

**TOULOUSE
CAPITOLE**
Publications



« Toulouse Capitole Publications » est l'archive institutionnelle de
l'Université Toulouse 1 Capitole.

**Émission d'une décision d'enquête européenne visant à la transmission de données de
télécommunications possédées par l'État d'exécution : suffisance du contrôle du procureur**

Hélène Christodoulou

Pour toute question sur Toulouse Capitole Publications,
contacter portail-publi@ut-capitole.fr

**La suffisance du contrôle du procureur dans le cadre de l'émission d'une
décision d'enquête européenne visant à la transmission de données de
télécommunications déjà possédées par l'État d'exécution**

CJUE, 30 avril 2024, aff. C-670/22

Résumé : La Cour de Justice de l'Union européenne vient de préciser les conditions entourant la transmission et l'exploitation des preuves issues d'une décision d'enquête européenne. Alors qu'elle semblait jusqu'alors très méfiante à l'égard du procureur, elle lui permet de contrôler son émission en vue de la transmission de preuves déjà recueillies directement par l'État d'exécution, si le droit de l'État d'émission le prévoit et selon ses conditions. Un contrôle judiciaire ultérieur doit, néanmoins, garantir le respect des droits fondamentaux des personnes concernées. De surcroît, lorsqu'un État réalise une interception sur le territoire d'un autre, il est tenu de le lui notifier en s'adressant à toute autorité que l'État interceptant considère apte à cet effet. Enfin, le juge pénal doit, dans certaines circonstances, écarter des éléments de preuve si la personne concernée n'est pas en mesure de les commenter.

L'accès aux données de connexion - permise par la mise en œuvre de réquisitions - a fait l'objet d'une jurisprudence abondante et exigeante concernant les garanties que doit revêtir l'organe de contrôle de la mesure. En interprétant la directive « vie privée et communication électronique » (Dir. 2002/58/CE du 12 juillet 2002), la Cour de justice considère, en effet, que l'accès aux données de trafic et de localisation, en passant par un service de communication, doit nécessairement faire l'objet d'un contrôle par un juge ou une autorité administrative indépendante (CJUE, gde ch., 2 mars 2021, aff. C-746/18, *Prokuratuur*, §59) et non par un procureur et encore moins par la police (CJUE, gde ch., 5 avr. 2022, aff. C-140/20, *GD c/ Commissioner of An Garda Siochana*, §114).

Pour autant, elle semble infléchir sa jurisprudence, en interprétant la décision d'enquête européenne (Dir. 2014/41 du 3 avril 2014), lorsque la donnée demeure déjà en la possession des autorités compétentes de l'État d'exécution. Plus largement, dans cet arrêt en date du 30 avril 2024, elle précise les conditions entourant la transmission et l'utilisation des preuves issues d'une décision d'enquête européenne (ci-après DEE ; Dir. 2014/41/UE du parlement européen et du conseil concernant la DEE en matière pénale, 3 avr. 2014). Pour rappel, cet instrument de reconnaissance mutuelle, en matière pénale, permet la réalisation d'une ou plusieurs mesures

d'investigation au sein de l'État d'exécution en vue de recueillir des preuves, lesquelles peuvent déjà être possédées par ledit État (art. 1 § 1 de la directive DEE).

Lors d'une enquête, les autorités françaises ont découvert que des personnes poursuivies usaient de téléphones portables cryptés - dont les données sont insusceptibles d'être interceptées par des méthodes d'enquête traditionnelles - afin de commettre des infractions liées essentiellement au trafic de stupéfiants (§19). Avec l'autorisation d'un juge français, sur le fondement d'une technique spéciale d'enquête (CPP, art. 706-102-1), les données de 33 477 utilisateurs, répartis dans 122 pays, ont tout de même pu être sauvegardées à l'aide d'un logiciel de type « cheval de Troie » développé par une équipe commune d'enquête (§20). La collecte de ces données n'avait donc pas nécessité l'intervention d'un fournisseur de services. Les représentants des autorités allemandes, composés de l'Office fédéral de la police judiciaire (*Bundeskriminalamt*) et du parquet général de Francfort, ont, durant une vidéoconférence organisée par Eurojust, manifesté leur intérêt pour les données des 4 600 utilisateurs allemands (§21). Le parquet général de Francfort a, ensuite, ouvert une enquête contre X (§23) ; l'usage du service cryptant les données (EncroChat) permettait « de soupçonner la commission d'infractions graves » (§22). Sur le serveur d'Europol, les données étaient diffusées aux polices des États membres intéressés par ces dernières, mais pour être utilisées dans une procédure pénale une autorisation était nécessaire (§25). À ce titre, le parquet général de Francfort a émis plusieurs DEE. Le tribunal correctionnel de Lille les a donc exécutées en autorisant la police allemande à utiliser sans restriction les données issues du service EncroChat dans des procédures pénales au motif que les autorités policières allemandes avaient été informées par Europol qu'un grand nombre d'infractions très graves pouvaient être commises sur leur territoire par des personnes encore non identifiées (§§ 26 et 27).

Certaines procédures diligentées contre des utilisateurs connus ont été réattribuées à des parquets locaux. À ce titre, le tribunal régional de Berlin saisi (*Landgericht Berlin*) s'est interrogé sur la légalité des DEE émises par le parquet général de Francfort. Face aux doutes, en octobre 2022, il a donc posé de multiples questions préjudicielles - cinq principales se découpant en quatorze sous-interrogations - relatives à l'interprétation des dispositions de la directive 2014/41/UE (art. 1 § 1 ; art. 2, c) ; art. 6 § 1 ; art. 14 § 7 et art. 31) et des principes d'équivalence et d'effectivité (§54). Ces dernières peuvent être résumées synthétiquement ainsi : quelle autorité est d'une part, compétente pour émettre une DEE visant à la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution ; d'autre part,

notifiée de l'interception de la donnée ? Quel est l'objectif de cette notification envisagée par le droit dérivé ? À quelle condition la DEE peut-elle être émise ? Et enfin, dans quelle mesure les preuves obtenues à l'aide d'une DEE sont-elles recevables ?

La Cour de justice répond en cinq temps. Premièrement, les articles 1^{er} § 1 et 2 c) de la directive supposent que la DEE peut être émise par un procureur lorsque, en vertu du droit de l'État d'émission, dans une procédure exclusivement interne, il est compétent pour ordonner la transmission desdites preuves. Deuxièmement, l'article 6 § 1 dudit texte, ne s'oppose pas à ce qu'un procureur adopte une DEE qui vise à la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution, lorsque ces dernières ont été acquises à la suite de l'interception, par ces autorités, sur le territoire de l'État d'émission, si la décision respecte l'ensemble des conditions prévues, le cas échéant, par le droit de cet État pour la transmission de telles preuves dans une situation purement interne. Troisièmement, l'article 31, quant à lui, concerne l'hypothèse où l'État interceptant n'a pas la capacité d'identifier l'autorité compétente de l'État qui doit être notifié. La Cour considère donc que cette notification peut être adressée à toute autorité que l'État interceptant considère apte à cet effet. Cette disposition vise, quatrièmement, « à protéger les droits des utilisateurs concernés par une mesure d' « interception de télécommunications » ». Cinquièmement, l'article 14 § 7, « impose au juge pénal national d'écarter, dans le cadre d'une procédure pénale ouverte contre une personne soupçonnée d'actes de criminalité, des informations et des éléments de preuve si cette personne n'est pas en mesure de commenter efficacement ces informations ainsi que ces éléments de preuve et que ceux-ci sont susceptibles d'influencer de manière prépondérante l'appréciation des faits » (§132).

En somme, au sein de cet arrêt, la Cour de justice précise tant les conditions entourant l'émission d'une DEE que l'usage des données issues d'une telle mesure.

Les conditions entourant l'émission d'une DEE

La Cour de justice va déterminer l'autorité d'émission d'une DEE visant à la transmission d'une preuve déjà récoltée par l'État d'exécution, il en ressortira que le droit de l'État d'émission demeure prépondérant pour répondre à cette interrogation.

L'autorité d'émission d'une DEE visant à la transmission d'une preuve déjà récoltée

La DEE demeure un instrument de reconnaissance mutuelle. Ainsi, contrairement à l'harmonisation, elle ne modifie pas les droits nationaux, mais elle se superpose à eux dans le cadre d'enquêtes transfrontières au sein de l'Union européenne. Pour la première fois, au sein du droit dérivé, le législateur de l'Union européenne avait précisé la composition de l'autorité judiciaire d'émission d'une telle décision - « un juge, une juridiction, un juge d'instruction ou un procureur compétent(e) dans l'affaire concernée » (art. 2, c), i)) - ou toute autorité compétence sous son contrôle. Ainsi, à la lecture de la directive, il ne semble pas y avoir de difficulté à ce que la DEE soit émise par un procureur (§ 69 et s.).

Pour autant, la Cour de justice apporte de nouvelles précisions. À première vue, la détermination de l'autorité compétente pour émettre une DEE suppose d'identifier deux éléments : d'une part, son objet à savoir, la collecte ou la transmission considérée, quant à elle, comme moins attentatoire ; d'autre part, le droit de l'État d'émission. Ainsi, comme dans cet arrêt, la DEE avait pour but la simple transmission d'une preuve déjà récoltée, la mesure pouvait être émise par un procureur (§77). De surcroît, son droit national le lui permettait. En réalité, cette solution ne dépend pas vraiment de l'objet de la DEE - la collecte ou la transmission - comme il est possible de le déduire au départ, mais plutôt de l'intervention ou non d'un opérateur de télécommunications. En effet, cette jurisprudence doit être lu à la lumière d'autres arrêts au sein desquels la Cour de justice de l'Union, en interprétant la directive « vie privée et communications électroniques », précise que l'accès aux données de connexion suppose l'intervention d'un juge ou d'une autorité administrative indépendante. Ainsi, à l'aune du principe de primauté du droit de l'Union et de ses précédentes jurisprudences (CJUE, gde ch., 2 mars 2021, aff. C-746/18, *Prokuratuur* ; CJUE, 4^e ch., 16 dec. 2021, *Spetsializirana prokuratura c/ H. P.*, aff. C-724/19), une DEE exigeant leurs transmissions ou leurs collectes, en y associant un opérateur de télécommunications, suppose le contrôle préalable d'un juge, même si la législation française n'est toujours pas conforme (H. CHRISTODOULOU, « à technique de géolocalisation différente, organe de contrôle différent », Dr. Pen., n° 4, avril 2024, Comm.78). À l'inverse, si la transmission ou la collecte ne nécessite pas l'intervention d'un fournisseur de services, comme en l'espèce, la Cour de justice ne pourra pas imposer le contrôle d'un juge. Elle devra donc, dans cette hypothèse, s'en remettre au droit de l'État d'émission.

Le droit de l'État d'émission prépondérant dans la mise en œuvre d'une DEE

Les juges luxembourgeois poursuivent, cette fois, en interprétant l'article 6 § 1 de la directive, propre aux conditions d'émission et de transmission d'une DEE, et entérine la compétence du procureur sous conditions. Concrètement, ils rappellent les deux exigences, posées par le droit dérivé, que doit vérifier l'État d'émission à savoir, le respect : d'une part, des principes de nécessité et proportionnalité de la mesure aux finalités de la procédure compte tenu des droits du suspect ou de la personne poursuivie ; d'autre part, de son propre droit national (§87). Concernant la première condition, la Cour de justice considère que la directive « n'exige pas que l'émission d'une DEE visant la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution, soit nécessairement subordonnée à l'existence d'une présomption d'infraction grave fondée sur des faits concrets, contre chaque personne concernée, au moment où cette décision d'enquête européenne est ordonnée, lorsqu'une telle exigence ne découle pas du droit de l'État d'émission » (§89). Elle estime que les droits fondamentaux seront garantis au moment de la recevabilité de la preuve devant le juge de l'État d'émission (§103). Le contrôle de l'autorité judiciaire de l'État d'exécution demeure classiquement écarté afin que la décision puisse circuler au mieux.

Concernant la seconde condition, propre à l'organe compétent, le droit de l'État d'émission s'avère essentiel, comme elle le rappelle explicitement (§91 et s.). À ce titre, elle avait déjà apporté des précisions sur l'autorité d'émission d'une DEE en vue d'obtenir des données de connexion (H. CHRISTODOULOU, « Le rôle de l'autorité de poursuite suspendu aux juges de l'Union européenne », *Rev. de l'UE*, 2022, p. 353 et s.). Elle avait conclu que le ministère public bulgare ne pouvait pas l'émettre, car au regard du droit de cet État membre, dans une affaire nationale similaire, un juge ou une juridiction sont exclusivement compétents pour ordonner l'obtention de cette preuve (CJUE, 4^e ch., 16 dec. 2021, *Spetsializirana prokuratura c/ H. P.*, aff. C-724/19). Alors pourquoi la solution apparaît-elle différente à la lecture de ce nouvel arrêt rendu le 30 avril 2024 ? À la lumière des articles 1^{er}, § 1 et, 2 c) de la directive, la DEE ne doit pas nécessairement être prise par une autorité juridictionnelle lorsque, en vertu du droit de l'État d'émission, dans une procédure purement interne à cet État, la collecte initiale de ces preuves aurait dû être ordonnée par un juge, mais qu'un procureur est compétent pour ordonner la transmission desdites preuves (comme le prévoit l'article 100e, § 6, point 1 de la *StPO* - le CPP allemand) ; même dans l'hypothèse où il est un fonctionnaire subordonné au pouvoir exécutif comme en Allemagne. Si la Cour de justice ingère dans les droits nationaux concernant l'accès aux données de connexion, lorsqu'elle interprète la directive « communication électronique et vie privée », elle n'a aucune compétence pour rapprocher les droits nationaux concernant les conditions entourant la collecte ou la transmission de ces

données lorsque les opérateurs de télécommunications n'y sont pas associés. En l'espèce, comme les autorités nationales détenaient directement la donnée - en implantant un virus dans le système EncroChat, sans le soutien d'un fournisseur de services - les États membres demeuraient libres, sous réserve de respecter les termes de la directive relative à la DEE à savoir, son émission « par une juridiction, un juge, un juge d'instruction ou un procureur compétent(e) dans l'affaire concernée » ou par une autre autorité sous son contrôle.

Au-delà de la mise en œuvre des conditions entourant l'émission des DEE, elle se concentre sur la donnée transmise. Autrement dit sur la preuve exigée par l'autorité judiciaire d'émission.

L'usage des données issues d'une DEE

En l'espèce, les données demandées au sein des DEE étaient issues d'interceptions de télécommunications, par les autorités françaises, lesquelles demeurent soumises à un régime spécifique que la Cour de justice interprète avec souplesse. Une fois la preuve possédée par l'État d'émission, à la suite de l'exécution de la demande, elle pose des règles, finalement strictes, concernant la recevabilité des preuves devant la juridiction nationale.

La souplesse entourant la notification de l'interception des données

Le chapitre V de la directive relative à la DEE concerne spécifiquement « l'interception de télécommunications ». La Cour de justice a dû, à cet égard, interpréter l'article 31 propre à la « notification de l'État membre où se trouve la cible de l'interception et dont l'assistance technique n'est pas nécessaire ». Selon la juridiction de renvoi, lorsqu'un État membre, en l'occurrence la France, souhaite intercepter les télécommunications de personnes se trouvant sur le territoire allemand, il doit le notifier à l'autorité compétente de cet État avant le début de la mise en œuvre de la mesure ou dès qu'il a connaissance du lieu où se trouve cette personne (§§ 41 - 46). Avant de se prononcer, les juges luxembourgeois rappellent le caractère autonome de la notion de « télécommunication » (§109), renvoyant « dans son sens usuel à l'ensemble des procédés de transmission d'informations à distance » (§119). Ils concluent donc qu'il était bien question d'intercepter de telles données, lesquelles supposent la notification d'une autorité compétente de l'État sur le territoire duquel la donnée a été interceptée, autrement appelé « l'État membre notifié » (§115). Toutefois, par une interprétation souple, elle affirme que dans l'hypothèse où l'État interceptant n'est pas en mesure d'identifier l'autorité compétente de

l'État notifié, cette notification peut être adressée à toute autorité de cet État que l'État membre interceptant juge apte à cet effet (§119). Il apparaît, néanmoins, difficile d'imaginer que les autorités françaises ne connaissent pas le destinataire, Allemand, d'une telle notification dont l'objet est de « protéger les droits des utilisateurs concernés » (§125).

Une fois la DEE exécutée, qu'en est-il de la recevabilité des preuves devant la juridiction nationale de l'État d'émission ?

La rigidité entourant l'admissibilité des données devant la juridiction

Par sa cinquième question, la juridiction de renvoi interroge la Cour de justice sur le fait de savoir si le principe d'effectivité impose au juge pénal national d'écarter, dans le cadre d'une procédure pénale ouverte contre une personne soupçonnée d'actes de criminalité, des preuves qui ont été obtenues en méconnaissance du droit de l'Union (§126). La réponse à cette question ne s'impose, selon la Cour de justice, que dans l'hypothèse où la juridiction de renvoi aboutirait à la conclusion que les DEE ont été ordonnées illégalement (§127). En effet, les règles relatives à l'admissibilité et à l'appréciation des preuves relèvent « en principe » du seul droit national (§ 128 ; CJUE, 6 oct. 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, § 222). De surcroît, par une formule difficilement déchiffrable déjà employée par la Cour de justice (CJUE, gde ch., 2 mars 2021, aff. C-746/18, *Prokuratuur*, §59), elle rappelle que la directive « impose au juge pénal national d'écarter, dans le cadre d'une procédure pénale ouverte contre une personne soupçonnée d'actes de criminalité, des informations et des éléments de preuve si cette personne n'est pas en mesure de commenter efficacement ces informations ainsi que ces éléments de preuve et que ceux-ci sont susceptibles d'influencer de manière prépondérante l'appréciation des faits » (§131). Elle s'immisce donc, comme toujours, dans les droits nationaux en la matière alors qu'elle n'en a pas « en principe » la compétence et que la directive apparaît muette sur ce point. Cette dernière ne s'intéresse qu'aux recours et se contente d'opérer un renvoi aux droits nationaux (Art. 14 de la directive).

Quoi qu'il en soit la portée de cet arrêt doit être relativisée à l'aune de l'application, à partir du 18 août 2026, du règlement *e-evidence* (Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale). Ce dernier prévoit la possibilité pour une autorité judiciaire nationale

d'enjoindre directement à un fournisseur de services, situé dans un autre État membre, de conserver et de produire des données afin de faciliter la collecte et l'utilisation transfrontière des preuves numériques. Dès lors, la DEE ne devrait plus être utilisée pour la collecte ou la transmission de données quand elles nécessitent l'intervention d'un tel fournisseur. En revanche, elle perdurera dans l'hypothèse où elles seront collectées et/ou détenues directement par les autorités nationales comme en l'espèce. Le nouvel instrument détermine explicitement l'autorité judiciaire de l'injonction en fonction de la donnée demandée et de son objet. D'une part, les injonctions de production visant à obtenir des données propres aux abonnés ou dans l'unique but d'identifier l'utilisateur (art. 4 § 1 du règlement) et les injonctions de conservation, si les données de toute catégorie ont été recueillies en amont (art. 4 § 3 du règlement - reprend l'hypothèse de l'espèce) peuvent être émises ou contrôlées en amont par « un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée » (art. 4 § 1 du règlement), à moins d'une urgence justifiant un contrôle *a posteriori* dans un délai de quarante-huit heures (art. 4 § 5 du règlement). D'autre part, les injonctions de production visant à obtenir les seules données relatives au trafic ou au contenu (art. 4 § 2 du règlement), considérées comme plus sensibles, ne peuvent être émises que par une autorité juridictionnelle à savoir, « un juge, une juridiction ou un juge d'instruction compétents dans l'affaire concernée », excluant alors les Parquets nationaux, sans dérogation possible (V. H. CHRISTODOULOU, « L'injonction de production et de conservation des preuves électroniques : prémices d'un acte d'investigation de l'Union européenne », JCP G n° 36, sept. 2023, p. 1561 et s.). En somme, cette solution ne fait que reprendre les exigences du règlement *e-evidence*, la Cour de justice apparaît donc en symbiose avec le législateur de l'Union.