MINISTÈRE DE LA JUSTICE
DIRECTION DE L'ADMINISTRATION PÉNITENTIAIRE

****

CONCOURS EXTERNE
POUR LE RECRUTEMENT DE
DIRECTEURS PÉNITENTIAIRES D'INSERTION
ET DE PROBATION

SESSION 2023

2ème épreuve d'admissibilité

Une épreuve de note de synthèse à partir d'un dossier portant sur le droit pénal et la procédure pénale
(durée : 5H00 ; coefficient : 5)

****

SUJET PRINCIPAL
L'accès aux données de connexion dans l'enquête pénale

Aucun document n'est autorisé.

Le sujet est composé d'une page de garde suivie de la liste des annexes et d'un dossier documentaire de 9 documents.

Annexes

Document 1 - Téléphonie : le risque des enquêtes « à moitié » après les arrêts du 12 juillet - AJ Pénal 2022 p.396 - Christophe Korell, Ancien OPJ, assistant spécialisé, TJ Paris

Document 2 – Code de procédure pénale

Document 3 - Accès aux données de connexion : quelles pistes pour une mise en conformité ? - AJ Pénal 2022 p.400 - Alexandre Archambault, Avocat au barreau de Paris

Document 4 – Arrêt de Cour, grande chambre, 2 mars 2021

Document 5 – Décision n°2022-993 QPC du 20 mai 2022

Document 6 – Enquêtes pénales : conservation et accès aux données de connexion

Document 7 - Évolution normative et jurisprudentielle sur le thème des métadonnées - AJ Pénal 2022 p.392 -

Thomas Lebreton, Substitut du procureur au parquet de Nanterre

Document 8 – DACG fiches criminologique, juridique ou technique : les données de trafic et de localisation pendant l'enquête pénale

Document 9 – Données téléphoniques : les procureurs dénoncent « des obstacles majeurs » à la conduite des enquêtes

Document 1

AJ Pénal 2022 p.396

Téléphonie : le risque des enquêtes « à moitié » après les arrêts du 12 juillet

Christophe Korell, Ancien OPJ, assistant spécialisé, TJ Paris

C'est un euphémisme de dire que la jurisprudence des derniers mois sur les « données de connexion », émanant de la Cour de justice de l'Union européenne, du Conseil constitutionnel ou encore du Conseil d'État, est scrutée par les enquêteurs. Les signaux européens les inquiètent fortement. Ils craignent pour la qualité de leur travail quotidien, la réussite de leurs enquêtes. Avec ce sentiment latent d'aller à contre-courant des évolutions technologiques, mises à profit par les malfaiteurs mais que l'on a tendance à interdire du côté de l'enquête, ce qui crée une perte d'efficacité.

(…)

2. De quoi parle-t-on ?

Travailler sur la téléphonie, c'est travailler sur deux axes un peu distincts. On peut tout d'abord rechercher des éléments de preuve directs. Prenons l'exemple d'une plainte déposée pour des appels téléphoniques malveillants. La démarche de l'enquêteur sera de demander une facturation détaillée de la ligne de la victime et d'établir la réalité de ces appels téléphoniques. On pourra alors en connaître la fréquence (sont-ils rapprochés ?), les horaires (plutôt le jour, la nuit ?), et ensuite, dans la recherche de l'auteur, découvrir à partir de quel numéro de téléphone il a appelé. Est-ce toujours le même numéro ? S'agit-il d'un abonnement ? L'auteur a-t-il acheté une carte prépayée ? A-t-il utilisé la ligne pour faire d'autres victimes ?

Et puis, autre manière de travailler au-delà de la recherche de la preuve directe : le travail sur l'environnement. Souvent pour des infractions et affaires un peu plus complexes. On va dans ces hypothèses travailler sur les habitudes, pour connaître la « cible » ; en apprenant sur ses habitudes, on apprend surtout sur ce qui est inhabituel. Par exemple, les malfaiteurs savent aujourd'hui (la plupart du temps) qu'il ne faut pas prendre son téléphone sur soi au moment de la commission d'une infraction. Mais on pourra chercher, via la facturation détaillée si au moment de l'infraction, l'utilisation de la ligne du suspect relève de ses habitudes. Cela ne constituera pas un élément de preuve direct, mais pourra participer d'un faisceau d'indices.

La facturation détaillée permet de connaître les déplacements d'une personne (en fonction des relais téléphoniques déclenchés, avec des précisions variables) mais aussi ceux d'une partie de ses contacts. On peut imaginer deux suspects, complices, interpellés dans une affaire. En audition, les deux nient se connaître. Comparer leurs facturations détaillées et voir s'ils s'appellent peut constituer un élément intéressant. Qu'ils se connaissent ou pas d'ailleurs. À charge ou à décharge. Même si l'on sait aussi qu'une absence d'appels ne signifie pas, indéniablement, que les personnes ne se connaissent pas. Elles peuvent aussi bien (et c'est fréquent) se contacter par un autre moyen. À « l'ancienne », uniquement physiquement, ou en utilisant des applications chiffrées, telles que WhatsApp, voire même des lignes téléphoniques spécifiquement dédiées à leur entreprise criminelle (ce que les enquêteurs recherchent régulièrement).

3. Cadre des réquisitions issu de la loi du 2 mars 2022

La conservation des données. Le code des postes et des communications électroniques (CPCE), et plus particulièrement son article L. 34-1 (II), prévoit que les opérateurs de téléphonie ont l'obligation d'effacer ou de rendre anonymes les données relatives aux communications électroniques. Mais à chaque règle, ses exceptions (II à VI). Ils

doivent ainsi conserver :

1° les données nominatives, durant cinq ans, à compter de la fin de validité du contrat, pour « les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale » ;

2° les autres informations fournies par l'utilisateur (par exemple celles relatives au paiement), pendant un an, à compter de la fin de validité du contrat ;

3° les « données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux », et ce pour « les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale ».

La base est ici établie. Elle est ensuite déclinée dans le code de procédure pénale.

S'agissant de l'accès aux données, le fondement des réquisitions émises par les enquêteurs se trouvait initialement aux articles 60-1 et 60-2, alinéa 1er, en flagrance, aux articles 77-1-1 et 77-1-2 en préliminaire, et aux articles 99-3 et 99-4 dans le cadre d'une instruction (3). Pour tenter de faire correspondre le droit interne aux exigences européennes, le législateur a toutefois dû intervenir. C'est donc l'article 60-1-2 (qui se réfère à l'article L. 34-1 du CPCE), issu de la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire, qui précise désormais les cas dans lesquels les policiers peuvent procéder à des réquisitions portant sur des données techniques.

En ce qui concerne le cadre général, la procédure doit porter « sur un crime ou délit puni d'au moins trois ans d'emprisonnement ». Mais si le législateur en était resté là, nombre de situations problématiques auraient émergé, dans lesquelles une réquisition est absolument nécessaire, ne serait-ce que pour commencer une enquête, alors que l'infraction est punie de moins de trois ans d'emprisonnement. Trois exceptions ont donc été prévues. Les réquisitions sont possibles dans les procédures relatives à des infractions commises par l'utilisation d'un réseau de communications électroniques punissables d'au moins un an d'emprisonnement. Autre exception, lorsqu'il s'agit de terminaux appartenant à la victime et que la demande intervient à la demande de celle-ci, à la condition que l'infraction soit punissable d'une peine d'emprisonnement. Enfin, dernière exception, lorsqu'il s'agit de retrouver une personne disparue.

Ainsi, le législateur s'est-il attaché ici à restreindre le droit à réquisition en limitant le champ infractionnel.

Voici le nombre de réquisitions adressées à la PNIJ, au cours des trois dernières années, par cadre juridique, étant précisé que ces chiffres ne prennent pas en compte les réquisitions aux fins d'identification de l'abonné, dans la mesure où ces demandes résident hors périmètres de la jurisprudence de la CJUE (4).

À ce jour, une facturation détaillée coûte, via la PNIJ, 10,20 € (sur une période indivisible d'un mois), + 1 € par mois, une fadette de trois jours étant donc facturée de la même manière qu'une fadette de 30 jours.

4. Et maintenant ?

À la suite des arrêts de la Cour de cassation, mais également de la note de la Direction des affaires criminelles et des grâces du 13 juillet 2022, deux distinctions semblent s'opérer, dans l'attente d'une modification législative répondant aux critères exigés par les juridictions, notamment quant à l'impartialité de l'autorité autorisant les réquisitions.

Une première distinction en fonction du cadre juridique. Aucun changement en ce qui concerne la commission rogatoire, « dès lors, d'une part, que le juge d'instruction n'est pas une partie à la procédure mais une juridiction et, d'autre part, qu'il n'exerce pas l'action publique mais statue de façon impartiale sur le sort de celle-ci, mise en mouvement par le ministère public ou, le cas échéant, la partie civile ». Ainsi, les OPJ conservent le droit de réquisition sans autre autorisation que la commission rogatoire, étant précisé que si une information a été ouverte, c'est que l'infraction est criminelle (condition préalable obligatoire) ou nécessite des investigations complexes (criminalité organisée), ce qui semble déjà répondre à une partie des exigences de la Cour.

En ce qui concerne la flagrance et l'enquête préliminaire, les deux types d'enquêtes étaient jusque-là régies par une règle distincte : l'OPJ avait toute latitude à réquisition en flagrance, là où un avis du parquet était nécessaire en préliminaire. À la suite des récentes évolutions, se dessine une incertitude. Les parquets n'ont en effet pas tous fait le même choix. Deux notes de parquets différents auxquelles j'ai pu avoir accès en sont l'illustration. Pour le premier, les deux cadres juridiques sont désormais fondus et répondent à une même règle de demande d'autorisation, le magistrat devant alors arbitrer en fonction « [...] de la nature des agissements de la personne poursuivie, de l'importance du dommage qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue ». Un autre parquet préconise une demande d'autorisation motivée en préliminaire, laissant l'initiative aux OPJ en flagrance, en leur demandant de procéder eux-mêmes à un « contrôle de nécessité et de proportionnalité », lequel devra être acté.

Une seconde distinction en fonction du type d'infraction. Toutes les atteintes liées au terrorisme ou à la criminalité organisée sont, en quelque sorte « sanctuarisées » ; donc, aucun changement. En ce qui concerne les atteintes aux personnes, il y a désormais lieu de solliciter une autorisation au parquet, et les réquisitions ne sont possibles, en tout état de cause, que pour les infractions punissables d'au moins trois ans d'emprisonnement (conformément à l'article 60-1-2 du code de procédure pénale). Demeure une incertitude, en ce qui concerne les atteintes dites « aux biens ». En effet, certains parquets auraient tendance, dans leurs directives, à les exclure du champ d'application des réquisitions (sauf affaires criminelles ou criminalité organisée).

Le parquet de Paris, quant à lui, pose le principe d'une autorisation par procédure « après appréciation de la nécessité et de la proportionnalité ». On le voit, des questions d'harmonisation se posent, les parquets n'ayant pas, à ce jour, tous la même lecture et interprétation de la portée de ces arrêts. Cela fait peser une grande incertitude juridique sur les procédures, mais également, pour les OPJ qui peuvent avoir affaire à différents parquets (comme c'est le cas, par exemple, pour la police judiciaire parisienne), à des façons de procéder qui divergent, ce qui peut naturellement amener de la confusion.

Le bornage. Des questions se posent à ce sujet qui ne sont pour le moment pas arbitrées de la même manière selon le parquet de compétence. Le bornage est le fait, pour l'enquêteur, de solliciter un opérateur (via la PNIJ) pour recevoir l'ensemble des communications émises sur son réseau à partir d'un endroit défini. Faire un bornage peut recouvrer deux possibilités :
- chercher à savoir si un numéro était présent sur « tel » secteur ;
- chercher le numéro de téléphone d'un suspect que l'on sait être passé par « tel » secteur, et qui nous est inconnu (auquel cas, si un numéro suspect est découvert, il faudra passer par l'identification et la fadette pour vérifier l'hypothèse).

Doit-on considérer le bornage comme une donnée de connexion au sens de la CJUE et de la Cour de cassation ? *A priori,* on aurait tendance à répondre par la négative. Les arrêts récents visent à protéger la vie privée, donc tout ce qui semble relatif aux habitudes, à l'orientation sexuelle, politique, etc. Ce qu'il serait parfois possible de trouver/comprendre via la facturation détaillée d'une personne, mais impossible par un « simple » bornage. En tout état de cause, avec un bornage, il est impossible de connaître des habitudes de vie d'une personne et les détails liés à sa vie privée, comme ce pourrait être le cas avec une fadette (j'utilise volontairement le conditionnel parce que, dans la

pratique, les enquêteurs se fichent bien de toutes ces considérations).

En pratique. Prenons l'exemple d'un vol de téléphone portable commis en même temps qu'une agression sexuelle. Il s'agit de faire une réquisition portant sur le téléphone volé de la victime. Les questions que l'on peut se poser sont : la ligne a-t-elle été utilisée par le mis en cause ? Si oui, de quelle manière s'est-il déplacé ? L'auteur du vol (ou potentiellement quelqu'un à qui il aurait donné/vendu le téléphone) a-t-il mis sa propre puce téléphonique dans le téléphone ? L'enquêteur se trouve dans le champ d'application de l'article 60-1-2 du code de procédure pénale. Il s'agit d'une infraction, l'agression sexuelle, punissable de cinq ans d'emprisonnement ; par ailleurs, comme il s'agit du terminal de la victime, qui a donné l'autorisation de procéder à une recherche sur sa ligne, il n'y a pas de difficulté (encore que la question peut se poser de savoir si, là aussi, l'enquêteur doit tout de même solliciter une autorisation du parquet). Bingo !, il semblerait qu'une puce téléphonique ait été insérée dans le boitier. Deux informations distinctes pourraient alors être utiles :

- l'identification de l'abonné de la nouvelle puce : d'expérience, neuf fois sur dix, la puce de l'auteur est au nom de ce que l'on appelle un « toc », c'est-à-dire un nom fantaisiste, qui soit n'existe pas, soit est usurpé. Ou alors, aucune identité n'est associée (certains opérateurs « MVNO »(5) ne prennent même pas la peine d'enregistrer une identité ou de la vérifier). En l'absence d'identité réelle, il s'agit alors de travailler sur cette nouvelle puce ;

- le détail des appels : quels sont ses contacts ? Comment l'utilisateur se déplace-t-il ? S'agit-il du voleur ? Le téléphone a-t-il déjà été revendu, auquel cas on se trouve face au receleur. Bref, bien des questions peuvent (et doivent) se poser. Quoi qu'il en soit, l'enquêteur doit alors procéder à une seconde réquisition auprès de l'opérateur. Donc il formule une demande d'autorisation auprès du parquet (par mail ou par téléphone). Nous sommes vendredi, il est 17 heures... Il ne reçoit pas de réponse. Se passe une journée, voire le week-end (oui, le parquetier n'a pas que cela à faire, doit probablement avoir quelques demandes du genre sans compter les autres tâches qui sont les siennes). Finalement, il donne l'autorisation. L'enquête globale permet d'identifier un homme qui sera interpellé et reconnu par la victime. Mais ne permettra pas de retrouver le téléphone volé. Peut-être que sans ce temps perdu, on aurait pu retrouver l'objet du délit. Ou pas. Est-ce important ? Je le pense ; c'est à la fois un moyen de preuve, mais aussi une perte directe pour la victime.

Autre exemple (appuyé sur le fait que les réquisitions ne seraient pas autorisées en ce qui concerne les atteintes aux biens). Un homme met sa voiture en vente sur un site internet. Il est appelé par un acheteur potentiel. Ils se mettent d'accord pour la transaction. La vente se fait, l'acheteur payant avec un chèque de banque. Quelques jours plus tard, le vendeur s'aperçoit que le chèque était faux. La victime dépose plainte. L'un des axes d'investigation est de savoir avec quel numéro la victime a été appelée. Plusieurs informations à rechercher : est-ce que ce téléphone s'est déplacé sur le lieu de rendez-vous ? Peut-être que les autres numéros de téléphone figurant sur la facturation détaillée appartiennent à d'autres victimes ? L'enquête pourrait donc permettre d'identifier d'autres victimes d'escroquerie ou de tentatives. Mais, s'agissant d'une atteinte aux biens, une réquisition à l'opérateur dans le cadre d'une enquête de flagrance ne serait à ce jour plus possible.

On oublie aussi, trop souvent, que la téléphonie peut aussi être utilisée à décharge. Un homme est en garde à vue pour une affaire d'atteinte aux biens. Dans ses auditions, il nie être l'auteur des faits. Un téléphone est découvert lors de la perquisition à son domicile. Pour l'enquêteur, il y aurait lieu de faire une fadette de ce numéro et de vérifier le comportement de la ligne téléphonique au moment des faits. Il ne pourrait plus, là non plus, procéder à la vérification. D'ailleurs, on peut aller plus loin. Peut-être même que cette vérification pourrait être faite avant interpellation (le numéro de téléphone peut être découvert à la suite d'un certain nombre d'investigations). Et de telles recherches pourraient éviter une garde à vue. Il m'est arrivé à plusieurs reprises d'effectuer des recherches en téléphonie ayant permis de démontrer qu'une personne suspectée ne pouvait pas avoir participé aux faits sur lesquels nous enquêtions.

5. Conclusion

La téléphonie est l'une des pistes importantes d'une enquête. Dans chaque cas pratique, on expliquera que l'enquêteur peut faire d'autres vérifications et avancer ainsi. Peut-être. Mais la téléphonie reste un axe qui peut avoir son importance. Et s'en priver, c'est un peu comme fermer les yeux et refuser de voir ce qui est visible.

Le principal problème rencontré dans l'application de ces nouveaux arrêts réside dans la perte d'autonomie de l'OPJ dans ses investigations et dans la perte de temps. Demander l'autorisation (par téléphone ou par mail), attendre celle-ci, en cas de réponse favorable, procéder à la réquisition, l'analyser. Puis, en fonction de ces nouvelles analyses, refaire de nouvelles demandes d'autorisation, etc., lorsque l'on sait qu'il n'est pas rare qu'un enquêteur attende une heure au téléphone pour un avis du parquet...

Enfin, tous les juristes auront noté que, à droit constant, ces arrêts ne satisfont pas pleinement la jurisprudence établie par la CJUE, s'agissant du parquet qui « dirige la procédure d'enquête et exerce [...] l'action publique ». La Cour de cassation a certes jugé que le parquet ne pourrait plus autoriser les réquisitions de fadettes, mais, pour sauver les procédures en cours, elle a exigé, pour retenir la nullité, la caractérisation d'une atteinte à la vie privée.

Finalement, plus on met de pression sur les enquêteurs en les obligeant à demander de plus en plus d'autorisations, prenant encore plus de temps, engendrant une baisse d'efficacité, moins ils feront de demandes, ne souhaitant pas passer les trois quarts de leur journée à écrire des mails ou à attendre au téléphone. Ce qui aura de fait un impact non négligeable sur le contenu des enquêtes soumises à l'autorité judiciaire.

Voilà un nouveau signal négatif envoyé aux enquêteurs français. Certains services avaient déjà du mal à recruter, tant l'investigation subit un désamour depuis plusieurs années. Un signe parmi d'autres : il y a encore quelques années de cela, pour arriver dans un service d'investigation local, une expérience de terrain était demandée et le chef de service faisait son choix parmi plusieurs demandes. Aujourd'hui, dans nombre de commissariats, on retrouve des élèves tout juste sortis de l'école dans les services d'investigation. Sans même qu'ils aient forcément été volontaires. Mais rien n'est fait pour que cela s'arrange. Une procédure toujours plus complexe, des investigations toujours plus techniques. En parallèle de moins en moins de personnes pour les mener, et plus aucun avantage à sacrifier une vie de famille au travail d'investigation, extrêmement chronophage. Avec, en creux, cette sensation que cela n'intéresse à aucun moment la classe politique. Une fois passées les statistiques sur les interpellations, le devenir de ces affaires n'évoque rien à personne. Pour finir, on « priorise » ce qui est possible de l'être, et le reste est placé sur la pile « VR » pour « vaines recherches », en vue d'un classement sans suite qui sera décidé par le magistrat. Parce que, faute de temps, il faut bien choisir. Et choisir, c'est renoncer. Au détriment de qui ? Des plaignants, d'abord. Mais aussi de ceux qui restent encore, qui trouvent chaque jour de moins en moins de sens à leur investissement. Et tout cela sans même parler de la future réforme de la police nationale, laquelle verra s'organiser, dans un ressort unique, départemental, l'ensemble de la filière d'investigation, qu'elle soit issue de la sécurité publique, de la police aux frontières, ou encore de la police judiciaire. Cette nouvelle organisation laissant craindre un nivellement par le bas du judiciaire. Les « péjistes » étant susceptibles de se retrouver à traiter, en plus de leurs affaires de haut niveau, des dossiers priorisés par la politique du moment, pour moins d'efficacité.

On en revient finalement, ici, aux problématiques de la justice. Un manque cruel de moyens, et surtout d'intérêt. Cela paraît une évidence : pour que la justice fonctionne, que les citoyens aient confiance en leur justice (et accessoirement, que les personnes qui s'y emploient ne soient pas les victimes d'une perte de sens de leur mission), les institutions se doivent d'avoir des moyens de travailler. Là où aujourd'hui, il semblerait que l'on doive toujours avoir de meilleurs résultats, avec moins de moyens.

Document 2

Code de procédure pénale

Article 60-1

Le procureur de la République ou l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris, sous réserve de l'article 60-1-2, celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord.

A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre à cette réquisition dans les meilleurs délais et s'il y a lieu selon les normes exigées est puni d'une amende de 3 750 euros.

A peine de nullité, ne peuvent être versés au dossier les éléments obtenus par une réquisition prise en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.

Article 60-1-2

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

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

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

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

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

Article 60-2

Sur demande de l'officier de police judiciaire, ou sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au d du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 précité et au 2° de l'article 80 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi et sous réserve de l'article 60-1-2 du présent code, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire ou, sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, 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.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 euros.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises.

Article 77-1-1

Le procureur de la République ou, sur autorisation de celui-ci, l'officier ou l'agent de police judiciaire, peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris, sous réserve de l'article 60-1-2, celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord.

En cas d'absence de réponse de la personne aux réquisitions, les dispositions du second alinéa de l'article 60-1 sont applicables.

Le dernier alinéa de l'article 60-1 et l'article 60-1-1 sont également applicables.

Le procureur de la République peut, par la voie d'instructions générales prises en application de l'article 39-3, autoriser les officiers ou agents de police judiciaire, pour des catégories d'infractions qu'il détermine, à requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique, de leur remettre des informations intéressant l'enquête qui sont issues d'un système de vidéoprotection. Le procureur est avisé sans délai de ces réquisitions. Ces instructions générales ont une durée qui ne peut excéder six mois. Elles peuvent être renouvelées.

Article 77-1-2

Sur autorisation du procureur de la République, l'officier ou l'agent de police judiciaire peut procéder aux réquisitions prévues par le premier alinéa de l'article 60-2 sous réserve de l'article 60-1-2.

Sur autorisation du juge des libertés et de la détention saisi à cette fin par le procureur de la République, l'officier ou l'agent de police peut procéder aux réquisitions prévues par le deuxième alinéa de l'article 60-2.

Les organismes ou personnes concernés mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni conformément aux dispositions du quatrième alinéa de l'article 60-2.

Article 99-3

Le juge d'instruction ou l'officier de police judiciaire par lui commis peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'instruction, y compris, sous réserve de l'article 60-1-2, ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-3 et à l'article 56-5, la remise des documents ne peut intervenir qu'avec leur accord.

En l'absence de réponse de la personne aux réquisitions, les dispositions du deuxième alinéa de l'article 60-1 sont applicables.

Le dernier alinéa de l'article 60-1 est également applicable.

Lorsque les réquisitions portent sur des données mentionnées à l'article 60-1-1 et émises par un avocat, elles ne peuvent être faites que sur ordonnance motivée du juge des libertés et de la détention, saisi à cette fin par le juge d'instruction, et les trois derniers alinéas du même article 60-1-1 sont applicables.

Article 99-4

Pour les nécessités de l'exécution de la commission rogatoire, l'officier de police judiciaire peut procéder aux réquisitions prévues par le premier alinéa de l'article 60-2.

Avec l'autorisation expresse du juge d'instruction, l'officier de police peut procéder aux réquisitions prévues par le deuxième alinéa de l'article 60-2.

Les organismes ou personnes concernés mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni conformément aux dispositions du quatrième alinéa de l'article 60-2.

AJ Pénal 2022 p.400

Accès aux données de connexion : quelles pistes pour une mise en conformité ?

Alexandre Archambault, Avocat au barreau de Paris

Par une série d'arrêts(1) rendus dans la torpeur estivale, la Cour de cassation a rappelé à ses responsabilités le législateur sur la nécessaire, et hélas trop longtemps esquivée, réforme de la procédure pénale s'agissant de l'accès aux données détenues par les opérateurs de communications électroniques.

Ces arrêts sont tout sauf une surprise au regard des messages en creux distillés dans de précédents arrêts et transmissions de QPC. Traitant avant tout de la question de l'accès aux données, ils viennent compléter la solution, pour le moins créative, dégagée par le Conseil d'État en 2021 dans son arrêt *French Data Network* (2), et qui se focalisait sur la question de l'obligation de conservation pouvant être imposée aux opérateurs, laissant au juge judiciaire le soin de se prononcer sur la validité de l'accès s'agissant des enquêtes pénales.

Si les arrêts de la CJUE(3) ont suscité de profondes interrogations en France, « il paraît difficile de soutenir qu'en renforçant les garanties protectrices de la vie privée, la Cour de justice aurait porté atteinte à l'identité constitutionnelle de la France », pour reprendre les termes de l'avocat général Desportes dans son avis rendu dans le cadre de l'examen des pourvois.

Dans ses arrêts du 12 juillet 2022 empreints de la culture européenne de son nouveau premier président, la Cour de cassation, loin de bloquer l'accès à des données cruciales pour l'identification et la poursuite d'auteurs d'infractions pénales, vient fournir quelques précieuses indications pour une véritable mise en conformité du droit national avec le droit de l'Union.

Avant d'aborder les conditions de validité posées par le juge tant européen que national ainsi que les pistes de réforme possibles, il importe de préciser que l'encadrement ne porte que sur les données de connexion et de localisation. Parce que l'atteinte à la vie privée n'est pas jugée disproportionnée au regard de l'objectif de recherche et poursuite des auteurs d'infractions pénales(4), les demandes d'identification, qui concentrent une part très significative des réquisitions(5), ne sont donc nullement remises en question ; la notice explicative publiée par la Cour de cassation en accompagnement de ses arrêts est parfaitement claire sur ce point. C'est donc à la question de l'accès aux données de connexion et de localisation que s'attacheront à répondre les développements qui vont suivre.

Les conditions posées par la CJUE et reprises par la Cour de cassation

L'article préliminaire du code de procédure pénale dispose qu'« au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction ». Sur ces bases, des chambres de l'instruction rejetaient les demandes en nullité de réquisitions portant sur des données de connexion et de localisation effectuées sous l'autorité du parquet par des requérants invoquant la jurisprudence de la CJUE. Car jusqu'aux arrêts de la Cour de cassation en date du 12 juillet 2022 subsistait une divergence d'interprétation avec le juge européen sur le sens à donner à « l'autorité judiciaire », la CJUE estimant que le ministère public ne présentait pas les garanties attendues en matière d'accès aux données de connexion et de localisation(6).

Pourquoi encadrer plus particulièrement les données de connexion et de localisation qui, à première vue, ne sont que purement techniques ? La raison provient de la richesse des informations (7) qui peuvent en être tirées en les combinant entre elles au moyen de capacités de traitement de masse sans cesse plus importantes, comme les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements, les activités exercées, les relations sociales, les milieux fréquentés, les orientations politiques, religieuses, philosophiques ou sexuelles. Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données ont été sollicitées, ce qui amène la CJUE à considérer ces informations tout aussi sensibles, au regard du droit au respect de la vie privée, que le contenu même des communications. Dès lors, l'ingérence que constituent la conservation et l'accès aux données de connexion est particulièrement grave (8).

Depuis son revirement opéré en 2015 (9) s'inscrivant dans un mouvement jurisprudentiel plus large visant à élever le niveau d'exigences en matière de protection de la vie privée au regard de l'importance du numérique dans la vie quotidienne, le Conseil constitutionnel rappelle constamment que « compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée » (10) et s'attache à vérifier la présence de garanties permettant de s'assurer d'une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions.

S'agissant des données de connexion et de localisation, les données d'activité établies par la Direction des affaires criminelles et des grâces mettent en évidence un recours désormais massif par les services enquêteurs agissant sur instruction du parquet ou sur commission rogatoire d'un juge aux demandes d'accès aux données de connexion conservées par les opérateurs et fournisseurs de services de communications. Ainsi, en 2021, environ un million deux cent vingt et un mille réquisitions de données de connexion ont été formulées dans le cadre d'une enquête préliminaire ou de flagrance et cinq cent cinq mille dans le cadre d'une commission rogatoire d'un juge d'instruction.

C'est pourquoi, compte tenu de l'ingérence particulière forte dans la vie privée des personnes concernées et du développement considérable de la volumétrie de réquisitions portant sur les données de connexion, les juges, tant européens que nationaux, ont entendu encadrer les modalités d'accès.

1.1. Les conditions

Au fil de sa demi-douzaine d'arrêts sur cette question, la CJUE a posé plusieurs conditions cumulatives pour la validité de l'accès aux données de connexion.

En premier lieu, l'accès ne peut être accordé que pour les données conservées par les opérateurs et fournisseurs de services de communications électroniques de manière conforme au droit de l'Union européenne (11). En particulier, la demande ne peut exiger des opérateurs et fournisseurs de services ni de conserver et communiquer des données qui ne sont nullement pertinentes pour l'acheminement d'une communication, telle par exemple l'URL (adresse précise d'un contenu consulté ou d'un compte de réseau social avec lequel il y a eu une interaction), ni de maintenir la conservation au-delà du seuil fixé par la loi (un an après l'acheminement s'agissant des données de connexion et de localisation).

En second lieu, l'accès ne peut être justifié en principe que par la finalité ou une finalité plus grave que celle pour laquelle cette conservation a été imposée (12).

En troisième lieu, au regard de l'exigence de proportionnalité, une législation nationale n'est valable que si elle

comporte des règles claires et précises encadrant la portée et l'application de la mesure en cause et imposant des exigences minimales : en particulier, elle doit prévoir les conditions matérielles et procédurales régissant cette utilisation (13) ; elle doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause en se cantonnant au strict nécessaire (14) et en exigeant une motivation des demandes (15), pourtant non exigée par la Cour de cassation dans de précédents arrêts (16).

En quatrième lieu, l'accès aux données de trafic et de localisation présentant par nature une ingérence grave, quelles que soient la durée de la période pour laquelle l'accès est sollicité, la quantité ou la nature des données disponibles, il importe de ne réserver cet accès qu'aux procédures visant la lutte contre la criminalité et délinquance grave (que les infractions soient réalisées ou projetées) ou la prévention de menaces graves contre la sécurité publique, quelles que soient la durée de la période pour laquelle l'accès est sollicité et la quantité ou la nature des données disponibles pour une telle période (17).

En cinquième lieu, l'accès doit être soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant, présentant toutes les garanties nécessaires en vue d'assurer une conciliation entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de l'identification et la poursuite des auteurs d'infractions pénales et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont sollicitées. La décision de cette juridiction ou de cette entité doit intervenir à la suite d'une demande motivée des services enquêteurs. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais (18).

En dernier lieu, la Cour a établi depuis l'arrêt *Tele2 Sverige* (19) que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé doivent en informer les personnes concernées, dès lors que cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, cette information est nécessaire pour permettre aux personnes dont les données ont été sollicitées d'exercer leur droit de recours. Au regard de l'objectif de poursuite des auteurs d'infractions pénales, il est admis que cette information puisse être différée s'agissant des infractions d'une particulière gravité afin de ne pas mettre en péril la conduite des enquêtes en cours.

1.2. Déclinaison de ces principes par la Cour de cassation

Historiquement, l'accès aux données détenues par les opérateurs n'était possible que dans le cadre des crimes et délits passibles d'une peine de prison de trois ans.

Avec la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, cet accès a été étendu pour les enquêtes de flagrance (création des articles 60-1 et 60-2 du code de procédure pénale) et préliminaires (art. 77-1-1 et 77-1-2), avec autorisation du juge des libertés et de la détention (JLD) pour ce dernier cas pour les données détenues par un opérateur.

La motivation des demandes n'est nullement exigée (20), pas plus que l'information des personnes concernées, ce qui en pratique peut entraîner des frictions avec des acteurs majeurs du numérique établis dans des pays dont la législation interne impose l'information des personnes concernées sauf infractions particulièrement graves.

Enquêtes préliminaires et de flagrance. Dans ses arrêts du 12 juillet 2022, et notamment dans l'arrêt n° 21.83-710 portant sur des dispositions antérieures à la loi n° 2022-299 du 2 mars 2022, la Cour de cassation, rappelant la primauté du droit de l'Union, estime les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale ne sont pas conformes au droit de l'Union en ce que les réquisitions formulées en enquête préliminaire ne font pas l'objet d'un contrôle

préalable par une juridiction ou une autorité administrative indépendante (21) dotée de pouvoirs contraignants. En effet, quel que soit son statut, le procureur de la République dirige la procédure d'enquête et exerce, le cas échéant, l'action publique.

Informations judiciaires. Dans ses arrêts en date du 12 juillet 2022, la Cour de cassation valide les réquisitions formulées par un juge d'instruction. La Cour relève d'une part que le juge d'instruction n'est pas une partie à la procédure mais une juridiction qui statue notamment sur les demandes d'actes d'investigation formées par les parties, lesquelles disposent d'un recours en cas de refus, et d'autre part qu'il n'exerce pas l'action publique mais statue de façon impartiale sur le sort de celle-ci, mise en mouvement par le ministère public ou, le cas échéant, la partie civile (22). Dès lors, sur ces bases, les articles 99-3 et 99-4 du code de procédure pénale sont donc conformes au droit européen.

On relèvera enfin que le fait que les techniques de sonorisation soient autorisées par un magistrat du siège a été également mis en avant quelques jours après par la Cour de cassation pour rejeter la demande de transmission d'une QPC (23).

Les pistes envisageables pour une mise en conformité de l'accès aux données

Une véritable réforme de la procédure pénale s'agissant de l'accès aux données de connexion conservées par les opérateurs apparaît d'autant plus inéluctable que la date d'effet des censures opérées par le Conseil constitutionnel arrive à échéance le 31 décembre 2022, et que le dispositif mis en place par l'article 12 de la loi n° 2022-299 visant à combattre le harcèlement scolaire se retrouve fragilisé à la lumière des principes rappelés par la Cour de cassation dans ses arrêts du 12 juillet.

Dès lors, sur le fondement des jalons posés par le juge européen, et repris par la Cour de cassation dans ses arrêts du 12 juillet 2022, deux pistes semblent se dégager pour le contrôle de la validité des réquisitions portant sur les données de connexion et localisation.

2.1. La piste judiciaire

En première approche, il apparaît parfaitement logique de confier à un magistrat du siège le soin de contrôler et d'autoriser les demandes d'accès aux données de connexion et localisation.

2.1.1. Le juge d'instruction

Historiquement, l'accès aux données de connexion et de localisation conservées par les opérateurs n'était possible que dans le cadre d'une information judiciaire conduite par un juge d'instruction. Lui confier la compétence de contrôler et autoriser les demandes d'accès aux données de connexion et de localisation serait quelque part un retour aux sources, d'autant plus qu'une telle piste est validée tant par le Conseil constitutionnel que par la Cour de cassation dans ses arrêts du 12 juillet 2022. Ainsi, dans les affaires enregistrées sous les n^{os} 21-83.820 et 21-84.096, la chambre criminelle écarte toute irrégularité, après avoir relevé que les enquêteurs n'ont eu accès aux données de trafic et de localisation du requérant que sur commission rogatoire du juge d'instruction.

Toutefois, cette piste se heurte en pratique à plusieurs obstacles majeurs. En premier lieu, la compétence spécialisée du juge d'instruction, qui ne traite à ce jour qu'une infime minorité des enquêtes pénales, puisque seules 3 % des procédures font l'objet d'une information.

En second lieu, la problématique des moyens, dans un contexte où les effectifs de la magistrature en France sont significativement inférieurs à ceux de nos voisins européens (24), générant un mal-être indéniable (25), et sachant

qu'il se passe plusieurs années entre l'entrée à l'École nationale de la magistrature et l'affectation en juridiction.

On peut donc légitimement s'interroger sur l'efficience à court terme d'une telle piste.

2.1.2. Le juge des libertés et de la détention

Cette piste est déjà à l'oeuvre puisque, dans le prolongement des nombreuses censures du Conseil constitutionnel relatives au droit de communication de l'administration portant sur les données de connexion, le JLD contrôle désormais les demandes d'accès à de telles données formulées par les autorités administratives.

Par ailleurs, en application de l'article 77-1-2 du code de procédure pénale, les données de connexion et de localisation conservées par les opérateurs doivent faire l'objet d'une autorisation du JLD.

Comme pour le juge d'instruction, cette piste se heurte cependant une nouvelle fois à la cruelle réalité du manque de moyens octroyés par le législateur à la Justice, puisque notre pays se distingue de ses voisins européens par un budget très réduit par rapport aux standards des pays comparables, se traduisant par un déficit de magistrats et de fonctionnaires des services judiciaires et, plus inquiétant pour la qualité des enquêtes, un profond mal-être des personnels.

Il reste que, selon une étude d'impact établie par la direction des services judiciaires du ministère de la Justice, en retenant l'hypothèse la plus favorable, celle où les réquisitions aux fins d'identification de l'abonné ne relèveraient pas du contrôle préalable, l'extension du périmètre du JLD impliquerait au minimum un triplement des effectifs ; actuellement près de deux cent seize JLD sont affectés au sein des tribunaux judiciaires. D'après cette étude d'impact, pour le moins optimiste de l'avis des principaux intéressés, confier aux JLD le contrôle et l'autorisation des demandes de réquisitions portant sur les données de connexion et de localisation impliquerait la création d'au moins cinq cent trente-six postes. Soit en pratique un nombre significativement supérieur compte tenu des périodes d'astreintes pour contrôler et autoriser les demandes effectuées en dehors des heures ouvrables, des congés et sessions de formation. En outre, une telle extension du périmètre impliquera une nécessaire augmentation des effectifs de fonctionnaires de greffe, évaluée à deux cent dix-huit postes par cette même étude d'impact.

S'agissant des magistrats du parquet, ce transfert impliquerait également un renforcement substantiel des effectifs ou permettrait au contraire un gain, selon que le juge des libertés et de la détention interviendrait sur la saisine du ministère public ou non.

Pour les mêmes raisons que pour le juge d'instruction, tenant à l'indigence dans laquelle le législateur maintient la Justice depuis plusieurs décennies, on peut légitimement s'interroger sur l'efficience à court terme d'une telle piste, même si elle apparaît comme la plus respectueuse des libertés publiques.

2.2. Le recours à une autorité administrative indépendante (AAI)

Aussi étrange que cela puisse paraître de prime abord au regard des interrogations, notamment sur la conformité constitutionnelle (26), qu'elle peut susciter, la piste du contrôle préalable des demandes judiciaires d'accès aux données de connexion et de localisation est pourtant validée par la CJUE depuis l'arrêt *Tele2 Sverige* (27).

L'intervention d'une autorité administrative indépendante dans le cadre d'actes d'investigation diligentés par l'autorité judiciaire est par ailleurs déjà une réalité en droit national, par exemple pour les éléments couverts par le secret de la Défense nationale dont l'accès est conditionné à l'autorisation de la Commission du secret de la Défense

nationale (28).

Pour la CJUE, le contrôle opéré par une autorité administrative doit répondre à plusieurs garanties : l'autorité doit jouir d'un statut lui permettant d'agir de manière objective et impartiale (29). Elle doit également être dotée de pouvoirs contraignants (30).

2.2.1. La CNCTR ?

En première approche, il pourrait être envisagé d'étendre aux demandes judiciaires le périmètre d'action de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante, héritière de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) et chargée de veiller à ce que les techniques de renseignement soient légalement mises en oeuvre sur le territoire national (31). En effet, si la chaine de traitement peut différer, les données de connexion et de localisation sont les mêmes, que la réquisition soit administrative ou judiciaire. La CNCTR, qui compte parmi ses membres deux magistrats de la Cour de cassation, dispose donc des compétences techniques et juridiques pour contrôler les demandes.

Toutefois, à date, cette piste ne répond pas pleinement aux exigences rappelées par le juge européen, dans la mesure où la CNCTR n'est nullement dotée d'un pouvoir contraignant. Si elle est consultée *a priori*, sauf cas d'urgence, sur des demandes qui doivent être motivées (32), les services demandeurs ne sont nullement liés par les avis rendus par la CNCTR. Cette absence de pouvoir contraignant a d'ailleurs été mise en exergue par le Conseil d'État dans son arrêt *French Data Network* (33) s'agissant de l'accès administratif aux données de connexion pour justifier l'annulation des dispositions réglementaires régissant l'accès des services de renseignement aux données de connexion et de localisation. Dès lors, confier à la CNCTR la mission de contrôler la validité des demandes d'accès aux données détenues par les opérateurs nécessiterait de faire évoluer son périmètre d'action en la dotant d'un véritable pouvoir contraignant.

Enfin, se posera là aussi la question de l'adéquation des moyens, car la volumétrie traitée à ce jour par la CNCTR (quatre-vingt-sept mille cinq cent quatre-vingt-huit demandes traitées en 2021) est sans commune mesure avec le volume de réquisitions judiciaires portant sur les données de connexion et de localisation (un million sept cent vingt-six mille cent quarante-quatre selon les chiffres communiqués par le ministère de la Justice dans le cadre de l'examen des pourvois ayant donné lieu aux arrêts du 12 juillet 2022).

2.2.2. Une nouvelle AAI dédiée aux données de connexion ?

Compte tenu du périmètre particulier de l'intervention de la CNCTR (sécurité nationale et concentration du contrôle sur quelques services précisément identifiés) et du changement d'échelle qu'implique le contrôle de réquisitions judiciaires émises depuis l'ensemble du territoire, le législateur pourrait opter pour la création, *ex nihilo* ou plus probablement sur la base d'une agence existante, d'une nouvelle autorité administrative indépendante, dotée de pouvoirs contraignants, dédiée au contrôle de la validité des demandes de réquisitions judiciaires.

L'Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) chapeautant la plateforme nationale des interceptions judiciaires (PNIJ), l'entité assurant l'interface avec les opérateurs et fournisseurs de services de communications électroniques, pourrait constituer une base de travail, à condition de faire évoluer sa gouvernance et sa composition pour y associer des magistrats des deux ordres ainsi que parlementaires et personnalités qualifiées (34) dotés d'une véritable culture européenne.

DOCUMENT 4

ARRET DE LA COUR (grande chambre)

2 mars 2021 (*)

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Directive 2002/58/CE – Fournisseurs de services de communications électroniques – Confidentialité des communications – Limitations – Article 15, paragraphe 1 – Articles 7, 8 et 11 ainsi que article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne – Législation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation par les fournisseurs de services de communications électroniques – Accès des autorités nationales aux données conservées à des fins d'enquêtes – Lutte contre la criminalité en général – Autorisation donnée par le ministère public – Utilisation des données dans le cadre du procès pénal en tant qu'éléments de preuve – Recevabilité »

Dans l'affaire C-746/18,

LA COUR (grande chambre),

composée de (…)

Arrêt

Par ces motifs, la Cour (grande chambre) dit pour droit :

1) **L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période.**

2) **L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.**

Signatures

DOCUMENT 5

Conseil constitutionnel

Décision n° 2022-993 QPC du 20 mai 2022

NOR : *CSCX2214929S*

(M. LOTFI H.)

Le Conseil constitutionnel a été saisi le 11 mars 2022 par la Cour de cassation (chambre criminelle, arrêt n° 387 du 8 mars 2022), dans les conditions prévues à l'article 61-1 de la Constitution, d'une question prioritaire de constitutionnalité. Cette question a été posée pour M. Lotfi H. par Me Raphaël Chiche, avocat au barreau de Paris. Elle a été enregistrée au secrétariat général du Conseil constitutionnel sous le n° 2022-993 QPC. Elle est relative à la conformité aux droits et libertés que la Constitution garantit des articles 60-1 et 60-2 du code de procédure pénale, dans leur rédaction résultant de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

Au vu des textes suivants :

- la Constitution ;
- l'ordonnance n° 58-1067 du 7 novembre 1958 portant loi organique sur le Conseil constitutionnel ;
- le code de procédure pénale ;
- la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice ;
- le règlement du 4 février 2010 sur la procédure suivie devant le Conseil constitutionnel pour les questions prioritaires de constitutionnalité ;

Au vu des pièces suivantes :

- les observations présentées pour le requérant par Me Bertrand Périer, avocat au Conseil d'Etat et à la Cour de cassation, et Me Chiche, enregistrées le 30 mars 2022 ;
- les observations présentées par le Premier ministre, enregistrées le même jour ;
- les observations en intervention présentées pour M. Ibrahim K. par Mes Périer et Chiche, enregistrées le même jour ;
- les autres pièces produites et jointes au dossier ;

Après avoir entendu Me Chiche, pour le requérant et la partie intervenante, et M. Antoine Pavageau, désigné par le Premier ministre, à l'audience publique du 10 mai 2022 ;

Et après avoir entendu le rapporteur ;

Le Conseil constitutionnel s'est fondé sur ce qui suit :

1. L'article 60-1 du code de procédure pénale, dans sa rédaction résultant de la loi du 23 mars 2019 mentionnée ci-dessus, prévoit :

« Le procureur de la République ou l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord.

« A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre à cette réquisition dans les meilleurs délais et s'il y a lieu selon les normes exigées est puni d'une amende de 3 750 euros.

« A peine de nullité, ne peuvent être versés au dossier les éléments obtenus par une réquisition prise en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse ».

2. L'article 60-2 du même code, dans sa rédaction résultant de la même loi, prévoit :

« Sur demande de l'officier de police judiciaire ou, sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa du 3° du II de l'article 8 et au 2° de l'article 67 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

« L'officier de police judiciaire, ou, sous le contrôle de ce dernier, l'agent de police judiciaire intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de

l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, 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.

« Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

« Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 euros.

« Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises ».

3. Le requérant, rejoint par la partie intervenante, reproche à ces dispositions de permettre au procureur de la République ou à l'officier de police judiciaire, dans le cadre d'une enquête de flagrance, de requérir la communication de données de connexion sans le contrôle préalable d'une juridiction indépendante. Il en résulterait une méconnaissance du droit au respect de la vie privée.

4. Par conséquent, la question prioritaire de constitutionnalité porte sur 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 60-1 du code de procédure pénale et sur les mots *« contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent »* figurant au premier alinéa de l'article 60-2 du même code.

5. Aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 : *« Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression »*. La liberté proclamée par cet article implique le droit au respect de la vie privée.

6. En vertu de l'article 34 de la Constitution, il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il lui incombe d'assurer la conciliation entre, d'une part, l'objectif de valeur constitutionnelle de recherche des auteurs d'infraction et, d'autre part, le droit au respect de la vie privée.

7. L'article 60-1 du code de procédure pénale permet au procureur de la République, à un officier de police judiciaire ou, sous le contrôle de ce dernier, à un agent de police judiciaire, dans le cadre d'une enquête de flagrance, de requérir par tout moyen des informations intéressant l'enquête 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.

8. L'article 60-2 du même code prévoit notamment que l'officier de police judiciaire ou, sous le contrôle de ce dernier, 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 utiles à la manifestation de la vérité non protégées par un secret prévu par la loi, contenues dans un système informatique ou un traitement de données nominatives.

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

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

11. En premier lieu, en adoptant les dispositions contestées, le législateur a poursuivi l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions.

12. En deuxième lieu, d'une part, ces dispositions ne permettent les réquisitions de données que dans le cadre d'une enquête de police portant sur un crime flagrant ou un délit flagrant puni d'une peine d'emprisonnement. D'autre part, la durée de cette enquête est limitée à huit jours. Elle ne peut être prolongée, pour une nouvelle durée maximale de huit jours, sur décision du procureur de la République, que si l'enquête porte sur un crime ou un délit puni d'une peine d'emprisonnement égale ou supérieure à cinq ans et si les investigations ne peuvent être différées.

13. En dernier lieu, ces réquisitions ne peuvent intervenir qu'à l'initiative du procureur de la République, d'un officier de police judiciaire ou, sous le contrôle de ce dernier, d'un agent de police judiciaire. Ces officiers et agents étant placés sous la direction du procureur de la République, les réquisitions sont mises en œuvre sous le contrôle d'un magistrat de l'ordre judiciaire auquel il revient, en application de l'article 39-3 du code de procédure pénale, de contrôler la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits.

14. Dès lors, les dispositions contestées opèrent une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée.

15. Par conséquent, ces dispositions, qui ne méconnaissent aucun autre droit ou liberté que la Constitution garantit, doivent être déclarées conformes à la Constitution.

Le Conseil constitutionnel décide :

Art. 1er. – 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 60-1 du code de procédure pénale, dans sa rédaction résultant de la loi nº 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, et les mots *« contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent »* figurant au premier alinéa de l'article 60-2 du même code, dans sa rédaction résultant de la même loi, sont conformes à la Constitution.

Art. 2. – Cette décision sera publiée au *Journal officiel* de la République française et notifiée dans les conditions prévues à l'article 23-11 de l'ordonnance du 7 novembre 1958 susvisée.

Jugé par le Conseil constitutionnel dans sa séance du 19 mai 2022, où siégeaient : M. Laurent FABIUS, Président, Mme Jacqueline GOURAULT, M. Alain JUPPÉ, Mmes Corinne LUQUIENS, Véronique MALBEC, MM. Jacques MÉZARD, François PILLET et François SÉNERS.

Rendu public le 20 mai 2022.

DOCUMENT 6

Enquêtes pénales : conservation et accès aux données de connexion

Pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652

La Cour de cassation tire les conséquences des décisions rendues par la Cour de justice de l'Union européenne relatives à la conservation des données de connexion et à l'accès à celles-ci dans le cadre de procédures pénales.

Avertissement *: le communiqué n'a pas vocation à exposer dans son intégralité la teneur des arrêts rendus. Il tend à présenter de façon synthétique leurs apports juridiques principaux.*

Droit de l'Union européenne : protection de la vie privée, des données personnelles et de la liberté d'expression

La règle

Les États membres de l'Union européenne ne peuvent imposer aux opérateurs de communications électroniques, fournisseurs d'accès à internet et hébergeurs, une conservation généralisée et indifférenciée de l'ensemble des données de trafic et de localisation.

Des exceptions

Cette **conservation** peut avoir lieu, sous certaines conditions, en cas de menace grave et actuelle pour la sécurité nationale.

Afin d'élucider une infraction déterminée relevant de la criminalité grave, les États membres peuvent également imposer aux opérateurs et fournisseurs de procéder à la **conservation « *rapide* »** des données, s'ils entourent cette obligation d'un certain nombre de garanties.

L'accès aux données conservées doit, en tout état de cause, être autorisé par une juridiction ou une entité administrative indépendante.

De quelles données de connexion parle-t-on ici ?

Il s'agit des :

- **données de trafic**, qui établissent les contacts qu'une personne a eus par téléphone ou SMS / la date et l'heure de ces contacts / la durée de l'échange ;
- **données de localisation**, qui permettent de : connaître les zones d'émission et de réception d'une communication passée avec un téléphone mobile identifié / obtenir la liste des appels ayant borné à la même antenne relais.

Ces données sont accessibles sur les « *fadettes* ».

Repère :

Selon la Cour de justice de l'Union européenne (CJUE), ces données sont « susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé [...].

Prises dans leur ensemble, **lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes** dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. »

Les faits et la procédure

Dans plusieurs affaires, notamment de meurtre ou de trafic de stupéfiants, des personnes mises en examen ont demandé **l'annulation des réquisitions** portant sur leurs données de trafic et de localisation, délivrées par des enquêteurs agissant en enquête de flagrance sous le contrôle du procureur de la République ou sur commission rogatoire du juge d'instruction, ainsi que des actes d'**exploitation de ces données**.

Selon les requérants, ces données avaient fait l'objet :

- d'une conservation irrégulière car la législation française alors en vigueur imposait aux opérateurs de conserver pendant un an l'ensemble des données de connexion pour la recherche de toutes les infractions pénales ;

- d'un accès irrégulier car ces données personnelles ont été obtenues par les enquêteurs avec l'autorisation du procureur de la République ou du juge d'instruction, qui ne sont ni une juridiction ni une entité administrative indépendante.

Les **principes**

Repère :

Afin de garantir l'effectivité du droit de l'Union au sein des différents Etats membres, le juge national doit interpréter le droit français de manière conforme au droit de l'Union.

À défaut de pouvoir procéder à une telle interprétation conforme, le juge national est tenu de laisser inappliquées les règles de droit français contraires au droit de l'Union.

Si le juge ne respecte pas la législation de l'Union européenne, il expose l'Etat à un recours en manquement.

Conservation générale des données de trafic et de localisation (régime antérieur à la loi du 30 juillet 2021)

La sauvegarde de la sécurité nationale permettait une conservation générale et indifférenciée des données.

La réglementation française en ce qu'elle prévoyait la conservation générale des données de connexion pour la **protection des intérêts fondamentaux de la Nation** et la **lutte contre le terrorisme** était conforme au droit de l'Union, sous réserve d'un réexamen périodique de l'existence d'une menace grave pour la sécurité nationale.

Dans les affaires examinées, une menace pour la sécurité de la Nation existait avant les faits : c'est ce qui ressort des pièces produites par le procureur général près la Cour de cassation relatives aux **attentats commis en France depuis décembre 1994**. La durée de conservation pendant un an est jugée strictement nécessaire à la sauvegarde de la sécurité nationale.

En revanche, la **conservation générale à d'autres fins** était contraire au droit de l'Union.

Il était possible de procéder, par voie de réquisitions, à la conservation « rapide » des données pour élucider une infraction grave et dans les limites de la stricte nécessité : le juge saisi d'une contestation doit s'assurer de cette nécessité.

Les données conservées par les opérateurs pour leurs besoins propres ou au titre de sauvegarde de la sécurité nationale, peuvent l'être également, à la demande des enquêteurs, par voie de réquisitions, pour la répression d'une infraction grave déterminée.

Les réquisitions valent alors **injonction de conservation « *rapide* »**.

Afin de s'assurer du respect du droit de l'Union, lorsqu'il est saisi d'un moyen de nullité critiquant la régularité des réquisitions, **le juge doit vérifier** que :

- les faits en cause relèvent de la **criminalité grave** ;

- la conservation « *rapide* » des données de connexion et l'accès à celles-ci respectent les limites du **strict nécessaire**.

Accès aux données de trafic et de localisation

Le juge d'instruction, qui est une juridiction, peut contrôler l'accès aux données ; le procureur de la République, qui n'est pas un tiers dans les enquêtes, ne peut y procéder.

La loi en ce qu'elle permet au **procureur de la République**, ou à un **enquêteur**, d'accéder aux données est contraire au droit de l'Union car elle ne prévoit **pas un contrôle préalable par une juridiction ou une entité administrative indépendante**.

Le procureur de la République dirige la procédure d'enquête et exerce, le cas échéant, l'action publique : il est ainsi impliqué dans la conduite de l'enquête pénale et n'a pas une position de neutralité vis-à-vis des parties à la procédure pénale, comme l'exige le droit de l'Union.

En revanche, **le juge d'instruction est habilité** à exercer ce contrôle, puisqu'il n'est pas une partie à la procédure mais une **juridiction** et qu'il n'exerce pas l'action publique.

Par conséquent, la personne mise en examen peut, sous certaines conditions, invoquer la violation de l'exigence de contrôle indépendant de l'accès à ses données de connexion.

L'acte ayant permis d'accéder aux données ne peut être annulé par le juge que s'il a été porté atteinte à la vie privée de la personne mise en examen et si celle-ci a subi un préjudice.

La Cour de cassation précise les **conséquences d'un accès irrégulier aux données** de connexion sur la validité des actes d'enquête :

- La loi donne à la personne mise en examen la possibilité de contester efficacement la pertinence des preuves tirées de ses données, en particulier dans le cadre d'une demande d'expertise.
- Le droit de l'Union cherche à protéger la vie privée : ne pas le respecter revient à porter atteinte à un intérêt privé. Dès lors, la personne mise en examen ne peut invoquer la violation des exigences en matière de contrôle de l'accès aux données que si elle prétend être **titulaire ou utilisatrice d'une ligne identifiée** ou si elle démontre qu'à l'occasion de ces investigations, il a été porté **atteinte à sa vie privée**.
- Le juge pénal ne peut annuler les actes ayant permis d'accéder aux données que si l'irrégularité constatée a occasionné un **préjudice à la personne mise en examen**. Ce préjudice est établi :
- lorsque les données ne pouvaient être conservées au titre de la conservation « *rapide* » ;
- *ou* lorsque les catégories de données visées et la durée pendant laquelle il a été possible d'y avoir accès n'étaient pas limitées à ce qui était **strictement nécessaire** au bon déroulement de l'enquête en cause.

Les conséquences dans les affaires examinées

Dans les affaires pour lesquelles les personnes mises en examen n'avaient aucun droit sur les lignes téléphoniques, les requêtes en nullité sont jugées **irrecevables**.

Dans les affaires pour lesquelles les personnes mises en examen avaient un droit sur les lignes téléphoniques, **les pourvois sont rejetés** car :

1. Les données de connexion ont été **régulièrement conservées** dès lors que les faits relevaient bien de la **criminalité grave** (meurtre en bande organisée, destruction par moyen dangereux, importations et exportations de centaines de kilos de stupéfiants par organisation criminelle de dimension internationale etc.), et que les réquisitions aux opérateurs des données de connexion (identité, trafic, localisation) et leur exploitation étaient nécessaires au bon déroulement des enquêtes.
2. **L'accès** par des enquêteurs ayant agi sur commission rogatoire du juge d'instruction a été régulièrement accordé.
3. Bien que des enquêteurs ont eu **irrégulièrement accès** aux données de trafic et de localisation dans le cadre d'une enquête de flagrance menée sous le contrôle du procureur de la République, la chambre de l'instruction a valablement pu rejeter les demandes de nullité, car, **en l'espèce**, les catégories de données visées et la durée pendant laquelle il a été possible d'y avoir accès étaient limitées à ce qui était **strictement nécessaire au bon déroulement de l'enquête**.

DOCUMENT 7

AJ Pénal 2022 p.392 - Évolution normative et jurisprudentielle sur le thème des métadonnées
Thomas Lebreton, Substitut du procureur au parquet de Nanterre

L'essentiel

Le présent dossier (trois articles) examine l'évolution normative et jurisprudentielle au terme de laquelle la Cour de cassation a rendu ses quatre arrêts majeurs du 12 juillet 2022, ses conséquences pratiques et les solutions envisageables pour reformer, conformément au droit européen, la législation relative à l'accès et à la conservation des données dites de connexion. Pour une bonne compréhension du dossier, nous vous conseillons de prendre également connaissance du commentaire des arrêts du 12 juillet (v. infra, p. 413).

Les métadonnées, appelées « données de connexion » pour les distinguer des données de contenu, ont pris une importance dans l'élucidation des enquêtes pénales qui ne sera jamais suffisamment soulignée. Elles correspondent aux données :
- d'identité, lesquelles permettent, notamment, d'identifier le titulaire d'une carte SIM, d'une adresse IP ou d'une adresse mail ;
- de trafic, qui établissent les contacts qu'une personne a eus ainsi que la date, l'heure et la durée de l'échange (fadettes) ;
- de localisation, lesquelles désignent les zones d'émission et de réception d'une communication et visent les appels émis ou reçus par le biais d'une antenne-relais déterminée (bornage).

L'encadrement textuel de la conservation et de l'accès aux métadonnées par les autorités a conduit les juridictions suprêmes, européennes et internes, toutes réunies dans leurs formations les plus solennelles, à rendre ces dix dernières années des décisions majeures qui ont suscité une réaction des pouvoirs normatifs.

1. Encadrement normatif

Droit interne (conservation des métadonnées). La conservation des métadonnées est régie par l'article L. 34-1 du code des postes et des communications électroniques (CPCE). Dans sa version issue de la loi n° 2013-1168 du 18 décembre 2013, cet article faisait obligation aux opérateurs d'effacer et d'anonymiser les métadonnées (§ II) mais prévoyait deux exceptions :
- les opérateurs devaient conserver ces données pendant une durée d'un an pour les « besoins de la recherche, de la constatation et de la poursuite des infractions pénales »(§ III) ;
- les opérateurs étaient admis à conserver ces données, pendant un certain temps, pour leurs propres besoins (§ IV).

Droit interne (accès aux métadonnées). L'accès aux métadonnées se fait par le biais de réquisitions adressées à l'opérateur de télécommunications concerné, à savoir le fournisseur d'accès à internet ou l'opérateur téléphonique. Les réquisitions sont fondées sur les articles :
- 60-1 et 60-2 du code de procédure pénale dans le cadre d'une enquête de flagrance, dispositions permettant aux officiers de police judiciaire (OPJ), aux agents de police judiciaire (APJ), sous le contrôle de ces derniers, et au parquet d'émettre de telles réquisitions ;
- 77-1-1 et 77-1-2 du code de procédure pénale en préliminaire, lesquels supposent une intervention du procureur ;
- 99-3 et 99-4 du code de procédure pénale au cours de l'instruction, lesquels confient ce pouvoir aux magistrats instructeurs et aux forces de l'ordre en exécution d'une commission rogatoire.

Le législateur a par ailleurs largement étendu les possibilités d'accès à ces données au bénéfice de diverses administrations et autorités chargées de certaines fonctions de police judiciaire.

Droit européen (conservation des métadonnées). La directive 2002/58/CE du 12 juillet 2002, dite directive Vie privée et communications électroniques ou directive e-Privacy, interdit aux opérateurs de stocker les métadonnées et leur fait obligation de les effacer ou de les anonymiser (art. 5, § 1 et 6, § 1). Toutefois, il est prévu que les opérateurs puissent les conserver pour leurs propres besoins (art. 6, §§ 2 et 3) et que les États puissent déroger à cette interdiction en imposant aux opérateurs une conservation des données, pendant une durée limitée, aux fins de sauvegarder la sécurité nationale, la défense et la sécurité publique, ou pour assurer « la prévention, la recherche, la détection et la poursuite d'infractions pénales » (art. 15, § 1).

Poursuivant l'objectif d'uniformiser les dispositifs nationaux de conservation des données de connexion, la directive 2006/24/CE du 15 mars 2006, en son article 6, a transformé l'exception de l'article 15, §1, de la directive précitée en obligation pour les États membres d'imposer aux opérateurs la conservation de toutes les données de trafic pour une durée comprise entre six mois et deux ans au maximum.

Droit européen (exploitation des métadonnées). Le règlement général sur la protection des données (RGPD) prévoit que les données à caractère personnel collectées pour des finalités déterminées, explicites et légitimes, ne peuvent être ultérieurement traitées d'une manière incompatible avec ces finalités (art. 5, 1, b). Des exceptions poursuivant des objectifs de nature pénale sont toutefois admises (art. 23).

2. Évolution jurisprudentielle

CJUE 8 avr. 2014, aff. jtes C-293/12 et C-594/12, *Digital Rights Ireland Ltd*. Estimant disproportionnée l'atteinte d'une conservation généralisée des données à la vie privée des individus et au droit à la protection des données personnelles, la CJUE, par cet arrêt précurseur, annule la directive 2006/24/CE.

Cons. const. 5 août 2015, n° 2015-715 DC, ***Loi pour la croissance, l'activité et l'égalité des chances économiques***. Après avoir longtemps jugé l'inverse, le Conseil constitutionnel juge que la possibilité d'accès aux métadonnées offerte aux administrations et autorités doit être entourée de garanties.

CE 12 févr. 2016, n° 388134 , *Association French Data Network et autres*. Le Conseil d'État eu égard aux garanties supplémentaires offertes par le droit interne, adopte une « interprétation souple » de la jurisprudence de la CJUE et juge la conservation indifférenciée des données conforme au droit de l'Union.

CJUE 21 déc. 2016, aff. jtes C-203/15 et C-698/15, ***Tele2 Sverige AB c/ Post-och telestyrelsen***. La CJUE interprète l'article 15, § 1, de la directive 2002/58/CE « à la lumière » des articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union et en déduit des conséquences tenant à la fois à la conservation et à l'accès aux données de connexion. Elle juge notamment que le droit dérivé s'oppose à ce qu'une législation nationale permette une conservation généralisée et indifférenciée des données de trafic et de localisation à des fins pénales. Elle juge également que l'accès à ces métadonnées les plus sensibles doit être limité à la seule lutte contre la criminalité « grave » et, sauf urgence, être préalablement soumis à une juridiction ou à une autorité administrative indépendante (pt. 125). Cet arrêt a, pour reprendre les termes d'Alexandre Lallet, rapporteur public au Conseil d'État, « suscité la sidération et la consternation parmi les autorités et professionnels concernés, en France comme à l'étranger. Peut-être serait-il plus juste, d'ailleurs, de parler d'un effet d'hallucination, à laquelle les intéressés n'ont pas voulu croire : car, paradoxalement, aucune conséquence concrète n'en a été tirée en France depuis 2016, ni par le législateur, qui a continué à étendre les droits d'accès comme si de rien n'était, ni par l'autorité judiciaire ».

CEDH 8 mai 2018, n° 31446/12, *Ben Faiza c/ France*. Dans le cadre d'une enquête portant sur un trafic de stupéfiants au cours de laquelle des réquisitions aux fins d'obtention de métadonnées avaient été émises, la CEDH a reconnu la nécessité de l'ingérence et a considéré que les réquisitions, adressées à un opérateur de téléphonie sur le fondement de l'article 77-1-1 du code de procédure pénale, n'avaient pas violé l'article 8 de la Convention européenne des droits de l'homme.

CJUE 2 oct. 2018, aff. C-207/16 , *Ministerio fiscal*. La CJUE juge que si les infractions graves peuvent seules justifier une ingérence grave et donc un accès aux métadonnées sensibles, les infractions pénales d'une gravité moindre peuvent justifier un accès aux données peu sensibles.

CJUE 6 oct. 2020, aff. jtes C-511/18, C-512/18, C-520/18, La Quadrature du Net et autres. Notamment saisie par une question préjudicielle du Conseil d'État, la CJUE opère une appréciation différenciée selon les métadonnées concernées :
- les données les plus sensibles, que sont les données de trafic et de localisation, peuvent donner lieu à une conservation :

• généralisée et indifférenciée, mais uniquement en vue de sauvegarder la sécurité nationale, c'est-à-dire pour lutter contre les activités susceptibles de déstabiliser les structures mêmes d'un État, et constituant une menace grave, réelle et actuelle ou prévisible. La décision de recourir à une telle conservation, d'une durée limitée mais renouvelable, doit pouvoir faire l'objet d'un recours devant une juridiction ou une entité administrative indépendante,

• ciblée, eu égard aux personnes ou aux lieux concernés, sur la base d'éléments objectifs et non discriminatoires, lorsqu'elles sont utiles à la lutte contre la criminalité grave. Cette conservation est d'une durée strictement nécessaire ;

- les données relatives aux adresses IP attribuées à la source d'une connexion peuvent donner lieu à une conservation généralisée et indifférenciée aux fins de lutter contre la criminalité grave. La durée de conservation doit toutefois être temporellement limitée au strict nécessaire ;

- les données les moins sensibles, à savoir celles relatives à l'identité civile des utilisateurs, peuvent donner lieu à une conservation généralisée et indifférenciée aux fins de prévention, de recherche, de détection et de poursuite d'infractions pénales en général.

Le CJUE décide ainsi qu'une législation ne peut prévoir, à titre préventif, la conservation généralisée et indifférenciée des données de trafic et de localisation aux fins de lutte contre la criminalité quel que soit son degré de gravité. Toutefois, elle admet qu'une législation nationale puisse prévoir qu'une autorité confrontée à une situation dans laquelle il importe de conserver des données aux fins d'élucidation d'infractions pénales graves, puisse, en se soumettant à un contrôle juridictionnel effectif a posteriori, émettre une injonction de conservation rapide de données de connexion alors stockées (pts. 160 à 166). Émise à destination des opérateurs, cette demande vise à les enjoindre de conserver temporairement des données ciblées, déjà conservées pour un autre motif, aux fins de divulgation à une autorité (elle constitue donc une décision distincte de celle d'accès). Outre celles du suspect, peuvent être ciblées les données d'autres personnes (l'entourage social et professionnel du suspect, les victimes, etc.) et même de zones géographiques déterminées (lieu de commission ou de préparation de l'infraction) dès lors qu'elles apparaissent utiles à la manifestation de la vérité.

CJUE 2 mars 2021, aff. C-746/18 , *H.K. / Prokuratuur* . Sur question préjudicielle de la Cour suprême d'Estonie, la CJUE dit pour droit que le procureur, « 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 », est « impliqué [...] dans la conduite de l'enquête pénale » et n'a ainsi pas « une position de neutralité ». Faute d'être objectivement impartial, il ne peut autoriser les forces de l'ordre à accéder aux données de trafic et de localisation ni y accéder lui-même directement. Si le parquet n'est évidemment pas une juridiction, il n'est donc pas non plus une « entité administrative indépendante » au sens du droit de l'UE. Cette solution ne manque pas de surprendre dans la mesure où la CJUE a jugé, quinze mois plus tôt, que le parquet français répond aux exigences requises pour décerner des mandats d'arrêt européens considérant que ses membres, libres « d'apprécier de manière indépendante » la nécessité d'en émettre, constituent bien des « autorités judiciaires d'émission ».
(…)
Cons. const. 20 mai 2022 n° 2022-993 QPC. Le Conseil juge les articles 60-1 et 60-2 du code de procédure pénale conformes au bloc de constitutionnalité eu égard à l'encadrement, quant à leur durée et la gravité des faits poursuivis, des enquêtes de flagrance et de l'intervention du parquet, magistrat de l'ordre judiciaire, chargé d'apprécier la proportionnalité des actes d'enquête aux faits. Il fait ici primer les objectifs de valeur constitutionnels précités sur le principe, lui aussi constitutionnel, de primauté du droit de l'Union qui aurait imposé de prendre en compte la jurisprudence de la CJUE. Prévisible, cette décision révèle une opposition entre le Conseil constitutionnel et la CJUE.

3. Réaction des pouvoirs normatifs (…)
Accès aux données de connexion. Tirant les conséquences de la jurisprudence du Conseil constitutionnel plus qu'elle ne prend en compte celle de la CJUE, la loi n° 2022-299 du 2 mars 2022 a créé, sur amendement sénatorial, l'article 60-1-2 du code de procédure pénale. S'il ne modifie pas les acteurs pouvant émettre des réquisitions, cet article limite, pour l'essentiel et à peine de nullité, l'accès aux principales métadonnées pour les besoins des seules enquêtes portant sur des infractions punies d'au moins trois ans d'emprisonnement.

DACG FOCUS

Fiche criminologique, juridique ou technique

LES DONNEES DE TRAFIC ET DE LOCALISATION PENDANT L'ENQUETE PENALE

Juillet 2022

Le présent focus a pour objet d'exposer les règles applicables à la conservation et à l'accès aux données de trafic et de localisation pour les besoins des enquêtes pénales qui résultent du droit européen et droit interne tels qu'interprétés par la Cour de justice de l'Union européenne[1] et la Cour de cassation[2].

Les données de trafic et de localisation correspondent essentiellement aux éléments contenus dans la facturation détaillée établie par les opérateurs de téléphonie, à savoir la liste des communications émises ou reçues depuis la ligne concernée et des connexions à internet, leur date et leur durée ainsi que la localisation des équipements terminaux au moment de ces communications ou encore le détail des communications localisées à partir d'une antenne relais identifiée (FADETS).

Ce focus ne concerne pas les conditions de conservation et d'accès relatives aux autres données de connexion (données d'identité, adresse IP, numéro IMEI, etc.).

1. S'agissant de la conservation des données de trafic et de localisation :

Les opérateurs de communications électroniques ont l'obligation de conserver les données de trafic et de localisation pour les besoins du renseignement en application du III de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) et du décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion[3].

Pour la lutte contre la criminalité grave, l'autorité judiciaire peut demander **un gel des données** que détiennent les opérateurs pour les besoins du renseignement en application des dispositions mentionnées ci-dessus (méthode de la conservation rapide). L'injonction de conservation rapide a pour objet d'ajouter, pour les besoins des enquêtes pénales, la criminalité grave aux finalités initiales pour lesquelles les données de trafic et de

[1] Notamment les décisions Télé2Sverige du 21 décembre 2016 (C-203-15), La Quadrature du Net et autres du 6 octobre 2020 (C-511/18 et 512/18), Prokuratuur du 2 mars 2021 (C-746/18).
[2] Cass. crim., 12 juillet 2022, n° 21-83.710, n° 21-83.820, n° 21-84.096, n° 20-86.652. Ces arrêts sont accompagnés d'une note explicative. Ces arrêts ont fait l'objet d'une présentation dans la dépêche du 13 juillet 2022.
[3] Le III de l'article L. 34-1 du code des postes et des communications électroniques permet au Premier ministre d'enjoindre par décret aux opérateurs de communications électroniques, pour des motifs tenant à la sauvegarde de la sécurité nationale et lorsqu'une menace grave, actuelle ou prévisible contre cette dernière est constatée, de conserver pour une durée d'un an certaines catégories de données de trafic et de localisation.

localisation sont conservées par les opérateurs et de permettre ainsi d'y accéder. **Les dispositions du code de procédure pénale relatives aux réquisitions de produire les données de connexion[4] constituent des injonctions de conservation rapide**.

2. **S'agissant de l'accès aux données de trafic et de localisation :**

Il convient d'opérer une distinction selon le cadre d'enquête :

- Dans le cadre d'une information judiciaire : les réquisitions peuvent être délivrées aux opérateurs de communications électroniques en application des articles 99-3 et 99-4 du code de procédure pénale lorsque la gravité de l'infraction et les nécessités de l'enquête l'exigent ;

- Dans le cadre d'une enquête préliminaire et d'une enquête de flagrance : les réquisitions peuvent être délivrées aux opérateurs de communications électroniques lorsque la gravité de l'infraction et les nécessités de l'enquête l'exigent, sous le contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

  Les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale relatifs aux réquisitions dans le cadre de l'enquête de flagrance et de l'enquête préliminaire ne prévoient pas un tel contrôle préalable et il n'est pas envisageable d'en créer un de façon prétorienne.

  Toutefois, cela ne signifie pas que la délivrance des réquisitions selon les modalités existantes (c'est-à-dire sans le contrôle préalable exigé par le droit européen) est interdite.

  En effet, l'absence de contrôle préalable sur de tels actes d'enquête par une autorité indépendante et impartiale n'encourt l'annulation que si la personne concernée peut se prévaloir d'un grief, c'est-à-dire d'une atteinte injustifiée au droit au respect de sa vie privée. Tel n'est pas le cas lorsque, au regard de la gravité de l'infraction et des nécessités de l'enquête, l'accès aux données de connexion apparaît justifié. Il revient donc aux juridictions d'instruction et de jugement de contrôler *a posteriori* le caractère nécessaire et proportionné des réquisitions délivrées pendant les enquêtes préliminaires et de flagrance, en application de l'article préliminaire du code de procédure pénale.

  Il appartient donc aux magistrats du parquet de s'assurer *in concreto* que de telles réquisitions sont réservées uniquement aux affaires relevant de la criminalité grave.

Ainsi, qu'il s'agisse d'une information judiciaire, d'une enquête préliminaire ou de flagrance, les réquisitions sont possibles pour les affaires relevant de la criminalité grave.

[4] Il s'agit des articles 60-1 et 60-2 du code de procédure pénale dans le cadre d'une enquête préliminaire, 77-1-1 et 77-1-2 dans le cadre d'une enquête de flagrance ainsi que 99-3 et 99-4 dans le cadre d'une information judiciaire.

Il convient de rappeler que l'article 60-1-2 du code de procédure pénale ne permet d'accéder aux données de trafic et de localisation pendant une enquête pénale que dans les cas suivants :

- La procédure porte sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement[5] ;
- La procédure porte sur un délit puni d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques ;
- La procédure porte sur un délit puni d'une peine d'emprisonnement si les réquisitions concernent les équipements terminaux de la victime et interviennent à sa demande ;
- La procédure est relative à une enquête tendant à rechercher une personne disparue ou à retracer un parcours criminel.

L'appréciation du caractère grave de la criminalité, exigé par la jurisprudence, peut résulter d'autres éléments que le seul respect des exigences légales de l'article 60-1-2 du code de procédure pénale.

Une telle appréciation doit également être effectuée au regard de la nature des agissements de la personne mise en cause, de l'importance du dommage qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue. Ces critères constituent un faisceau d'indices et ne doivent pas être interprétés comme étant cumulatifs.

A titre d'exemple, le critère de la criminalité grave apparaît satisfait dès lors que la procédure porte sur un crime, un délit d'atteinte aux personnes puni d'au moins 3 ans d'emprisonnement, une infraction relevant de la criminalité et de la délinquance organisées.

[5] Comme indiqué dans la dépêche du 25 février 2022, le seuil de 3 ans est également applicable aux procédures de recherche d'une personne en fuite (article 74-2 du code de procédure pénale). En revanche, les réquisitions portant sur les données de trafic et de localisation sont interdites pour les enquêtes en recherche des causes de la mort ou des blessures suspectes (article 74 du code de procédure pénale).

SOCIÉTÉ • VIE PRIVÉE

Données téléphoniques : les procureurs dénoncent des « obstacles majeurs » à la conduite des enquêtes

La chambre criminelle de la Cour de cassation a rendu quatre arrêts tirant les conséquences des décisions rendues ces dernières années par la Cour de justice de l'Union européenne et encadrant les réquisitions téléphoniques.

Par Thomas Saintourens et Simon Piel

Publié le 19 juillet 2022 à 09h35, mis à jour le 19 juillet 2022 à 09h36 • Lecture 3 min.

Article réservé aux abonnés

Le dialogue des juges sur la conservation et la saisie des données téléphoniques en matière d'enquête pénale se poursuit. Mercredi 13 juillet, la chambre criminelle de la Cour de cassation a rendu quatre arrêts tirant les conséquences des décisions rendues ces dernières années par la Cour de justice de l'Union européenne. Celle-ci avait jugé contraire au droit de l'Union européenne (UE) la conservation généralisée et indifférenciée des données de connexion (liste des appels entrants et sortants d'un téléphone, géolocalisation, adresses IP, liste des sites Internet consultés, etc.) opérée pour les besoins des services de renseignement et les enquêtes judiciaires.

Sans remettre en cause la conservation des données, la Cour de cassation précise qui est légitime à les demander en matière de *« criminalité grave »* et qui ne l'est pas. *« L'accès aux données conservées doit, en tout état de cause, être autorisé par une juridiction ou une entité administrative indépendante »*, dit-elle, ajoutant que *« la loi française en ce qu'elle permet au procureur de la République, ou à un enquêteur, d'accéder aux données est contraire au droit de l'Union car elle ne prévoit pas un contrôle préalable par une juridiction ou une entité administrative indépendante. »*

Lire aussi : Le Conseil constitutionnel censure la conservation généralisée des données de connexion

Dans un communiqué publié vendredi, la Conférence nationale des procureurs a déploré que ces arrêts créent une *« insécurité juridique majeure à laquelle doit faire face la lutte contre toutes les formes de délinquance »* et autant *« d'obstacles majeurs à l'identification des délinquants et des criminels »*. Elle compare le procureur *« au médecin à qui l'on demande de lutter contre des maladies de plus en plus sophistiquées et dangereuses, et qui ne peut plus utiliser de scanner pour les diagnostiquer et les traiter »*.

Une réaction quelque peu exagérée, estime-t-on dans les couloirs de la direction des affaires criminelles et des grâces (DACG) où l'on tient à souligner que les procureurs pourront toujours utiliser les données téléphoniques pour leurs enquêtes mais de façon plus encadrée.

« L'enjeu, ce n'est pas le rôle du parquet. Cela va bien au-delà. L'enjeu, c'est la lutte contre la délinquance. Est-ce qu'un ex-mari qui harcèle son ex-compagne c'est de la criminalité grave ? Qu'est-ce que la criminalité grave ? », s'interroge Jean-Baptiste Bladier, procureur de Senlis et président de la Conférence nationale des procureurs. *« Dans mon ressort, plus de la moitié des dossiers reposent sur les données téléphoniques. Un vol, un cambriolage, ça commence par les investigations sur les antennes relais par exemple*, poursuit-il. *Le système judiciaire français est à des années-lumière d'être configuré pour appliquer ce que demande la Cour de cassation. Ce sera des dizaines, des centaines de réquisitions à faire auprès du juge des libertés et de la détention. »*

Lire aussi | Le Conseil d'Etat autorise la poursuite de la conservation généralisée des données

« Ni révolution ni coup de tonnerre »

« Même si on a le sentiment que la Cour de cassation a essayé de concilier des intérêts contradictoires, certains points-clés demeurent flous. Qu'est-ce que la "criminalité grave" ? Parle-t-on des meurtres, des viols, de la criminalité financière ou uniquement de la criminalité organisée ? (…) *Le juge d'instruction considéré comme une juridiction est préservé jusqu'ici, mais il est certain que ces évolutions risquent d'entraver le travail d'enquête et alourdiront le travail des parquetiers mais aussi des enquêteurs »*, réagit pour sa part auprès du *Monde* Marion Cackel, présidente de l'Association française des magistrats instructeurs.

La moue est de mise aussi du côté des défenseurs des libertés publiques, mais pour des raisons opposées. *« Juridiquement, cette décision était attendue, mais sur le contenu, il s'agit d'une énorme déception, ce texte est une hypocrisie*, dénonce Noémie Levain, juriste à La Quadrature du Net. *Dans les faits, on conserve préventivement la localisation des Français pendant un an… Tout le monde est suspect. »* Pour Nicolas Hervieu, juriste, collaborateur au cabinet d'avocats Spinosi et enseignant à Sciences Po, *« on est au cœur d'un conflit d'influence et de conception dans l'équilibre entre la protection des données personnelles et la lutte contre le crime. La décision est formellement respectueuse des exigences européennes, mais, en substance, elle les détourne. Il s'agit d'une interprétation à des fins de sauvetage du dispositif pénal français. Il s'agit d'un sauvetage des procédures en cours, et un moyen de ne pas empêcher celles à venir. »*

L'ancien président de la chambre criminelle de la Cour de cassation Didier Guérin tempère ces analyses. *« On ne peut pas faire procès à la Cour de cassation d'avoir voulu entraver le cours des enquêtes. Elle fait un état du droit compatible avec la loi actuelle. Elle ne pouvait pas faire autrement*, dit-il au *Monde*. *La Cour de cassation n'a, au fond, pris qu'une initiative qui consiste à décliner les conséquences de la jurisprudence européenne. La solution trouvée n'est pas complète mais c'est la solution du moment. C'est désormais au législateur de tirer éventuellement les conséquences de ces arrêts. »*

Clarisse Taron, procureure à Fort-de-France et ancienne présidente du Syndicat de la magistrature, n'est pas surprise par ces arrêts. *« Ce n'est ni une révolution ni un coup de tonnerre, car c'est conforme à ce que dit l'UE depuis plusieurs années sur le parquet à la française. »* Elle reconnaît toutefois une *« difficulté sur les enquêtes à venir »* et attend que la direction des affaires criminelles et des grâces (DACG) traduise dans une circulaire les applications concrètes de ces arrêts. Celle-ci devrait être envoyée ce mercredi.

Thomas Saintourens et **Simon Piel**