conservation des données. En posant une obligation de conservation généralisée et indifférenciée

22 Décision commentée, pt 79.
23 Cass. crim., 1er avril 2020, préc.
24 Décision commentée, pt 94.
25 CJUE, gde ch., 8 avril 2014, préc.
26 CJUE, gde ch., 21 décembre 2016, préc.
27 CJUE, gde ch., 6 octobre 2020, préc.

des données de connexion, cette directive comportait une ingérence dans les droits fondamentaux disproportionnée et non limitée au strict nécessaire.

Une relative souplesse a été apportée avec l'arrêt *La Quadrature du Net* de 2020, où la Cour a hiérarchisé les possibilités de conserver les données en fonction des objectifs des États, admettant ainsi une conservation généralisée et indifférenciée, quoique temporaire, des données relatives au trafic en cas de menace pour la sécurité nationale. À défaut, la lutte contre la criminalité grave permettrait une conservation généralisée des adresses IP, considérée comme peu intrusive, ainsi qu'une conservation ciblée des données relatives au trafic délimitée en fonction de catégories de personnes concernées ou au moyen d'un critère géographique ou encore une injonction de conservation rapide, pour une durée déterminée, des données relatives au trafic et des données de localisation. Enfin, la lutte contre la criminalité non grave autoriserait quant à elle seulement la conservation généralisée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques. Cette hiérarchie reflète l'importance accordée par la juridiction européenne au droit au respect de la vie privée, face à des États membres cherchant à contourner les principes de la directive *e-Privacy* pour satisfaire aux impératifs de sécurité et de répression pénale.

Outre la réaffirmation de l'interdiction d'une conservation généralisée des données aux fins de lutte contre la criminalité, également présente dans une autre décision rendue le même jour[28], l'arrêt *VD et SR* est intéressant car il en fait application aux abus de marché. Contrairement aux précédents arrêts de la CJUE qui portaient sur la matière criminelle « classique », la décision commentée porte en effet sur une enquête de l'Autorité des marchés financiers et la poursuite de deux personnes physiques pour des faits de délits d'initiés, recel de délits d'initiés, complicité, corruption et blanchiment.

La question de la qualification du niveau de criminalité se posait donc logiquement concernant les abus de marché. Or, sur ce point, l'arrêt *VD et SR* n'apporte pas de réponse.

2.- Une question en suspens : le seuil de gravité des abus de marché

Puisque la conservation généralisée et indifférenciée des données n'est pas admise à cette fin, cela signifie que les abus de marché n'entrent pas dans la catégorie des menaces graves pour la sécurité nationale. Cela se comprend, car dans son arrêt *La Quadrature du net*, la Cour de justice qualifiait celles-ci « *d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités*

28 CJUE, gde ch., 20 sept. 2022, aff. jointes C793/19 et C794/19, *Bundesrepublik Deutschland c/ SpaceNet AG et Telekom Deutschland GmbH.*

de terrorisme[29] ». C'est dire qu'il s'agit d'activités d'une particulière gravité. Certes, les abus de marché sont répréhensibles, mais « *cela ne signifie* [...] *pas que de tels comportements constituent une menace pour la sécurité nationale, au sens de l'arrêt La Quadrature du Net* », comme le souligne l'avocat général dans ses conclusions dans l'affaire *VD et SR*[30].

Si les abus de marché sont exclus de la catégorie des menaces graves pour la sécurité nationale, cela signifie qu'ils relèvent soit de la criminalité grave, soit de la criminalité ordinaire. Dans le premier cas, cela laisserait la possibilité aux États de prévoir une conservation ciblée et/ou rapide des données relatives au trafic, ainsi qu'une conservation généralisée et indifférenciée des adresses IP. Dans le second cas, seule la conservation des données relatives à l'identité civile des utilisateurs serait admise, selon la jurisprudence de la Cour de Justice.

Or, l'arrêt *La Quadrature du Net* ne renseigne pas sur le seuil de gravité des infractions d'abus de marché[31], pas plus que le présent arrêt. De plus, on constate une absence de définition autonome de la criminalité grave ou faible en droit de l'Union.

Certaines pistes avaient été envisagées par le rapporteur public dans ses conclusions dans l'affaire *FrenchDataNetwork* devant le Conseil d'État[32], notamment celle de fixer un seuil de peine encourue à partir duquel on pourrait considérer qu'il s'agit de criminalité grave. Mais, comme le souligne le rapporteur, le quantum de la peine encourue n'est pas toujours révélateur de la gravité des agissements en cause. Il faudrait se référer également aux « *circonstances de chaque infraction* » et à « *l'ampleur des préjudices subis par la société et par la victime*[33] ». De plus, force est de constater qu'en matière d'abus de marché les peines d'emprisonnement prévues (cinq ans maximum[34]) ne sont jamais prononcées. Le législateur français a également étendu aux abus de marché la voie de la composition administrative[35], ouvrant ainsi la possibilité pour l'Autorité des marchés financiers de proposer une sanction négociée aux auteurs de manquements.

Est-ce à dire que les abus de marché relèvent de la criminalité ordinaire ? Il faudrait que la Cour tranche cette question de qualification dans ses arrêts ultérieurs, et ce d'autant plus que les juridictions nationales ont pris quelques libertés en matière de conservation des données.

29 CJUE, gde ch., 6 octobre 2020, préc., pt 135.
30 Conclusions de l'Avocat général Manuel Campos Sanchez-Bordona dans l'arrêt *VD et SR*, pt 84.
31 BJB janv. 2021, note M. Galland, préc., spéc. II. B. 1.
32 Conseil d'État, 21 avril 2021, préc.
33 Conclusions du rapporteur public dans l'affaire *FrenchDataNetwork*, pt 6.2.
34 Art. L. 465-1, c. mon. fin.
35 Loi n° 2016-819 du 21 juin 2016 réformant le système de répression des abus de marché ; art. L. 621-14-1, c. mon. fin.

En effet, le Conseil d'État s'est relativement écarté de la jurisprudence européenne, soulignant l'intérêt opérationnel incertain de la conservation ciblée[36]. S'appuyant sur le point 164 de l'arrêt *La Quadrature du Net*, dans lequel la Cour envisage l'hypothèse dans laquelle « *la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement* », pour préciser que « *les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu* », et en se gardant bien de citer le point 166 du même arrêt, dans lequel la Cour précise qu'il n'est pas licite d'accéder à des données pour un objectif inférieur à celui pour lequel elles ont été conservées, la Haute juridiction administrative admet que les autorités utilisent, aux fins de lutter contre la criminalité grave et grâce à la conservation rapide, les données conservées de façon généralisée et indifférenciée aux fins de sauvegarde de la sécurité nationale. Dès lors, il serait possible, pour lutter contre la criminalité grave, d'utiliser, via une injonction de conservation rapide, des données initialement conservées pour la protection de la sécurité nationale. C'est d'ailleurs ce que prévoient les dispositions de l'article L. 34-1 du CPCE dans leur rédaction issue de la loi du 30 juillet 2021 : « *Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données*[37] ». L'accès aux données conservées pour la protection de la sécurité nationale serait donc autorisé pour satisfaire à un objectif plus faible de lutte contre la criminalité grave.

Il en va de même pour la chambre criminelle de la Cour de cassation, qui en 2022 a considéré que « *La conservation rapide peut donc porter sur les données que détiennent les opérateurs de télécommunications électroniques* [...] *au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale*[38] ».

Ces solutions entrent en contradiction avec la jurisprudence de la CJUE, y compris la plus récente, selon laquelle il est impossible d'utiliser des données conservées pour la protection de la sécurité nationale aux fins de lutte contre la criminalité grave[39]. On peut dès lors se demander comment se résoudra ce conflit.

Pour le moment, la CJUE maintient sa position, et cette constance se retrouve d'ailleurs dans les conséquences attachées aux arrêts rendus par la Cour, notamment dans le refus de différer l'effet d'éviction des dispositions nationales non conformes.

36 Conseil d'État, 21 avril 2021, *FrenchDataNetwork*, n°393099, préc., pts 54 à 57.
37 L. n° 2021-998 du 30 juill. 2021 relative à la prévention d'actes de terrorisme et au renseignement.
38 Cass. crim., 12 juillet 2022, n° 21-83.710, pt 18 ; M. Bendavid, C.Quendolo, « Conservation et accès aux données de connexion : la Cour de cassation prend position », *AJ pénal* 2022. 415 ; *JCP G* 2022. 1123, note O. Cahn.
39 CJUE, gde ch., 5 avril 2022, préc., pt 98.

II.- Les effets limités de la déclaration d'invalidité sur les mesures prises en violation du droit communautaire

Dans cet arrêt, la Cour réaffirme le principe de sa compétence exclusive pour refuser la modulation dans le temps des effets de la déclaration d'invalidité (A) tout en maintenant l'autonomie procédurale des États membres en matière de recevabilité des preuves (B).

A.- La réaffirmation du principe de la compétence exclusive de la Cour pour procéder à la modulation dans le temps des effets d'une déclaration d'invalidité

L'arrêt commenté rappelle que la Cour est en principe seule compétente pour procéder à la modulation dans le temps des effets d'une déclaration d'invalidité.

Dans un premier temps, l'arrêt rappelle que la compétence de la CJUE est fondée sur le principe de primauté et d'uniformité d'application du droit de l'Union européenne. En effet, le droit de l'Union européenne est prééminent sur le droit des États membres. Par conséquent, si le juge national ne peut interpréter la législation nationale de façon conforme aux exigences du droit de l'Union, il a pour obligation « *d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure*[40] ». À ce titre, l'arrêt du 5 avril 2022, *Commissioner of An Garda Síochána*[41] a précisé que cette obligation tend à s'appliquer « *sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel*[42] ».

Dans un second temps, la compétence de la Cour est également fondée sur des considérations impérieuses de sécurité juridique. Ce principe signifie que seule la Cour peut accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci[43]. L'encadrement strict de ce principe est rappelé dans la décision commentée : la suspension provisoire ne peut être accordée (i) qu'à titre exceptionnel, (ii) pour des considérations impérieuses de sécurité juridique et (iii) dans l'arrêt même qui statue sur l'interprétation sollicitée.

Ainsi, la compétence exclusive de la Cour se justifie par la volonté de préserver la sécurité juridique, mais également par le fait qu'il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si les juridictions nationales avaient le pouvoir de donner la primauté, même à titre provisoire, à leurs dispositions nationales par rapport au droit de l'Union.

40 Décision commentée, pt 97.
41 CJUE 5 avril 2022, préc.
42 CJUE 5 avril 2022, préc., pt 118.
43 Décision commentée, pt 98.

Certes, la Cour a déjà offert au juge national un pouvoir circonstancié de modulation des effets dans le temps d'une déclaration d'invalidité depuis un arrêt *Inter-Environnement Wallonie ASBL* de 2012[44]. Toutefois, cette faculté reste exceptionnelle et strictement encadrée. Ainsi, dans cette dernière décision, cette modulation se justifiait par les circonstances particulières de l'espèce puisqu'il s'agissait (i) d'une simple omission d'une obligation procédurale qui (ii) s'inscrivait dans le domaine spécifique de la protection de l'environnement et (iii) était susceptible d'être régularisée.

Pour en revenir à l'arrêt *VD et SR*, le refus par la Cour de justice d'admettre un tel pouvoir de modulation était donc attendu, d'autant plus qu'une telle faculté n'a jamais été admise en matière de conservation des données, la Cour se référant d'ailleurs explicitement à ses précédents arrêts *Tele 2 Sverige et Watson*[45] du 21 décembre 2016 et *La Quadrature du Net* du 6 octobre 2020[46] pour justifier sa décision.

La position de la Cour de justice diffère donc de celle du Conseil constitutionnel qui, dans une décision QPC du 25 février 2022[47], a maintenu les effets de l'ancien article L 34-1 du Code des postes et des communications électroniques alors même qu'il instaurait, pour les opérateurs de communications électroniques, une obligation de conservation des données généralisée et indifférenciée. En effet, pour le Conseil constitutionnel, la remise en cause des mesures prises sur le fondement de l'ancien article L 34-1, pourtant jugé inconstitutionnel, serait susceptible de provoquer « *des conséquences manifestement excessives* ». Le Conseil étant, conformément à l'alinéa 2 de l'article 62 de la Constitution, seul compétent pour déterminer « *les conditions et limites dans lesquelles les effets que la disposition a produits sont susceptibles d'être remis en cause* »[48], le report *ad futurum* des effets de l'inconstitutionnalité pouvait donc se justifier au regard des « *objectifs à valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions* »[49]. Face à de tels impératifs, le report dans le temps des effets de l'inconstitutionnalité de l'ancien article L. 34-1 du Code des postes et des communications électroniques semblait donc opportun aux yeux des Sages.

La solution de la Cour de justice dans l'arrêt commenté semble donc s'écarter de celle du Conseil constitutionnel, qui fait primer les objectifs de sauvegarde de l'ordre public et de recherche des auteurs d'infractions sur le droit à la vie privée. Toutefois, si la Cour refuse la modulation des effets de la déclaration d'invalidité, elle admet le maintien de l'autonomie procédurale des États membres en matière de recevabilité des preuves.

---

44 CJUE, 28 févr. 2012, *Inter-Environnement Wallonie ASBL e.a.*, aff. C-41/11.
45 CJUE, gde ch., 21 décembre 2016, préc.
46 CJUE, Gde ch., 6 octobre 2020, préc.
47 Décision n° 2021-976/977 QPC du 25 février 2022 ; *BJB* mai-juin 2022, p. 5, n° 200r5, note E. Dezeuze et C. Méléard ; *D.* 2022, p. 1540, note M. Lassalle.
48 Art. 62 al. 2 de la Constitution.
49 Décision n° 2021-976/977 QPC du 25 février 2022, préc.

B.- Le maintien de l'autonomie procédurale des États membres en matière de recevabilité des preuves

En interdisant toute obligation générale et indifférenciée de conservation de données relatives au trafic à des fins d'accès par les autorités compétentes en matière financière, la CJUE remet en cause le dispositif français applicable. Dès lors, on peut se questionner sur le sort des procédures ouvertes et nourries conformément à des dispositions alors applicables, aujourd'hui déclarées non conformes au droit de l'Union.

Conformément à ce qui a été dit précédemment, la Cour de justice dans cette décision énonce que le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe en vertu du droit national. Le principe de primauté du droit de l'Union suppose en effet que le droit national soit interprété conformément au droit de l'Union et que les décisions de la Cour de justice soient d'application immédiate, sauf décision à titre exceptionnel de la Cour elle-même en différant l'application. Permettre aux juridictions nationales de moduler dans le temps l'application d'une de ces décisions reviendrait à faire primer temporairement le droit national sur le droit de l'Union, dans la mesure où le maintien du droit national, ne serait-ce que pour un laps de temps déterminé, reviendrait à imposer aux opérateurs une conservation des données alors même que cette conservation est contraire au droit de l'Union et constitue une grave ingérence dans les droits fondamentaux.

En conséquence, la question soulevée était de savoir si les éléments de preuve obtenus à partir de ces données devaient être déclarés irrecevables. Il était plus précisément demandé à la Cour quelle était l'incidence de la non-conformité de l'article L. 621-10 du Code monétaire et financier au droit européen sur la recevabilité des preuves dans le cadre des procédures ouvertes.

En effet, la Cour de cassation, en opérant les renvois préjudiciels devant la Cour de Justice, ne manquait pas de souligner l'importance de la conservation des données de connexion en matière d'abus de marché, dès lors que celles-ci constituent, selon le considérant 65 du règlement Abus de marché, « *une preuve essentielle et parfois la seule, permettant de détecter et de démontrer l'existence d'une opération d'initié ou d'une manipulation de marché* ». En invoquant la législation issue de l'Union européenne, la Cour de cassation invitait le juge de l'Union à opérer une conciliation entre deux intérêts déclarés protégés par le droit de l'Union européenne lui-même.

La Cour de justice, appliquant sa jurisprudence *Prokuratuur* du 2 mars 2021[50], vient énoncer que la recevabilité des preuves relève, en vertu du principe d'autonomie procédurale, des États membres, donc du droit national, sous réserve pour

50 CJUE, 2 mars 2021, *Prokuratuur*, aff. C-746/18.

les juges nationaux de respecter le principe d'équivalence et le principe d'effectivité dégagés par la jurisprudence *Rewe et Comet* de la Cour de justice[51].

Tout en réaffirmant le principe d'autonomie procédurale des États membres, qui implique qu'un État membre puisse mettre en œuvre le droit de l'Union dans les formes et procédures du droit national[52], la Cour de justice vient immédiatement tempérer ce principe qui n'est pas absolu.

Tout d'abord, le principe d'équivalence est une limite à l'autonomie procédurale des États membres, puisqu'il signifie, en présence d'une violation du droit de l'Union, que « *les procédures appliquées doivent être identiques à celles appliquées par le droit national dans le cas d'une affaire interne de même nature* ». Ce principe concerne notamment les modalités de preuve et de recours en justice. Aussi le droit de l'Union doit-il bénéficier des mêmes conditions d'effectivité juridictionnelle que les normes nationales comparables[53].

Ensuite, le principe d'effectivité vient, quant à lui, protéger les justiciables contre une potentielle privation dans l'exercice des droits que l'Union leur confère. En effet, l'exercice de leurs droits ne doit pas être rendu « *impossible pratiquement ou excessivement difficile* »[54]. Le droit national ne peut priver les justiciables de ce principe d'effectivité et donc de toute voie de recours à l'encontre des décisions nationales.

Ainsi, en application du principe d'effectivité, il devrait être possible de remettre en cause la recevabilité des preuves obtenues puisque leur admissibilité est directement contraire au droit au respect à la vie privée consacré par le droit de l'Union.

Toutefois, une nuance doit être faite. L'arrêt *Prokuratuur* mentionné par la Cour de justice dans l'arrêt ci-commenté énonce, sur une question similaire, que malgré le principe d'autonomie procédurale, les éléments de preuve devront être écartés par le juge national si les personnes visées par la procédure ne sont pas en mesure de les commenter efficacement. En effet, la Cour de Justice cherche avant tout à protéger la présomption d'innocence et les droits de la défense en évitant que ces données, obtenues illégalement, ne viennent porter préjudice à une personne soupçonnée d'être à l'origine d'infractions. Cette possibilité de commenter les éléments de preuve serait donc une condition pour déclarer les preuves recevables, par respect du principe du contradictoire et donc du droit au respect d'un procès équitable. Or en l'espèce, le prévenu pouvait demander une contre-expertise et était donc en mesure de commenter efficacement les éléments de preuve. Le juge

51 CJCE, 16 décembre 1976, *Rewe*, aff. 33/76 ; CJCE, 16 décembre 1976, *Comet*, aff. 45/76.
52 CJCE, 11 février 1971, *Fleischkontor*, aff. 39-70.
53 Chahira Boutayeb, *Droit institutionnel de l'Union européenne*, LGDJ, 5e éd., p. 662.
54 CJUE, 6 octobre 2015, *Târșia*, aff. C-69/14.

national devrait admettre la recevabilité des éléments de preuve obtenus par une conservation généralisée des données de connexion.

C'est d'ailleurs la position récente de la Chambre criminelle de la Cour de cassation[55], qui, dans le cadre d'une affaire d'association de malfaiteurs en bande organisée, a confirmé la validité de preuves résultant de l'exploitation de données de connexion, dès lors que les articles 156 et suivants du Code de procédure pénale prévoient « *que toute personne mise en examen peut solliciter du juge d'instruction une expertise et, le cas échéant, une contre-expertise, sous le contrôle de la chambre de l'instruction* [...] » et qu'il « *en est de même devant la juridiction de jugement* ». Les accusés pouvaient ainsi contester et commenter l'utilisation de ces éléments de preuve.

En définitive, il apparaît que l'irrecevabilité des preuves, provenant de données de connexion conservées de manière générale et indifférenciée en violation du droit de l'Union, ne sera caractérisée que lorsque les justiciables « *ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits*[56] ».

Conclusion

L'affaire, qui questionnait la possibilité pour le législateur national de retenir une conservation généralisée et indifférenciée des données personnelles de trafic pendant un an, à titre préventif, ici pour lutter contre les délits d'abus de marché, notamment le délit d'initié, est loin d'être achevée. La chambre criminelle de la Cour de cassation devrait rendre une décision prochainement.

La décision *VD et SR* constitue un apport bienvenu à la protection des droits et libertés dans le domaine du numérique[57]. Ainsi, les mutations technologiques doivent s'accompagner « *d'une transformation juridique profonde qui garantisse l'équilibre entre les intérêts en présence et la protection des droits et des libertés au fondement de notre État de droit*[58] ». La jurisprudence de la Cour assure ainsi son rôle de mise en place d'un cadre uniforme de protection au sein des États membres. Il est toutefois possible d'envisager que cette jurisprudence soit amenée à être précisée voire à évoluer compte tenu des constantes évolutions dont témoigne le secteur du numérique. À ce sujet, présentent un intérêt important les négociations sur la

55 Cass. crim., 12 juillet 2022, préc. ; M. Bendavid, C. Quendolo, « Conservation et accès aux données de connexion : la Cour de cassation prend position », *AJ pénal* 2022. 415.
56 Décision commentée, pt 106.
57 D. Simon, « Protection des données numériques », *Europe* n° 11, Novembre 2022, comm. 357.
58 Intervention de Jean-Marc Sauvé lors de la remise des prix de thèse de la Fondation Varenne le 12 décembre 2017.

proposition de « *règlement e-Privacy* »[59] présentée par la Commission européenne et dont l'objectif est de renforcer la protection et la confiance dans le monde du numérique, notamment en sécurisant le contenu de toutes les communications électroniques.

59 Prop. Règl. Parl. et Cons. UE concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (COM/2017/010 final) ; v. égal. la position du Conseil arrêtée en février 2021.