EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

CINQUIÈME SECTION

DÉCISION

Requêtes nos 44715/20 et 47930/21
A.L. contre la France
et E.J. contre la France

La Cour européenne des droits de l'homme (cinquième section), siégeant le 24 septembre 2024 en une chambre composée de :

Lado Chanturia*, président*,
Mattias Guyomar,
María Elósegui,
Kateřina Šimáčková,
Mykola Gnatovskyy,
Stéphane Pisani,
Úna Ní Raifeartaigh*, juges*,

et de Martina Keller, *greffière adjointe de section,*

les requêtes (nos 44715/20 et 47930/21) dirigées contre la République française et dont deux ressortissants britanniques, MM. A.L. et E.J., ont saisi la Cour en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention ») le 5 octobre 2020 et le 20 septembre 2021,

la décision de porter ces requêtes à la connaissance du gouvernement français (« le Gouvernement »),

la décision de ne pas dévoiler l'identité des requérants,

les observations communiquées par le gouvernement défendeur et celles communiquées en réplique par les requérants,

les commentaires du gouvernement britannique, qui a été invité à intervenir à l'instance (article 36 § 2 de la Convention et article 44 § 3, a) du Règlement),

Après en avoir délibéré, rend la décision suivante :

EN FAIT

1. Les deux requêtes portent sur la captation des données des utilisateurs de la solution de communication chiffrée EncroChat et sur leur partage avec les autorités répressives britanniques. Les requérants invoquent l'article 8, seul et combiné avec l'article 13, ainsi que l'article 6 de la Convention.

2. Les requérants sont respectivement nés en 1990 et en 1965 ont été représentés par M[e] B. Tsiattalou, avocat à Londres et Manchester. Ils sont tous deux incarcérés au Royaume-Uni.

3. Le Gouvernement a été représenté par son agent, M. F. Alabrune, directeur des affaires juridiques au ministère de l'Europe et des Affaires étrangères, puis par M. D. Colas, qui lui a succédé en cette qualité.

A. La captation des données des utilisateurs d'EncroChat

4. EncroChat était une solution de communication chiffrée par téléphonie mobile, qui fut distribuée de façon occulte à plus de 66 000 exemplaires entre 2016 et 2020.

1. Les premières investigations menées par les autorités françaises

5. Le 15 novembre 2018, le Centre de lutte contre les criminalités numériques de la direction générale de la gendarmerie nationale (« le C3N ») informa le parquet de la juridiction interrégionale spécialisée[1] (« JIRS ») de Lille de l'état de ses investigations au sujet d'EncroChat.

6. Un recoupement de procédures avait permis d'établir que plusieurs organisations criminelles opérant en France s'étaient converties à l'usage d'EncroChat. Des téléphones équipés d'EncroChat avaient été saisis dans sept affaires relevant de la criminalité organisée traitées par les sections de recherche de la gendarmerie nationale en 2017 et en 2018. Ces affaires portaient, pour la plupart, sur des trafics de stupéfiants de grande ampleur (ex. : saisie de 436 kg de résine de cannabis en janvier 2018, transport de 100 kg de résine de cannabis courant 2018). Cette tendance avait également été identifiée par plusieurs autres services de police judiciaire spécialisés en matière de criminalité organisée.

7. Des investigations techniques, menées avec le concours de l'Institut de recherche criminelle de la gendarmerie nationale (« IRCGN »), avaient par ailleurs permis d'établir que cette solution de communication fonctionnait en réseau fermé, au moyen de smartphones modifiés sur le plan technique. D'allure commune, ces appareils permettaient de lancer un système d'exploitation secondaire (EncroChat OS) donnant accès à des applications de messagerie, de téléphonie et prise de notes, dont les données étaient chiffrées de façon particulièrement robuste. Ces applications proposaient en outre des fonctionnalités de confidentialité avancées, telles que la possibilité de programmer la suppression automatique des messages envoyés à un autre utilisateur ou la possibilité d'effacer l'intégralité des données de l'appareil en urgence en saisissant un code spécifique depuis l'écran de déverrouillage. Les appareils équipés d'EncroChat étaient livrés avec une carte SIM ne

[1] Les JIRS sont compétentes pour l'enquête, la poursuite, l'instruction et le jugement de crimes et délits relevant de la criminalité organisée

nécessitant pas d'enregistrement nominatif. Il avait par ailleurs été établi que les appareils EncroChat échangeaient des données chiffrées avec un serveur situé à Roubaix.

8. Un site internet vantait les caractéristiques de ces appareils et le haut degré de confidentialité qu'ils permettaient de garantir. Toutefois, leur commercialisation ne s'effectuait pas librement, mais uniquement auprès de revendeurs opérant dans la clandestinité. Les enquêteurs avaient relevé que l'un d'entre eux proposait un appareil à la vente pour 1 610 €, pour une licence d'utilisation de seulement six mois.

9. Il avait enfin été observé que cette solution de chiffrement n'avait pas été déclarée auprès de l'Agence nationale de la sécurité des systèmes d'information (« ANSSI ») avant sa mise sur le marché en France.

10. Le 7 décembre 2018, le ministère public ouvrit une enquête préliminaire des chefs d'association de malfaiteurs en vue de la commission de crimes et délits punis de dix ans d'emprisonnement (et notamment de trafic de stupéfiants) et de fourniture, transfert et importation d'un moyen de cryptologie sans déclaration préalable auprès de l'ANSSI. Les investigations visaient à la fois les utilisateurs d'EncroChat et les individus ayant permis sa diffusion en France.

11. Huit autres saisies d'appareils équipés d'EncroChat effectuées entre 2017 et 2018 furent recensées par le ministère public dans des procédures relevant de la criminalité organisée suivies par la JIRS de Lille.

12. Le 21 décembre 2018, le juge des libertés et de la détention (« JLD ») du tribunal de grande instance de Lille autorisa la saisie et la copie des données stockées sur le serveur précité (paragraphe 7 ci-dessus). Une seconde copie de données fut autorisée en octobre 2019. Ces données, chiffrées pour la plupart, furent exploitées par l'IRCGN.

13. Les enquêteurs parvinrent à élucider le fonctionnement technique du réseau EncroChat et à accéder à certaines données relatives aux revendeurs et aux utilisateurs des téléphones qui y étaient connectés (adresses IP des revendeurs, numéros IMEI des appareils distribués, numéros IMSI des cartes SIM dont ils étaient équipés, identifiants de connexion, adresses auxquels les revendeurs étaient livrés, consommation détaillée de données pour chaque carte SIM...). Ces données permirent de déterminer qu'à cette date, 66 134 cartes SIM avaient été enregistrées sur le réseau depuis sa mise en service. L'étude des données de connexion des utilisateurs permit de déterminer leur localisation approximative et d'identifier les pays les plus concernés par son utilisation (les Pays-Bas, le Royaume-Uni, l'Irlande, l'Allemagne et l'Espagne notamment). Seule une fraction des utilisateurs étaient localisés en France.

14. Les données de communication des utilisateurs ne purent être mises au clair à ce stade. Toutefois, les enquêteurs identifièrent des données chiffrées correspondant à des notes ou mémos, à des contacts et à des listes

de contacts qui étaient synchronisées entre certains téléphones et ce serveur, et en parvinrent à en déchiffrer une petite partie.

15. Les 3 477 notes mises au clair furent exploitées. Les enquêteurs constatèrent qu'elles étaient incontestablement liées à des activités illicites et notamment à des trafics de stupéfiants (ex. : mention de numéros de conteneur, de tarifs et de quantités importantes de stupéfiants, de remises d'argent, de recours à des officines de blanchiment...).

16. Sur la base de ces travaux, un dispositif technique permettant de diffuser un logiciel espion sur les appareils connectés à EncroChat, de capter leurs données et de les transmettre sous forme déchiffrée aux autorités françaises fut élaboré.

2. Les décisions judiciaires internes autorisant la captation

17. Le 29 janvier 2020, le ministère public demanda à être autorisé à mettre en œuvre une captation de données (paragraphe 59 ci-dessous) portant sur l'ensemble des appareils reliés au réseau EncroChat.

18. Par deux ordonnances des 30 janvier et 12 février 2020, le JLD autorisa, pour un mois, la mise en place du dispositif technique précité (paragraphe 16 ci-dessus) sur le serveur hébergeant le réseau EncroChat. Il précisa que ce dispositif avait vocation à permettre la captation des données des utilisateurs en tous lieux, sur ce serveur et sur l'ensemble des appareils connectés à EncroChat. Les données concernées furent circonscrites (numéros IMEI, pseudonymes de leurs utilisateurs, messages échangés par les utilisateurs, photographies, messages vocaux, vidéos et documents échangés ou stockés dans les téléphones, numéros d'identification des antennes-relais utilisées par ces appareils, mots de passe de déverrouillage de l'écran et de l'application de prise de note, et notes et contacts sauvegardés dans les appareils).

19. Par trois autres décisions des 4, 20 et 31 mars 2020, le JLD autorisa un certain nombre d'opérations techniques permettant la mise en œuvre de l'opération de captation.

20. Pour motiver les cinq décisions précitées, les quatre magistrats ayant successivement statué en qualité de JLD détaillèrent précisément l'état des investigations (paragraphes 5 à 16 ci-dessus). Ils relevèrent que des téléphones EncroChat avaient été saisis dans diverses procédures relevant de la criminalité organisée, tant par les sections de recherche de la gendarmerie nationale que dans le cadre de procédures suivies par la JIRS de Lille (paragraphes 6 et 11 ci-dessus). Ils constatèrent en outre que le déchiffrement des notes découvertes dans les données saisies sur le serveur utilisé par EncroChat avait confirmé que les téléphones concernés étaient utilisés dans le cadre d'activités criminelles générant des revenus considérables (paragraphe 15 ci-dessus), et en conclurent que les terminaux EncroChat étaient utilisés à des fins criminelles. Ils estimèrent que la captation de données envisagée était le seul moyen disponible pour contourner le

chiffrement des données échangées par les utilisateurs, pour les identifier et pour les interpeller. Au vu de ces éléments, les magistrats estimèrent que cette mesure de captation était nécessaire et proportionnée.

3. Les dispositions prises en vue de la captation

21. Diverses mesures furent prises dans la perspective de la captation.

22. Sur le plan de la coopération internationale, un dossier relatif à EncroChat fut ouvert auprès de l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (« Eurojust ») afin de favoriser la collaboration des autorités françaises et néerlandaises. Une équipe commune d'enquête fut ultérieurement constituée. L'Agence de l'Union européenne pour la coopération des services répressifs (« Europol ») apporta son concours.

23. Lors de réunions organisées à Eurojust le 22 janvier 2020 et à Europol les 19 et 21 février 2020, les autorités françaises et néerlandaises informèrent leurs homologues britanniques de l'opération de captation envisagée et offrirent de mettre à leur disposition les données concernant les utilisateurs localisés sur leur territoire à des fins répressives.

24. Sur le plan interne, les gendarmes français mirent en œuvre un traitement de données destiné à recueillir et à exploiter les données issues de la captation. Le 26 mars 2020, ils transmirent à la Commission nationale de l'informatique et des libertés (« CNIL ») un engagement de conformité accompagné d'un dossier technique de présentation du traitement. Une cellule nationale d'enquête fut par ailleurs constituée au sein du C3N.

25. De son côté, le service national de lutte contre la criminalité (*National Crime Agency* – la *« NCA »*) britannique sollicita des mandats aux fins d'intrusion informatique ciblée *(targeted equipment interference*). Leur émission fut approuvée par des commissaires judiciaires les 4 et 26 mars 2020.

4. Le déroulement et le contrôle judiciaire des opérations de captation

26. La captation de données débuta le 1er avril 2020.

27. Le JLD fut informé des investigations accomplies par des soit-transmis des 1er, 15 et 28 avril 2020.

28. Après exploitation d'une partie des données captées, le champ des investigations fut étendu à des faits de trafic de stupéfiants et d'acquisition et de détention illicites d'armes de catégorie A et B.

29. Par une ordonnance du 29 avril 2020, le JLD prolongea l'autorisation de captation de données informatiques pour une durée d'un mois aux motifs suivants :

> « À ce jour, sont très précisément concernés par cette mesure de captation :
>
> - 31 477 téléphones, actifs dans un total de 121 pays (liste des numéros IMEI concernés transmise en pièce jointe (...)) ;

- 380 téléphones actifs sur le territoire national, dont 242 téléphones (soit une proportion de 63,7 %) sont utilisés à des fins délictuelles ou criminelles, une immense majorité d'entre eux étant aux mains de trafiquants de produits stupéfiants. Il doit être précisé que la flotte des 138 téléphones restants se scinde en téléphones inactifs, d'une part, ou non encore exploités, d'autre part, compte tenu de la masse de données que le service enquêteur a à gérer.

Les conversations exploitées, ainsi que l'examen des fichiers photos échangés, démontraient l'importance des trafics gérés par ces utilisateurs, leur impact profond sur l'ordre public national et les profits que ces derniers généraient.

Le coût particulièrement élevé des terminaux sécurisés EncroChat, tant à l'achat qu'en termes de frais d'abonnement, le réservait donc à des clients susceptibles de vite rentabiliser cet achat.

(...)

Les éléments d'ores et déjà recueillis, depuis le début de cette enquête préliminaire, relativement au caractère dédié de cette solution de téléphonie cryptée à des fins criminelles, se voyaient par ailleurs confortés par l'examen du volet relatif aux revendeurs de ces téléphones, qui apparaissaient entretenir des liens directs avec les techniciens et administrateurs de la plateforme, et donc faire l'interface avec une clientèle qui semblait se montrer exigeante.

Cette configuration ressortait notamment de ce que les enquêteurs observaient lors de la mise en place de l'outil de captation, qui provoquait une interruption de service amenant des utilisateurs qui étaient identifiés comme de gros revendeurs de téléphones à renseigner leur clientèle sur les causes et la durée de ce dysfonctionnement, assurant ce qu'il convenait de désigner comme un service après-vente. Ces revendeurs obtenaient des réponses de certains de leurs contacts qui pouvaient être identifiés comme des techniciens et administrateurs de la société EncroChat.

Les enquêteurs découvraient notamment dans une note figurant sur le téléphone EncroChat d'un revendeur australien un parfait manuel de commercialisation des terminaux cryptés. expliquant, outre le déroulement souhaité des différentes phases de l'achat par le vendeur jusqu'à la vente finale à l'utilisateur, que le paiement devait préférentiellement intervenir en cryptomonnaie, et qu'il fallait bien évidemment rester discret par rapport à la police, en évitant notamment de se faire repérer par des livraisons trop importantes en quantité (...). Il pouvait d'ailleurs être souligné que l'activité première de ce revendeur velléitaire était le trafic de cocaïne. (...) L'auteur de la note donne ensuite avec force détails, la méthode d'authentification et insiste sur les garanties de sécurité des appareils qui ne peuvent être "interceptés" ni être exploités indûment s'ils "tombent" entre de "mauvaises mains" ; il est notamment indiqué que « si la police récupère l'IMEI et la SIM du téléphone, ils ne pourront te localiser ».

La grande confiance de la clientèle dans la sécurité de ses communications ressortait d'ailleurs de la grande facilité avec laquelle celle-ci se photographiait à visage découvert, ou évoquait des éléments personnels susceptibles d'aboutir à des identifications, autant d'éléments qui ne se retrouvaient jamais sur les téléphones habituellement dédiés aux trafics de produits stupéfiants, *a fortiori* de cette intensité.

Les informations recueillies sur certains des plus gros revendeurs européens de ces terminaux cryptés, basés à Marbella en Espagne, indiquaient que ceux-ci procédaient à leur écoulement dans une "arrière-boutique", désignée comme telle dans les échanges interceptés, et venant encore une fois établir le très grand souci d'anonymat de cette clientèle.

(...)

Argumentaire commercial, souci de l'anonymat poussé à l'extrême, clientèle presque exclusivement criminelle, structure sociale disséminée et évanescente, le caractère ontologiquement illicite de la solution EncroChat, conçue pour être vendue à des réseaux criminels soucieux de rester dans l'ombre et de mettre en échec l'action des services répressifs, était conforté par ce premier mois de captation.

L'analyse des terminaux étant impossible, seule la mise en place du dispositif de captation de données informatique actuellement actif permet de contourner le chiffrement des données échangées par les utilisateurs (...). L'enquête a permis de démontrer qu'il s'agissait du seul moyen d'aboutir à l'identification de la structure commerciale occulte d'EncroChat, de comprendre ses modalités de fonctionnement, ainsi que celles de ses utilisateurs se livrant à des activités illicites d'envergure. »

Le magistrat releva en outre que les données exploitées avaient permis d'identifier un utilisateur appartenant au crime organisé irlandais, en lien avec près de 400 autres utilisateurs d'EncroChat dont les échanges faisaient écho à une vague de règlements de compte opposant deux clans rivaux. Par ailleurs, un utilisateur proche des organisateurs du réseau EncroChat et délivrant des conseils pour déjouer l'attention des autorités lors des mouvements de fonds internationaux avait été localisé à Vancouver.

Les données susceptibles d'être captées furent circonscrites de la même façon que précédemment (paragraphe 18 ci-dessus).

30. Le 28 mai 2020, une information judiciaire fut ouverte auprès de la JIRS de Lille sous diverses qualifications, dont celles d'association de malfaiteurs en vue de la préparation de différents crimes et délits punis de dix ans d'emprisonnement, d'infractions liées au trafic de stupéfiants, d'infractions au trafic d'armes, de blanchiment et de fourniture, transfert et importation d'un moyen de cryptologie sans déclaration préalable.

31. Par une ordonnance du même jour, la juge d'instruction autorisa la poursuite de la captation de données pour quatre mois, selon les mêmes modalités. La magistrate observa qu'au 26 mai 2020, la captation de données concernait 20 429 téléphones actifs dans 122 pays et qu'elle avait permis de capter près de 100 millions de messages et 1 136 Go de données. Elle constata que 317 des 454 téléphones actifs localisés en France étaient utilisés à des fins illicites, les 154 autres terminaux ne présentant pas ou peu de communications exploitables. Elle releva que l'organisation criminelle proposant la solution EncroChat exerçait de manière occulte, que les appareils EncroChat n'étaient pas en vente libre et que leur coût moyen d'utilisation était de 1 500 euros (EUR) pour six mois d'abonnement. Elle considéra que les données captées permettaient de conclure que cette solution de communication était « exclusivement [utilisée] à des fins criminelles » et que les revendeurs de téléphones EncroChat faisaient partie intégrante d'organisations criminelles. Le juge d'instruction estima que la captation restait le seul moyen d'exploiter les données chiffrées par EncroChat et qu'elle était nécessaire à la poursuite des investigations.

32. Dans la nuit du 12 au 13 juin 2020, EncroChat informa l'ensemble de ses utilisateurs que leur téléphone avait potentiellement été compromis et les incita à détruire leur terminal immédiatement.

33. La captation des données cessa le 2 juillet 2020. Elle porta sur un total de 39 571 terminaux, qui n'ont pas tous été effectivement utilisés sur cette période.

34. L'opération de captation fut dévoilée lors d'une conférence de presse qui s'est tenue à Eurojust le 2 juillet 2020. Dans un communiqué diffusé à cette occasion et accessible sur le site de l'agence, la gendarmerie nationale informa les utilisateurs d'EncroChat qu'ils pouvaient solliciter l'effacement de leurs données personnelles de la procédure judiciaire en indiquant les coordonnées du service compétent. Le Gouvernement indique n'avoir reçu aucune demande de cette nature.

B. Le partage des données captées avec les autorités britanniques

35. Informé de l'imminence de la captation (paragraphe 22 ci-dessus), le service des poursuites de la Couronne (*Crown Prosecution Service* – « le *CPS* ») émit dès le 11 mars 2020 une décision d'enquête européenne (« DEE ») afin d'obtenir la transmission de toutes les données concernant les appareils localisés sur le sol britannique que les autorités françaises parviendraient à capter, en tant qu'éléments de preuve recueillis dans l'État d'exécution. Il motiva sa demande par les considérations suivantes :

> « Si la détention et la vente d'appareils EncroChat ne sont pas incriminées au Royaume-Uni, il est considéré que les appareils EncroChat ont été développés et sont spécialement commercialisés à l'attention du milieu criminel afin de faciliter ses agissements illicites au Royaume-Uni.
>
> EncroChat est considéré comme la plus prolifique des plateformes de communication chiffrée dédiée à la criminalité au Royaume-Uni, avec près de 9 000 utilisateurs sur le sol britannique sur un total de plus de 50 000 utilisateurs à l'échelle mondiale.
>
> Il est considéré que l'usage d'EncroChat a significativement augmenté en 2019, en passant de près de 7 000 appareils en début d'année à près de 9 000 en fin d'année. Ils sont utilisés par des individus impliqués dans des activités criminelles, et par ceux qui les facilitent sur le plan logistique ou technique.
>
> L'utilisation d'appareils EncroChat a été relevée dans le cadre des opérations de la *NCA* et de la police dans tout le Royaume-Uni. Le haut degré de chiffrement du service EncroChat constitue un obstacle à l'action des forces de l'ordre tant en matière de renseignement criminel qu'en matière de collecte des preuves dans les affaires relevant de la criminalité la plus grave.
>
> Des investigations ont permis d'établir qu'EncroChat était utilisé au soutien d'activités relevant de la grande délinquance et de la criminalité organisée, en conséquence de quoi l'accès à ces données offrira des possibilités d'enquête et permettra [aux forces de l'ordre] de concentrer leurs ressources sur les utilisateurs de ces appareils et de poursuivre les infractions relevées sur le fondement de divers textes répressifs. On peut raisonnablement s'attendre que ceux-ci incluent la loi de 1971 sur

> l'abus de stupéfiants, la loi de 2002 sur les produits de la criminalité, la loi de 1968 sur les armes à feu et la loi de 1979 sur l'administration des douanes et les droits d'accises.
>
> Il est estimé que la majorité, sinon la totalité des utilisateurs de cette plateforme sont issus du milieu criminel et l'utilisent afin d'entraver délibérément l'action des forces de l'ordre. Il est considéré qu'il y a peu de raisons valables, pour un individu non impliqué dans la criminalité, d'utiliser des moyens de communication aussi onéreux et aussi complexes. (...)
>
> En outre, il est proposé en premier lieu de rassembler des renseignements criminels et de les transmettre aux services répressifs compétents au soutien d'enquêtes et de poursuites en cours, là où l'usage d'appareils EncroChat a d'ores et déjà été identifié. Par la suite, les données restantes seront utilisées pour identifier d'autres réseaux criminels et pour engager des investigations et des poursuites le cas échéant. »

36. Le 31 mars 2020, le procureur de la République de Lille ordonna l'exécution de cette DEE. En conséquence, des paquets de données furent périodiquement mis à la disposition de la *NCA* au cours de l'opération de captation.

37. Les données de 7 417 appareils furent ainsi transmises, selon les indications du gouvernement britannique. Dans une note du 15 octobre 2020, la *NCA* considérait que la très grande majorité de ces terminaux avaient été utilisée à des fins criminelles. Pour 390 d'entre eux (5,3 %), la *NCA* estimait ne pas pouvoir se prononcer sur ce point, en l'absence de données suffisantes. 17 appareils contenant des informations susceptibles d'être couvertes par le secret professionnel avaient été identifiés et avaient été mis à l'écart dans des conditions appropriées. En dépit d'un examen approfondi, aucun usage d'EncroChat par des universitaires, par des journalistes ou par des personnes légitimement soucieuses de la protection de leur vie privée n'avait pu être identifié. La NCA n'avait en outre reçu aucune plainte d'utilisateur invoquant un usage légitime d'EncroChat.

38. Selon un communiqué de presse d'Eurojust du 27 juin 2023, le démantèlement d'EncroChat permit l'arrestation de 6 558 suspects et la saisie de 103 tonnes de cocaïne, de 163 tonnes de cannabis et de 3,3 tonnes d'héroïne à travers le monde, outre la saisie d'armes, d'explosifs et d'avoirs criminels.

39. Selon les indications du Gouvernement britannique, les données communiquées par les autorités françaises permirent aux autorités répressives britanniques d'arrêter 746 personnes et de saisir 54 millions de livres sterling (GBP, soit 64 millions d'euros) en numéraire, plusieurs tonnes de drogues et 77 armes.

C. Les poursuites pénales exercées à l'encontre des requérants au Royaume-Uni

40. Les requérants firent l'objet de poursuites pénales au Royaume-Uni dans deux affaires distinctes, dans le cadre desquelles l'usage d'EncroChat leur fut reproché.

1. Les poursuites diligentées à l'encontre du premier requérant

41. La *NCA* communiqua à la police métropolitaine (*Metropolitan Police*) des jeux de données correspondant à des appareils EncroChat localisés sur son ressort.

42. L'analyse de certaines données issues de la captation permit aux enquêteurs d'identifier des échanges entre deux utilisateurs d'EncroChat au cours desquels un individu donnait pour instructions de collecter plusieurs kilos de cocaïne et d'héroïne. Le 18 mai 2020, des messages relatifs à la réception d'une cargaison de stupéfiants depuis l'étranger furent échangés. Le lendemain, O. fut interpellé en possession de 10 kg d'héroïne. Une perquisition à l'adresse qu'il venait de quitter permit de saisir 28 kg d'héroïne supplémentaires, 10 kg de cocaïne, une presse hydraulique, 37 735 GBP (44 807 EUR) en espèces et plusieurs téléphones dont un appareil équipé d'EncroChat. Les produits saisis avaient, selon les enquêteurs, une valeur marchande au détail comprise entre 4,6 et 4,8 millions de livres sterling.

43. Le premier requérant fut interpellé le 18 juin 2020.

44. Les enquêteurs lui reprochèrent d'être le donneur d'ordres d'O. Les conversations interceptées grâce à la captation litigieuse furent évoquées dans un interrogatoire et dans une synthèse de police réalisés le 19 juin 2020. Il garda le silence devant les enquêteurs.

45. Il fut mis en accusation des chefs de conspiration aux fins d'importation illicite de cocaïne et d'héroïne et de conspiration aux fins de détention illicite de cocaïne et d'héroïne avec intention de la céder à autrui.

46. Le premier requérant présenta une demande d'annulation des poursuites en faisant valoir que les preuves sur lesquelles se fondait l'accusation reposaient sur des communications interceptées dans de conditions contraires à la loi de 2016 sur les pouvoirs d'enquête (*Investigatory Powers Act 2016*).

47. Au dernier état connu, les poursuites diligentées à son encontre étaient toujours pendantes devant la *Crown Court* de Snarebrook.

2. Les poursuites diligentées à l'encontre du second requérant

48. D'autres données issues de la captation permirent par ailleurs aux enquêteurs britanniques de faire la lumière sur les agissements d'une organisation criminelle implantée à Liverpool, qui se livrait au stockage et à la vente en gros de produits stupéfiants. Les échanges analysés mirent en outre en lumière que quatre membres de ce groupe criminel, utilisateurs d'EncroChat, projetaient d'assassiner trois personnes à titre de représailles à la suite d'un vol de 30 kg de cocaïne survenu le 23 mai 2020.

49. Le second requérant fut arrêté le 16 juin 2020. Les enquêteurs lui reprochèrent d'être l'un des utilisateurs d'EncroChat concernés. L'intéressé garda le silence.

50. Il fut mis en accusation des chefs de conspiration en vue de la fourniture de cocaïne et de d'héroïne, de conspiration en vue de la commission de trois meurtres et de chantage. L'affaire fut portée devant la *Crown court* à Liverpool.

51. Le second requérant intervint comme partie intéressée à un recours introduit par un tiers, visant à être autorisé à contester la légalité de la DEE du 11 mars 2020 (paragraphe 35 ci-dessus). Le requérant soutint, d'une part, qu'une DEE aux fins de communication de preuves ne pouvait être émise qu'au sujet de faits déterminés et déjà commis, et, d'autre part, que la DEE litigieuse n'était pas susceptible de justifier une captation de données ordonnée à l'étranger et ayant des effets aux Royaume-Uni. Par décision du 26 octobre 2020, les juges de la *High court of Justice* rejetèrent ce recours.

Ils jugèrent en premier lieu qu'une DEE peut légalement porter sur la communication de preuves se rapportant à des infractions dont la matérialité et l'imputabilité restent à établir. Ils relevèrent que la DEE litigieuse portait sur une série d'infractions dont la commission pouvait raisonnablement être suspectée à la date de son émission.

Ils estimèrent en deuxième lieu qu'il ne leur appartenait pas, au titre du contrôle de la légalité de la DEE, d'apprécier si la captation ordonnée par les autorités françaises pouvait légalement avoir un effet extraterritorial. Ils relevèrent à ce titre qu'aucun moyen n'avait été et n'aurait pu être soulevé au sujet de la légalité de ces opérations de captation, qui sont régies par le seul droit français.

Ils considérèrent en troisième lieu qu'il n'y avait pas lieu de permettre l'introduction d'un recours portant sur la légalité de la DEE, dans la mesure où le requérant disposait d'un recours alternatif adéquat pour faire valoir ses griefs relatifs à l'équité du procès :

> « 44. (...) Le point fondamental de la présente affaire est que la préoccupation pratique du requérant n'est pas relative à la DEE, en tant que telle. En effet, il soutient lui-même qu'à la date de la DEE, les autorités [britanniques] ignoraient tout de lui. Son grief essentiel ne porte pas sur la régularité de la DEE en tant que telle, mais plutôt sur l'utilisation qui peut être faite des éléments transmis en exécution de la DEE dans le cadre de la procédure pénale subséquemment dirigée à son encontre. C'est exactement ce qui s'est produit depuis, avec la mise en accusation du requérant devant la *Crown Court*. Cela étaye, à notre avis, la conclusion selon laquelle le requérant dispose effectivement d'un recours alternatif adéquat pour le seul grief de fond dont il peut se prévaloir. Ce recours se trouve dans le pouvoir de la *Crown Court* d'exclure des preuves lorsqu'elles pourraient nuire à l'équité de la procédure en vertu de l'article 78 de la loi de 1984 sur la police et les preuves en matière pénale (*Police and Criminal Evidence Act 1984*). »

52. Par ailleurs, une audience préparatoire eut lieu du 16 novembre au 2 décembre 2020 dans le cadre des poursuites le concernant. Il contesta la recevabilité des messages échangés *via* EncroChat à titre de preuve et demanda la suspension du procès pour abus de procédure. Il fit notamment valoir que la technique utilisée correspondait à une interception au sens du

droit interne. Il en déduisit qu'un mandat d'interception ciblée (*targeted interception warrant*) était nécessaire à la régularité de la captation sur le territoire britannique et que les données qui en étaient issues ne pouvaient être admises à titre de preuve. Se référant à l'arrêt rendu par la Cour de justice de l'Union européenne le 6 octobre 2020 dans l'affaire *Privacy International* (C-623/17, EU:C:2020:790), il soutint par ailleurs que cette captation de données correspondait en réalité à une transmission généralisée et indifférenciée des données, dont il dénonça le caractère arbitraire et disproportionné. Invoquant l'article 6 de la Convention, il soutint par ailleurs que la conduite des agents de la *NCA* avait lésé l'équité du procès.

53. Par une décision du 4 janvier 2021, le juge déclara en premier lieu les données issues de la captation recevables à titre de preuve devant la *Crown court*, en considérant que les modalités techniques de la captation ne permettaient pas de la qualifier d'interception au sens du droit interne et en relevant que la captation avait été réalisée après qu'un mandat aux fins d'intrusion informatique ciblée avait été émis (paragraphe 25 ci-dessus).

Il rejeta en second lieu la demande de suspension du procès, en estimant que la conduite des agents britanniques dans le cadre de leur coopération avec les gendarmes français n'était pas constitutive d'un abus de procédure. Il releva notamment les éléments suivants :

> « 179. Les références [du requérant] à l'arrêt *Privacy International* et à la [Convention] n'affectent en rien mes conclusions. En réalité, en l'espèce, la transmission des données [issues de la captation] a découlé de leur obtention régulière en France, de l'émission d'une DEE dont la *High Court* a reconnu la légalité et de l'obtention de mandats aux fins d'intrusion informatique ciblé sous le contrôle de commissaires judiciaires du Commissariat aux pouvoirs d'enquête. En bref, il ne s'agit pas d'une collecte générale et indifférenciée de données, mais, pour les raisons précitées relatives au fonctionnement d'EncroChat, d'une collecte ciblée, soumise à un contrôle judiciaire en ce qui concerne la légalité des instruments impliqués dans l'activité. La procédure appropriée a été suivie, sans abus. Je ne suis donc pas en mesure d'accéder à la demande de suspension de la procédure. »

Il estima enfin que l'admission des données issues de la captation à titre de preuve n'était pas de nature à rendre la procédure inéquitable et qu'il n'y avait donc pas lieu de les exclure sur le fondement de l'article 78 du *Police and Criminal Evidence Act*.

54. Le second requérant fit appel de cette décision en limitant ses contestations à la question de l'admissibilité des données issues du piratage d'EncroChat à titre de preuve. Son appel fut rejeté par la Cour d'appel d'Angleterre et du Pays de Galles le 5 février 2021.

55. Le 12 mars 2021, le *Lord Chief Justice* refusa de l'autoriser à se pourvoir devant la Cour suprême.

56. Au dernier état connu, les poursuites diligentées à l'encontre du second requérant étaient toujours pendantes.

LE CADRE JURIDIQUE PERTINENT

57. Il convient de présenter successivement les dispositions relatives à la captation de données informatiques (A), celles relatives à la protection des données captées (B) et celles relatives à leur partage en exécution d'une décision d'enquête européenne (C).

A. Le cadre juridique relatif à la captation de données informatiques

1. Dispositions du code de procédure pénale

58. Les dispositions qui suivent sont issues de la loi n° 2019-222 du 23 mars 2019 et étaient applicables à la date de la captation litigieuse.

59. L'article 706-102-1 alinéa 1er du code de procédure pénale (CPP) définit la captation de données informatiques dans les termes suivants :

> « Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles quelles sont reçues et émises par des périphériques. »

60. Il résulte des travaux parlementaires que le champ de la captation à distance a été étendu aux données informatiques afin de « démanteler des réseaux et trafics qui recourent à des techniques sophistiquées » en donnant notamment aux enquêteurs « la possibilité de capter en temps réel les données informatiques telles qu'elles s'affichent à l'écran » d'un appareil surveillé (Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure, n° 1697, déposé devant l'Assemblée nationale le 27 mai 2009).

61. La captation de données est soumise au régime général des techniques spéciales d'enquête, qui est défini par les dispositions du CPP suivantes :

Article 706-95-11, alinéa 2

> « Ces techniques spéciales d'enquête peuvent être mises en œuvre si les nécessités de l'enquête ou de l'information judiciaire relatives à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent. »

Article 706-95-12

> « Les techniques spéciales d'enquête sont autorisées :
>
> 1° Au cours de l'enquête, par le juge des libertés et de la détention à la requête du procureur de la République ;
>
> 2° Au cours de l'information, par le juge d'instruction, après avis du procureur de la République. »

Article 706-95-13

« L'autorisation mentionnée à l'article 706-95-12 fait l'objet d'une ordonnance écrite et motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Elle n'a pas de caractère juridictionnel et n'est pas susceptible de recours. (...) »

Article 706-95-14

« Ces techniques spéciales d'enquête se déroulent sous l'autorité et le contrôle du magistrat qui les a autorisées. Ce magistrat peut ordonner à tout moment leur interruption.

Le juge des libertés et de la détention est informé sans délai par le procureur de la République des actes accomplis. Les procès-verbaux dressés en exécution de la décision du juge des libertés et de la détention lui sont communiqués.

Si le juge des libertés et de la détention estime que les opérations n'ont pas été réalisées conformément à son autorisation ou que les dispositions applicables du présent code n'ont pas été respectées, il ordonne la destruction des procès-verbaux et des enregistrements effectués. (...)

Les opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du magistrat. Le fait que ces opérations révèlent des infractions autres que celles visées dans l'autorisation du magistrat ne constitue pas une cause de nullité des procédures incidentes. »

Article 706-95-16

« L'autorisation mentionnée au 1° de l'article 706-95-12 est délivrée pour une durée maximale d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée.

L'autorisation mentionnée au 2° du même article 706-95-12 est délivrée pour une durée maximale de quatre mois, renouvelable dans les mêmes conditions de forme et de durée, sans que la durée totale des opérations ne puisse excéder deux ans. »

Article 706-95-18

« Le procureur de la République, le juge d'instruction ou l'officier de police judiciaire commis par lui ou requis par le procureur de la République (...), dresse procès-verbal de la mise en place des dispositifs techniques et des opérations effectuées en application de la présente section. (...)

Les enregistrements sont placés sous scellés fermés.

L'officier de police judiciaire (...) décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité. Aucune séquence relative à la vie privée étrangère aux infractions visées dans les ordonnances autorisant la mesure ne peut être conservée dans le dossier de la procédure.

Les conversations et données en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin. »

Article 706-95-19

« Les enregistrements et données recueillies lors des opérations effectuées en application de la présente section sont détruits, à la diligence du procureur de la

République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction. »

62. Les articles 703-73 et 706-73-1 du CPP, vers lesquels renvoie l'article 706-95-11, énumèrent une série d'infractions d'une particulière gravité ou relevant de la criminalité organisée. À la date des faits, ces listes comprenaient trente catégories d'infractions, dont les crimes et délits de trafic de stupéfiants et les délits de trafic d'armes, ainsi que les délits d'association de malfaiteurs et de blanchiment lorsqu'ils se rapportent à la préparation ou au produit de certaines infractions.

63. Le régime de la captation de données est outre complété par les dispositions suivantes :

Article 706-102-1, second alinéa

« Le procureur de la République ou le juge d'instruction peut désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique mentionné au premier alinéa du présent article. Le procureur de la République ou le juge d'instruction peut également prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale (...). »

Article 706-102-3

« À peine de nullité, la décision autorisant le recours au dispositif mentionné à l'article 706-102-1 précise l'infraction qui motive le recours à ces opérations, la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données ainsi que la durée des opérations. »

Article 706-102-5

« (...) / (...) / La mise en place du dispositif technique mentionné à l'article 706-102-1 ne peut concerner les systèmes automatisés de traitement des données se trouvant dans les lieux visés aux articles 56-1 *[le cabinet d'un avocat ou son domicile]*, 56-2 *[les locaux et véhicules des entreprises de presse et le domicile des journalistes]*, 56-3 *[le cabinet d'un médecin, d'un notaire ou d'un huissier]* et 56-5 *[les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles]* ni être réalisée dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7. »

2. Jurisprudence

64. Par deux arrêts des 11 et 25 octobre 2022 (n^{os} 21-85.148 et 21-85.763), la Cour de cassation a rejeté un moyen tiré du caractère imprécis de la définition de la captation, en jugeant, d'une part, que cette mesure peut porter non seulement sur les données informatiques stockées sur l'appareil visé mais aussi sur les données en cours de transmission, et, d'autre part, qu'elle autorise la mise en œuvre d'opérations techniques préalables à la captation telles que le blocage ou la redirection de flux de données.

65. Par une décision n^{o} 2022-987 QPC du 8 avril 2022, le Conseil constitutionnel a jugé le second alinéa de l'article 706-102-1 du CPP

conforme à la Constitution. En particulier, il a estimé que la circonstance qu'il puisse être recouru à des moyens couverts par le secret de la défense nationale ne portait pas une atteinte excessive aux droits de la défense et au principe du contradictoire aux motifs suivants :

> « 15. En premier lieu, en adoptant les dispositions contestées, le législateur a entendu permettre aux autorités en charge des investigations de bénéficier de moyens efficaces de captation et de mise au clair des données, sans pour autant fragiliser l'action des services de renseignement en divulguant les techniques qu'ils utilisent. Ce faisant, ces dispositions poursuivent l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et mettent en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation.
>
> 16. En deuxième lieu, il ne peut être recouru à ces moyens que pour la mise en œuvre d'une technique spéciale d'investigation qui doit être autorisée par le juge des libertés et de la détention ou par le juge d'instruction et justifiée par les nécessités d'une enquête ou d'une information judiciaire relatives à certains crimes et délits d'une particulière gravité et complexité. Cette technique est mise en œuvre sous l'autorité et le contrôle du magistrat qui l'a autorisée et qui peut ordonner à tout moment son interruption. Les données captées dans le cadre des investigations sont placées sous scellés en application de l'article 706-95-18 du code de procédure pénale.
>
> 17. En troisième lieu, si les dispositions contestées sont susceptibles de soustraire au contradictoire certaines informations techniques soumises au secret de la défense nationale, demeure obligatoirement versée au dossier de la procédure l'ordonnance écrite et motivée du juge qui autorise la mise en œuvre d'un dispositif de captation et mentionne, à peine de nullité, l'infraction qui motive le recours à ce dispositif, la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données concernés, ainsi que la durée pendant laquelle cette opération est autorisée. Sont également versés au dossier le procès-verbal de mise en place du dispositif, qui mentionne notamment la date et l'heure auxquelles l'opération a commencé et s'est terminée, et celui décrivant ou transcrivant les données enregistrées jugées utiles à la manifestation de la vérité. Enfin, l'ensemble des éléments obtenus à l'issue des opérations de mise au clair font l'objet d'un procès-verbal de réception versé au dossier de la procédure et sont accompagnés d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis.
>
> 18. En dernier lieu, la juridiction peut demander la déclassification et la communication des informations soumises au secret de la défense nationale, dans les conditions prévues aux articles L. 2312-4 à L. 2312-8 du code de la défense. »

66. Par un arrêt du 10 mai 2023 (n° 22-84.475), la Cour de cassation a jugé que la captation litigieuse avait permis aux autorités d'accéder à des données non chiffrées, de sorte qu'il n'y avait pas lieu de joindre à la procédure une attestation certifiant la sincérité prévue à l'article 230-3 du CPP en cas de mise au clair de données chiffrées.

B. Le cadre juridique relatif à la protection des données captées

1. La loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

67. Les dispositions pertinentes de la loi du 6 janvier 1978 sont les suivantes :

Article 87

« Le présent titre s'applique, sans préjudice du titre Ier, aux traitements de données à caractère personnel mis en œuvre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (...), par toute autorité publique compétente (...).

Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour l'une des finalités énoncées au premier alinéa, par une autorité compétente au sens du même premier alinéa et où sont respectées les dispositions des articles 89 et 90. Le traitement assure notamment la proportionnalité de la durée de conservation des données à caractère personnel, compte tenu de l'objet du fichier et de la nature ou de la gravité des infractions concernées. »

Article 105

« La personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, le droit d'accéder auxdites données ainsi qu'aux informations suivantes :

1º Les finalités du traitement ainsi que sa base juridique ;

2º Les catégories de données à caractère personnel concernées ;

3º Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées (...) ;

4º Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

5º L'existence du droit de demander au responsable de traitement la rectification ou l'effacement des données à caractère personnel, et l'existence du droit de demander une limitation du traitement de ces données ;

6º Le droit d'introduire une réclamation auprès de la [CNIL] et les coordonnées de la commission ;

7º La communication des données à caractère personnel en cours de traitement ainsi que toute information disponible quant à leur source. »

Article 106

« I.-La personne concernée a le droit d'obtenir du responsable de traitement :

(...)

3º Que soient effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la

présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable de traitement ;

4° Que le traitement soit limité dans les cas prévus au III du présent article.

II.-Lorsque l'intéressé en fait la demande, le responsable de traitement doit justifier qu'il a procédé aux opérations exigées en application du I.

III.-Au lieu de procéder à l'effacement, le responsable de traitement limite le traitement :

(...)

2° Soit lorsque les données à caractère personnel doivent être conservées à des fins probatoires.

(...)

IV.-Le responsable de traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ainsi que des motifs du refus.

(...)

VI.-Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I et III, le responsable de traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité. »

Article 107

« I.- Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant compte des droits fondamentaux et des intérêts légitimes de la personne pour :

1° Éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ;

2° Éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;

(...)

Ces restrictions sont prévues par l'acte instaurant le traitement.

II.- Lorsque les conditions prévues au I sont remplies, le responsable de traitement peut :

(...)

2° Refuser ou limiter le droit d'accès de la personne concernée prévu à l'article 105 ;

3° Ne pas informer la personne du refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ni des motifs de cette décision, par dérogation au IV de l'article 106.

III.- Dans les cas mentionnés au 2° du II du présent article, le responsable de traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès ainsi que des motifs du refus ou de la limitation. Ces

informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable de traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision et met ces informations à la disposition de la [CNIL].

IV.- En cas de restriction des droits de la personne concernée intervenue en application des II ou III, le responsable de traitement informe la personne concernée de la possibilité, prévue à l'article 108, d'exercer ses droits par l'intermédiaire de la [CNIL]. Hors le cas prévu au 1° du II, il l'informe également de la possibilité de former un recours juridictionnel. »

Article 108

« En cas de restriction des droits de la personne concernée intervenue en application des II ou III de l'article 107, la personne concernée peut saisir la [CNIL].

La commission désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. La commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. »

Article 111

« Les dispositions du présent chapitre ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données et les conditions de rectification ou d'effacement de ces données ne peuvent être régis que par les dispositions du code de procédure pénale. »

68. Les modalités d'exercice des droits garantis par les articles 105 et 106 de la loi du 6 janvier 1978 sont prévus à l'article 135 du décret n° 2019-536 du 26 mai 2016, qui prévoit que la « personne concernée » doit « [justifier] de son identité par tout moyen et [préciser] l'adresse à laquelle doit parvenir la réponse ». Cet article permet au responsable de traitement de solliciter des informations supplémentaires lorsqu'il a des doutes raisonnables sur l'identité de la personne, sur son adresse ou lorsque la demande est imprécise ou ne comporte pas tous les éléments lui permettant de procéder aux opérations qui lui sont demandée.

2. Le décret n° 2015-1700 du 18 décembre 2015

69. Les traitements de données mis en œuvre dans le cadre des captations de données effectuées en application de l'article 706-102-1 du CPP sont spécifiquement encadrés par le décret n° 2015-1700 du 18 décembre 2015, qui prévoit ce qui suit :

Article 3

« Les données à caractère personnel et informations exploitées par les traitements mentionnés à l'article 1er ne peuvent provenir que de dispositifs techniques autorisés conformément à l'article R. 226-3 du code pénal et mis en place dans le cadre :

1° d'investigations conduites en flagrance ou en préliminaire, sur ordonnance écrite et motivée du juge des libertés et de la détention, à la requête du procureur de la République ;

2° d'information judiciaire, sur ordonnance écrite et motivée du juge d'instruction, après avis du procureur de la République (...). »

Article 4

« I. – Les magistrats accèdent à l'ensemble des données à caractère personnel et informations enregistrées dans le traitement en application de l'article 706-102-1 du code de procédure pénale, dans le cadre des procédures dont ils sont saisis.

II. – Ont accès aux données à caractère personnel et aux informations mentionnées à l'article 2, pour les besoins exclusifs de la procédure dans le cadre de laquelle l'opération de captation a été autorisée :

1° Les agents et officiers de police judiciaire de la police et de la gendarmerie nationales ;

(...)

Article 5

« Les données enregistrées sont conservées dans le traitement jusqu'à la date de clôture des investigations. À cette date, elles sont placées sous scellés fermés et effacées. La transcription des enregistrements effectuée par les personnes mentionnées au II de l'article 4, dans les conditions prévues à l'article 706-95-18 du code de procédure pénale, est transmise à l'autorité judiciaire pour être versée au dossier de la procédure. Les scellés fermés lui sont également adressés. »

Article 6

« Toute opération de collecte, de modification, de consultation, de transfert et de suppression des données à caractère personnel et informations fait l'objet d'un enregistrement comprenant l'identification de l'auteur, la date, l'heure et la nature de l'opération.

Ces informations sont conservées pendant une durée de six ans. »

Article 7

« I. − Le droit d'opposition prévu à l'article 110 de la loi du 6 janvier 1978 susvisée ne s'applique pas aux présents traitements.

II. − Conformément aux articles 104 à 106 de la même loi, les droits d'information, d'accès, de rectification, d'effacement et à la limitation s'exercent directement auprès du responsable du traitement.

Afin d'éviter de gêner des enquêtes, des recherches ou des procédures judiciaires ou d'éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, de protéger la

sécurité publique ou de protéger la sécurité nationale, les droits mentionnés à l'alinéa précédent peuvent faire l'objet de restrictions en application des II et III de l'article 107 de la même loi.

La personne concernée par ces restrictions exerce ses droits auprès de la [CNIL] dans les conditions prévues à l'article 108 de la même loi. »

Article 8

« La mise en œuvre des traitements mentionnés à l'article 1er par le directeur général de la police nationale, le directeur général de la gendarmerie nationale, le directeur général de la sécurité intérieure, le préfet de police et le directeur général des douanes et des droits indirects s'accompagne de l'envoi à la [CNIL] d'un engagement de conformité faisant référence au présent décret accompagné d'un dossier technique de présentation du traitement. »

C. Le cadre juridique relatif au partage des données

1. Droit de l'Union européenne

a) La directive 2014/41/UE du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (« DEE »)

70. Les dispositions pertinentes de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la DEE en matière pénale (« la directive 2014/41 », *JO* 2014 L 130, pp. 1-36) sont les suivantes :

Article 1er : DEE et obligation de l'exécuter

« 1. La DEE est une décision judiciaire qui a été émise ou validée par une autorité judiciaire d'un État membre (ci-après dénommé "État d'émission") afin de faire exécuter une ou plusieurs mesures d'enquête spécifiques dans un autre État membre (ci-après dénommé "État d'exécution") en vue d'obtenir des preuves conformément à la présente directive.

La DEE peut également être émise pour l'obtention de preuves qui sont déjà en possession des autorités compétentes de l'État d'exécution.

2. Les États membres exécutent une DEE sur la base du principe de reconnaissance mutuelle et conformément à la présente directive.

(...)

4. La présente directive n'a pas pour effet de modifier l'obligation de respecter les droits fondamentaux et les principes juridiques inscrits à l'article 6 du traité sur l'Union européenne ["TUE"], y compris les droits de la défense des personnes faisant l'objet d'une procédure pénale, et il n'est porté atteinte à aucune des obligations qui incombent aux autorités judiciaires à cet égard. »

Article 4 : Types de procédures pour lesquelles la DEE peut être émise

« Une DEE peut être émise :

a) aux fins des procédures pénales qui sont engagées par une autorité judiciaire, ou à engager devant celle-ci, concernant une infraction pénale conformément au droit de l'État d'émission ;

(...) »

Article 6 : Conditions d'émission et de transmission d'une DEE

« 1. L'autorité d'émission ne peut émettre une DEE que si les conditions suivantes sont réunies :

a) l'émission de la DEE est nécessaire et proportionnée aux finalités des procédures visées à l'article 4, compte tenu des droits du suspect ou de la personne poursuivie ; et

b) la ou les mesures d'enquête indiquées dans la DEE auraient pu être ordonnées dans les mêmes conditions dans le cadre d'une procédure nationale similaire.

2. Dans chaque cas, le respect des conditions visées au paragraphe 1 est vérifié par l'autorité d'émission.

3. Lorsque l'autorité d'exécution a des raisons de penser que les conditions visées au paragraphe 1 n'ont pas été respectées, elle peut consulter l'autorité d'émission sur l'importance d'exécuter la DEE. Après cette consultation, l'autorité d'émission peut décider de retirer la DEE. »

Article 14 : Recours

« 1. Les États membres veillent à ce que des voies de recours équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire soient applicables aux mesures d'enquête indiquées dans la DEE.

2. Les motifs de fond qui sont à l'origine de l'émission de la DEE ne peuvent être contestés que par une action intentée dans l'État d'émission, sans préjudice des garanties des droits fondamentaux dans l'État d'exécution.

(...)

4. Les États membres veillent à ce que les délais de recours soient identiques à ceux qui sont prévus dans le cadre de procédures nationales similaires et qu'ils s'appliquent de manière à garantir aux personnes concernées la possibilité d'exercer un recours effectif.

5. L'autorité d'émission et l'autorité d'exécution s'informent mutuellement des recours formés contre l'émission, la reconnaissance ou l'exécution d'une DEE.

(...)

7. L'État d'émission tient compte du fait que la reconnaissance ou l'exécution d'une DEE ait été contestée avec succès conformément à son droit national. Sans préjudice des règles de procédure nationales, les États membres veillent à ce que, dans une procédure pénale dans l'État d'émission, les droits de la défense et l'équité de la procédure soient respectés dans le cadre de l'évaluation des éléments de preuve obtenus au moyen de la DEE. »

71. Ces dispositions doivent être lues à la lumière des considérants 11, 19 et 22 de la directive 2014/41, selon lesquels :

« (11) Une DEE devrait être choisie lorsque l'exécution d'une mesure d'enquête semble proportionnée, adéquate et applicable au cas en question. L'autorité d'émission devrait par conséquent vérifier si la preuve recherchée est nécessaire et proportionnée aux fins de la procédure, si la mesure d'enquête choisie est nécessaire et proportionnée aux fins de l'obtention de la preuve concernée, et si une DEE devrait être émise aux fins d'associer un autre État membre à l'obtention de cette preuve. (...)

(...)

(19) La création d'un espace de liberté, de sécurité et de justice dans l'Union est fondée sur la confiance mutuelle et la présomption que les autres États membres respectent le droit de l'Union et, en particulier, les droits fondamentaux. Cette présomption est toutefois réfragable. Par conséquent, s'il existe des motifs sérieux de croire que l'exécution d'une mesure d'enquête indiquée dans la DEE porterait atteinte à un droit fondamental de la personne concernée et que l'État d'exécution méconnaîtrait ses obligations concernant la protection des droits fondamentaux reconnus dans la charte [des droits fondamentaux de l'Union européenne, « la Charte »], l'exécution de la DEE devrait être refusée.

(...)

(22) Les voies de recours permettant de contester une DEE devraient être au moins égales à celles qui sont prévues dans le cadre d'une procédure nationale à l'encontre de la mesure d'enquête concernée. Conformément à leur droit national, les États membres devraient veiller à ce que ces voies de recours soient applicables, notamment en informant en temps utile toute partie intéressée des possibilités de recours. Dans les cas où des objections à l'encontre de la DEE sont soulevées par une partie intéressée dans l'État d'exécution en ce qui concerne les motifs de fond sous-tendant l'émission de la DEE, il est souhaitable que les informations relatives à cette contestation soient transmises à l'autorité d'émission et que la partie intéressée en soit dûment informée. »

b) Jurisprudence de la Cour de justice de l'Union européenne (« CJUE »)

72. Dans son arrêt *Staatsanwaltschaft Wien (Ordres de virement falsifiés)* du 8 décembre 2020, la CJUE, réunie en Grande chambre, a déterminé les responsabilités respectives de l'État d'émission et de l'État d'exécution d'une DEE dans le champ de la protection des droits fondamentaux (affaire C-584/19, EU:C:2020:1002, points 57-69).

D'une part, elle a jugé que l'autorité d'émission d'une DEE doit prendre en compte le principe de proportionnalité et les droits fondamentaux de la personne concernée, notamment ceux consacrés par la Charte, et que sa décision doit pouvoir faire l'objet de voies de recours effectives, au moins équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire (points 57-63). S'appuyant sur les termes de l'article 14 § 7 de la directive 2014/41, elle a plus particulièrement souligné qu'au cours de la procédure pénale dans l'État d'émission, les droits de la défense et l'équité de la procédure doivent être respectés lors de l'évaluation des éléments de preuve obtenus au moyen d'une DEE (point 62).

D'autre part, elle a rappelé que, dans l'État d'exécution, la procédure d'exécution est entourée des garanties prévues par le droit national (point 65). En outre, l'article 6 § 3 de la directive 2014/41 permet à l'autorité d'exécution de consulter l'autorité d'émission sur l'importance d'exécuter la DEE lorsqu'elle a des raisons de penser que la mesure d'enquête sollicitée n'est pas nécessaire et proportionnée aux finalités des procédures pour lesquelles elle a été émise, compte tenu des droits de la personne concernée, afin que son retrait soit envisagé (point 66). Par ailleurs, elle a relevé que l'article 10 de la directive 2014/41 permet à l'autorité d'exécution de recourir à une autre

mesure d'enquête que celle indiquée dans la DEE si cette mesure alternative permet d'obtenir le même résultat par des moyens impliquant une atteinte moindre aux droits fondamentaux (point 67). Enfin, elle a jugé que, selon l'article 11 § 1, f) de la directive 2014/41, l'exécution d'une DEE peut être refusée dans l'État d'exécution lorsqu'il existe des motifs sérieux de croire que l'exécution de la mesure d'enquête indiquée dans la DEE serait incompatible avec les obligations de l'État d'exécution conformément à l'article 6 TUE et à la Charte (point 68).

73. Dans son arrêt *Gavanozov II* du 11 novembre 2021 (affaire C-852/19, EU:C:2021:902), la CJUE a jugé que les États membres sont tenus d'assurer le respect du droit à un recours effectif consacré à l'article 47 de la Charte dans le cadre de la procédure d'émission et d'exécution d'une DEE, qui constitue une mise en œuvre du droit de l'Union (points 28 à 30). Elle a plus particulièrement considéré que les personnes concernées doivent disposer de voies de recours appropriées leur permettant, d'une part, de contester la régularité et la nécessité des mesures d'enquêtes et, d'autre part, de demander un redressement approprié si ces mesures ont été ordonnées ou exécutées illégalement (points 33 et 34).

Elle a par ailleurs rappelé que les motifs de fond qui sont à l'origine de l'émission d'une DEE ne peuvent être contestés que par une action intentée dans l'État membre d'émission, conformément à l'article 14 § 1 de la directive 2014/41, de sorte qu'une voie de recours doit nécessairement être ouverte à cette fin dans l'État membre d'émission (pts. 40-41). En outre, elle a rappelé que l'article 14 § 1 se borne à exiger que des voies de recours équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire soient applicables aux mesures d'enquête indiquées dans la DEE, sans imposer aux États membres de prévoir des voies de recours supplémentaires (points 25 à 27).

74. Dans son arrêt *M.N. (EncroChat)* du 30 avril 2024 (affaire C-670/22, EU:C:2024:372), la CJUE a examiné, en Grande chambre, une série de questions préjudicielles relatives à l'émission et à l'exécution de DEE ordonnées en vue d'obtenir la transmission de données collectées par les autorités françaises au moyen de la captation litigieuse.

Elle a jugé que l'autorité d'émission, lorsqu'elle a émis une DEE aux fins de transmission de preuves déjà en la possession des autorités de l'État d'exécution, n'est pas autorisée à contrôler la régularité de la procédure distincte par laquelle l'État membre d'exécution a collecté lesdites preuves (point 100).

Par ailleurs, elle a rappelé qu'en vertu de l'article 14 § 1 de la directive, les États membres doivent veiller à ce que des voies de recours équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire soient applicables à la mesure d'enquête faisant l'objet d'une DEE, la juridiction compétente devant dans ce cadre contrôler le respect des conditions d'émission d'une telle décision prévue à l'article 6 § 1 de la directive : il lui

revient, d'une part, de se prononcer sur la proportionnalité de la transmission de preuves sollicitée aux fins des procédures pénales engagées dans l'État d'émission et, d'autre part, de contrôler le respect des conditions prévues par le droit de l'État d'émission en matière de transmission de données issues dans une situation purement interne (points 101 à 103 et 87 à 95).

Enfin, elle a jugé que l'article 14 § 7 de 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, les informations et les éléments de preuve obtenus au moyen d'une DEE illégalement ordonnée si cette personne n'est pas en mesure de les commenter efficacement devant lui et si ceux-ci sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (points 130 et 131).

2. Droit interne

75. En droit français, la directive 2014/41 est transposée aux articles 694-15 à 694-50 et D47-1-1 à D47-1-29 du CPP.

76. S'agissant des voies de recours ouvertes dans le cadre de l'exécution d'une DEE, les dispositions pertinentes de ce code, dans leur version applicable à la date de la transmission des données, sont les suivantes :

Article 694-41

« Lorsque des mesures exécutées sur le territoire national en application d'une DEE auraient pu, si elles avaient été exécutées dans le cadre d'une procédure nationale, faire l'objet d'une contestation, d'une demande de nullité ou de toute autre forme de recours en application des dispositions du présent code, ces recours peuvent, dans les mêmes conditions et selon les mêmes modalités, être formés contre ces mesures par les personnes intéressés. Ces personnes sont informées de leur possibilité d'exercer ces recours lorsque cette information est prévue par les dispositions du présent code. »

Article D47-1-16

« Si un recours est formé contre la reconnaissance ou l'exécution de la DEE, le magistrat saisi en informe l'autorité d'émission, ainsi que de l'issue de ce recours. »

77. Ces dispositions ont été présentées par le ministre de la Justice (circulaire du 16 mai 2017, *BOMJ* nº 2017-06) dans les termes suivants :

« **3.1.4.2 Exécution des actes d'enquête demandés**

(...)

b) Contrôle juridictionnel des actes accomplis

En vertu de l'article 694-41 du code de procédure pénale, la mesure d'enquête exécutée sur notre territoire peut faire l'objet des mêmes recours que ceux prévus par le droit français dans le cadre d'une procédure nationale similaire, selon les mêmes conditions et les mêmes modalités. Ainsi, les personnes concernées par ces recours doivent être informées de leur possibilité de les exercer, dès lors que cette information est prévue par le code de procédure pénale. De même, ces recours ne suspendent pas l'exécution de la mesure d'enquête, sauf si une telle suspension est prévue par les

dispositions dudit code. En tout état de cause, les motifs de fond à l'origine de la DEE ne peuvent jamais être invoqués au soutien d'un recours intenté en France, le bien-fondé de cette décision ne pouvant en effet être contesté que par une action intentée dans l'Etat étranger d'émission. Si un recours est formé contre la reconnaissance de la décision (contre une commission rogatoire par exemple) ou contre un acte d'enquête d'exécution, le procureur de la république ou le juge d'instruction doit informer l'autorité étrangère de l'existence et de l'issue de ce recours. Cette obligation d'information, prévue à l'article D.47-1-16 du code de procédure pénale, n'est néanmoins pas prescrite à peine de nullité (...). »

D. Autres dispositions de procédure pénale

1. Le régime des nullités de procédure

78. Les dispositions du CPP permettant de solliciter l'annulation d'actes de procédure en cours d'instruction sont les suivantes :

Article 170

« En toute matière, la chambre de l'instruction peut, au cours de l'information, être saisie aux fins d'annulation d'un acte ou d'une pièce de la procédure par le juge d'instruction, par le procureur de la République, par les parties ou par le témoin assisté. »

Article 171

« Il y a nullité lorsque la méconnaissance d'une formalité substantielle prévue par une disposition du présent code ou toute autre disposition de procédure pénale a porté atteinte aux intérêts de la partie qu'elle concerne. »

Article 173, alinéa 3

« Si l'une des parties ou le témoin assisté estime qu'une nullité a été commise, elle saisit la chambre de l'instruction par requête motivée, dont elle adresse copie au juge d'instruction qui transmet le dossier de la procédure au président de la chambre de l'instruction. La requête doit, à peine d'irrecevabilité, faire l'objet d'une déclaration au greffe de la chambre de l'instruction. Elle est constatée et datée par le greffier qui la signe ainsi que le demandeur ou son avocat. (...) Lorsque le demandeur ou son avocat ne réside pas dans le ressort de la juridiction compétente, la déclaration au greffe peut être faite au moyen d'une lettre recommandée avec demande d'avis de réception. (...) »

Article 173-1, alinéa 1er

« Sous peine d'irrecevabilité, la personne mise en examen doit faire état des moyens pris de la nullité des actes accomplis avant son interrogatoire de première comparution ou de cet interrogatoire lui-même dans un délai de six mois à compter de la notification de sa mise en examen, sauf dans le cas où elle n'aurait pu les connaître. Il en est de même s'agissant des moyens pris de la nullité des actes accomplis avant chacun de ses interrogatoires ultérieurs ou des actes qui lui ont été notifiés en application du présent code. »

Article 174, alinéas 2 et 3

« La chambre de l'instruction décide si l'annulation doit être limitée à tout ou partie des actes ou pièces de la procédure viciée ou s'étendre à tout ou partie de la procédure ultérieure et procède comme il est dit au troisième alinéa de l'article 206.

Les actes ou pièces annulés sont retirés du dossier d'information et classés au greffe de la cour d'appel. Les actes ou pièces de la procédure partiellement annulés sont cancellés après qu'a été établie une copie certifiée conforme à l'original, qui est classée au greffe de la cour d'appel. Il est interdit de tirer des actes et des pièces ou parties d'actes ou de pièces annulés aucun renseignement contre les parties, à peine de poursuites disciplinaires pour les avocats et les magistrats. »

Article 802

« En cas de violation des formes prescrites par la loi à peine de nullité ou d'inobservation des formalités substantielles, toute juridiction, y compris la Cour de cassation, qui est saisie d'une demande d'annulation ou qui relève d'office une telle irrégularité ne peut prononcer la nullité que lorsque celle-ci a eu pour effet de porter atteinte aux intérêts de la partie qu'elle concerne. »

79. Par ailleurs, la personne poursuivie peut soulever une exception de nullité devant la juridiction répressive, à moins que la cause de nullité ait été purgée au cours de la procédure d'instruction (cf. articles 305-1 et 385 du CPP).

2. Le versement de matériaux issus d'une mesure de surveillance d'une procédure à une autre et sa contestation au plan interne

80. Dans une situation purement interne, la Cour de cassation juge qu'un magistrat peut annexer à une procédure pénale des éléments provenant d'une procédure distincte dont la production est de nature à contribuer à la manifestation de la vérité, à condition que cette jonction ait un caractère contradictoire et que les documents communiqués puissent être soumis à la discussion des parties (Crim., 7 décembre 2005, n° 05-85.876, *Bull. crim.* n° 327, et plus récemment, Crim., 14 décembre 2022, n° 21-86.427, publié au *Bulletin*).

81. Le cas échéant, la personne mise en examen peut solliciter l'annulation des pièces issues de cette autre procédure, en proposant des moyens tirés de l'irrégularité des actes accomplis dans celle-ci lorsqu'il invoque une atteinte à ses droits ou que les pièces versées sont susceptibles d'avoir été illégalement recueillies (Crim., 8 juin 2006, n° 06-81.796, *Bull. crim.* n° 166, Crim., 16 février 2011, n° 10-82.865, *Bull. crim.* n° 29 et Crim., 15 décembre 2015, n° 15-80.733, *Bull. crim.* n° 841). Elle est ainsi recevable à soutenir qu'une interception téléphonique ordonnée dans le cadre d'une procédure distincte, et dont les retranscriptions ont été versées à la procédure la concernant, méconnaît les exigences de l'article 8 de la Convention (Crim., 7 décembre 2005 et 8 juin 2006, précités). Cette

jurisprudence fait suite à l'arrêt *Matheron c. France* (n° 57752/00, 29 mars 2005).

82. La Cour de cassation a ainsi jugé qu'un utilisateur d'EncroChat, mis en examen dans le cadre d'une procédure séparée à laquelle ont été versées des pièces issues de la captation litigieuse, a qualité pour agir en nullité des opérations de captation en se prévalant d'une atteinte aux droits garantis par l'article 8 de la Convention, et ce dès lors qu'il résulte de la procédure que l'usage d'un téléphone crypté lui est imputé par les enquêteurs (Crim., 25 octobre 2022, n° 21-85.763, publié au *Bulletin*, §§ 49-67). S'agissant de la conciliation entre la preuve de la qualité à agir en annulation et le droit à ne pas contribuer à sa propre incrimination, la Cour de cassation a particulièrement jugé ce qui suit :

> « Vu les articles 6, § 1, de la [Convention] et 802 du code de procédure pénale :
>
> 49. Il résulte du premier de ces articles que toute personne a le droit de ne pas contribuer à sa propre incrimination.
>
> 50. La Cour européenne des droits de l'homme juge que ce droit présuppose que, dans une affaire pénale, l'accusation cherche à fonder son argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou les pressions, au mépris de la volonté de l'accusé.
>
> 51. Le droit de ne pas s'auto-incriminer constitue une protection non pas contre la tenue de propos incriminants en tant que telle mais contre l'obtention de preuves par la coercition ou l'oppression. Il concerne en premier lieu le respect de la détermination d'un accusé de garder le silence (CEDH, arrêt du 17 décembre 1996, *Saunders c. Royaume-Uni*, n° 19187/91 ; arrêt du 10 mars 2009, *Bykov c. Russie*, n° 4378/02).
>
> 52. Pour rechercher si une procédure a vidé de sa substance même le droit de ne pas contribuer à sa propre incrimination, il convient d'examiner la nature et le degré de coercition, l'existence de garanties appropriées dans la procédure et l'utilisation qui est faite des éléments ainsi obtenus.
>
> 53. En vertu du second de ces textes, en cas de violation des formes prescrites par la loi à peine de nullité ou d'inobservation des formalités substantielles, toute juridiction, qui est saisie d'une demande d'annulation ou qui relève d'office une telle irrégularité, ne peut prononcer la nullité que lorsque celle-ci a eu pour effet de porter atteinte aux intérêts de la partie qu'elle concerne.
>
> 54. La Cour de cassation en déduit que pour déterminer si le requérant a qualité pour agir en nullité, la chambre de l'instruction doit rechercher si la formalité substantielle ou prescrite à peine de nullité, dont la méconnaissance est alléguée, a pour objet de préserver un droit ou un intérêt qui lui est propre (Crim., 7 septembre 2021, pourvoi n° 21-80.642, publié au *Bulletin*).
>
> 55. Le moyen pose la question de savoir si, pour dénier au requérant qualité à agir en nullité, le juge peut lui opposer son choix de garder le silence ou ses dénégations, alors même qu'il résulte des investigations qu'il est concerné par la formalité dont il allègue qu'elle a été méconnue.
>
> 56. En premier lieu, il convient d'observer que la lettre de l'article 802 du code de procédure pénale ne s'oppose pas à ce que la preuve que la partie est concernée par la nullité résulte d'éléments de la procédure.

57. En deuxième lieu, dans l'hypothèse précitée, exiger du requérant qu'il justifie que l'acte critiqué a porté atteinte à un droit ou à un intérêt qui lui est propre a pour conséquence de le contraindre, sous peine d'être privé de son droit d'agir en nullité, à renoncer à exercer son droit au silence ou à revenir sur ses déclarations antérieures.

58. Cela peut aussi l'obliger, notamment lorsqu'est en cause un acte attentatoire à la vie privée, à admettre l'existence d'éléments à charge, voire à reconnaître les faits qui lui sont reprochés.

59. Or, les écrits du requérant devant la chambre de l'instruction, à l'appui de sa requête en nullité, sont susceptibles d'être pris en compte par la juridiction chargée de statuer sur son renvoi devant une juridiction de jugement ou de prononcer sur sa culpabilité.

60. Il s'ensuit, qu'en pareil cas, subordonner la recevabilité de l'action en nullité du requérant à la preuve par celui-ci qu'il est concerné par l'irrégularité est de nature à méconnaître son droit à ne pas s'auto-incriminer.

61. Enfin, le contentieux de l'annulation se rattachant au contentieux du bien-fondé de l'accusation, dès lors qu'il permet de contester la légalité du recueil d'un élément de preuve, il ne saurait être dénié au requérant qui est concerné par l'irrégularité le droit de contester la légalité d'un élément ainsi susceptible d'être retenu contre lui par l'accusation.

62. En conséquence, si le requérant n'allègue pas que la formalité méconnue a pour objet de préserver un droit ou un intérêt qui lui est propre, il appartient à la chambre de l'instruction de rechercher s'il résulte d'éléments de la procédure que tel pourrait être le cas. »

GRIEFS

83. Sous l'angle de l'article 8 de la Convention, les requérants se plaignent, d'une part, de la captation de données effectuée par les autorités françaises sur l'ensemble des terminaux reliés au réseau EncroChat, et, d'autre part, de la transmission aux autorités britanniques des données captées au Royaume-Uni. Ils critiquent la qualité des dispositions législatives relatives à la captation autant que la nécessité de ces ingérences.

84. Invoquant les articles 6 et 13 de la Convention, ils soutiennent par ailleurs qu'ils ne disposent d'aucun recours leur permettant de contester de manière effective les décisions ayant permis la captation de données litigieuse. Ils font valoir qu'ils n'ont pas qualité pour contester les décisions ayant ordonné la captation litigieuse dans le cadre de la procédure pénale française et se plaignent de ne pas pouvoir y accéder.

EN DROIT

A. Jonction des requêtes

85. Eu égard à la similarité de l'objet des requêtes, la Cour juge opportun de les examiner ensemble dans une décision unique.

B. Sur la violation alléguée de l'article 8 de la Convention

86. Les requérants se plaignent, d'une part, de la captation de données effectuée par les autorités françaises sur l'ensemble des terminaux reliés au réseau EncroChat, et, d'autre part, de la transmission aux autorités britanniques des données captées au Royaume-Uni. Ils invoquent l'article 8 de la Convention, dont les termes sont les suivants :

> « 1. Toute personne a droit au respect de sa vie privée et familiale (...) et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire (...) à la défense de l'ordre et à la prévention des infractions pénales (...) ou à la protection des droits et libertés d'autrui. »

Sur les exceptions préliminaires

a) Sur la juridiction de l'État défendeur

i. Thèses des parties

α) Le gouvernement défendeur

87. Le Gouvernement soutient que les faits dénoncés ne relèvent pas de la juridiction de la France et demande en conséquence à la Cour de déclarer les deux requêtes irrecevables.

88. Après avoir rappelé que la notion de « juridiction » est principalement territoriale, il fait valoir que les requérants se trouvent au Royaume-Uni, dont ils sont ressortissants et où ils sont poursuivis. À ses yeux, la circonstance que les données des requérants aient transité ou aient été stockées sur un serveur situé en France est fortuite et ne suffit pas à créer un lien de juridiction.

89. Il soutient que l'espèce ne relève par ailleurs d'aucune des exceptions au principe de territorialité reconnues par la jurisprudence (*M.N. et autres c. Belgique* (déc.) [GC], n° 3599/18, §§ 101-107, 5 mai 2020). Il considère en particulier qu'aucune circonstance d'ordre procédural n'est de nature à fonder un lien juridictionnel en l'espèce. S'il admet que les données litigieuses ont été captées dans le cadre d'une procédure pénale diligentée en France, il fait valoir que les requérants n'y sont pas parties, que les données collectées y sont conservées sous une forme ne permettant pas d'identifier les requérants et que les autorités françaises n'ont pas mené d'investigations à leur sujet.

90. Il ajoute que la France s'est bornée à transmettre des données brutes aux autorités britanniques correspondant à des utilisateurs inscrits à EncroChat sous des pseudonymes, sans être en mesure d'imputer ces données à quiconque à ce stade. Il soutient en substance que ces données ne sont devenues « personnelles » que grâce aux investigations menées par les enquêteurs britanniques. Or, il souligne que l'obligation de respecter les

droits de l'homme prévue par l'article 1er ne pèse qu'à l'égard des « personnes » relevant de sa juridiction.

91. Il fait enfin valoir que les faits litigieux relèvent principalement de la juridiction du Royaume-Uni. Il soutient qu'il incombe aux autorités britanniques de s'assurer de l'équité du procès pénal fait aux requérants (paragraphe 74 ci-dessus). En conséquence, il invite la Cour à éviter d'instaurer un conflit de juridictions.

β) Les requérants

92. Les requérants rappellent que la juridiction d'un État contractant peut s'étendre aux actes de ses organes qui déploient leurs effets en dehors de son territoire (*Al-Skeini et autres c. Royaume-Uni* [GC], no 55721/07, § 133, CEDH 2011). Ils soutiennent que la Cour n'a pas entendu confiner les exceptions au principe de territorialité dans une liste limitative.

93. Les requérants font valoir que la captation de données en cause est intervenue dans le cadre d'une procédure pénale régie par le droit français, grâce à une intervention sur un serveur situé en France. Selon eux, le fait que les données saisies n'aient pas pu être attribuées aux requérants avant leur transmission importe peu.

94. Par analogie, ils soulignent que la Cour a admis la juridiction d'un État requérant pour les conséquences qu'une demande d'extradition a emporté à l'étranger (*Stephens c. Malte (no 1)*, no 11956/07, §§ 50-52, 21 avril 2009, et *Vasiliciuc c. République de Moldova*, no 15944/11, §§ 21-25, 2 mai 2017). Ils font observer que la DEE est un instrument fondé sur le principe de la confiance mutuelle, de sorte que les autorités britanniques devraient pouvoir présumer de la licéité des preuves numériques transmises par la France.

95. En outre, ils soutiennent que la Cour a implicitement admis, dans l'affaire *Liberty et autres c. Royaume-Uni* (no 58243/00, 1er juillet 2008), la juridiction du Royaume-Uni sur des opérations d'interception de communications menées depuis des stations de radiodiffusion situées sur le sol britannique à l'égard de requérants installés en Irlande.

ii. Appréciation de la Cour

96. Seule la France est visée par les requêtes individuelles introduites par les requérants. Conformément à l'article 32 de la Convention, il revient à la Cour de déterminer si les actes incriminés sont imputables à cette Haute partie contractante (voir, par exemple, *Drozd et Janousek c. France et Espagne*, 26 juin 1992, § 91, série A no 240).

97. La jurisprudence relative à la notion de juridiction au sens de l'article 1er de la Convention a été présentée dans les affaires *M.N. et autres* (décision précitée, §§ 96-109) et *H.F. et autres c. France* ([GC], nos 24384/19 et 44234/20, §§ 184-188, 14 septembre 2022), auxquelles la Cour renvoie.

98. Elle rappelle que, du point de vue du droit international public, la compétence juridictionnelle d'un État est principalement territoriale. Celle-ci est présumée s'exercer normalement sur l'ensemble du territoire de l'État concerné. Cela étant, la Cour reconnaît, par exception au principe de territorialité, que des actes des États parties accomplis ou produisant des effets en dehors de leur territoire peuvent s'analyser en l'exercice par eux de leur juridiction au sens de l'article 1er de la Convention. Dans chaque cas, c'est au regard des faits particuliers de l'affaire qu'est appréciée l'existence de circonstances exceptionnelles justifiant de conclure à un exercice extraterritorial par l'État concerné de sa juridiction. Il s'agit avant tout d'une question de fait qui nécessite de s'interroger sur la nature du lien entre les requérants et l'État défendeur et de déterminer si celui-ci a effectivement exercé son autorité ou son contrôle sur eux (*M.N. et autres*, décision précitée, §§ 98-99 et 101-102, *Géorgie c. Russie (II)* [GC], no 38263/08, § 82, 21 janvier 2021, et *H.F. et autres*, précité, § 185).

99. La Cour a récemment appliqué ces critères en matière de surveillance de masse dans l'affaire *Wieder et Guarnieri c. Royaume-Uni* (nos 64371/16 et 64407/16, §§ 87-95, 12 septembre 2023). Elle a observé que chacune des étapes du processus de surveillance en cause (c'est-à-dire l'interception et la rétention des communications, leur criblage au moyens de sélecteurs spécifiques, leur analyse et l'utilisation des renseignements ainsi obtenus) avait été mise en œuvre depuis le territoire britannique par des services de renseignement britanniques et en a déduit que les requérants, bien qu'établis aux États-Unis et en Allemagne, relevaient de la juridiction du Royaume-Uni. La Cour a ainsi retenu sa compétence en se fondant sur le principe de territorialité.

100. De la même façon, la Cour examinera prioritairement si les actes dénoncés ont été commis en France. En l'espèce, les données litigieuses ont été captées au moyen d'une attaque informatique menée dans le cadre d'investigations confiées à des enquêteurs français agissant sous l'autorité de magistrats du tribunal judiciaire de Lille. Le Gouvernement ne conteste pas que les opérations de captation ont été menées depuis le territoire français. En outre, il résulte des pièces de la procédure que cette attaque informatique a été lancée depuis un serveur situé à Roubaix (paragraphes 7 et 18 ci-dessus). Il s'ensuit que la mesure de captation est imputable à la France. La circonstance que la captation des données ait produit une partie de ses effets en dehors du territoire français, en permettant d'accéder à distance aux données de terminaux situés à l'étranger, est sans incidence sur cette conclusion.

101. La Cour constate par ailleurs que les données concernant les utilisateurs d'EncroChat localisés au Royaume-Uni ont été collectées par les enquêteurs du C3N, avant d'être transmises à la *NCA* sur l'instruction du procureur de la République de Lille en exécution d'une DEE (paragraphe 36 ci-dessus). Il n'est pas soutenu que les données captées aient été conservées

hors de France. En outre, il résulte de procès-verbaux produits devant la Cour que les enquêteurs ont pu mettre la DEE britannique à exécution en agissant depuis le siège du C3N, qui est situé à Pontoise. La Cour tient donc pour établi que la conservation et le partage des données ont également été effectués depuis le territoire français.

102. S'il est exact que les données partagées avec les autorités britanniques ont ensuite fait l'objet d'une analyse ayant permis d'identifier un certain nombre d'individus et d'une utilisation à titre de preuve par les autorités britanniques dans le cadre de procédures engagées au Royaume-Uni – ces étapes étant sans nul doute les plus intrusives du processus (*Big Brother Watch et autres c. Royaume-Uni* [GC], nos 58170/13 et 2 autres, § 330, 25 mai 2021) –, ces actes ne figurent pas au nombre de ceux dont la Cour est saisie.

103. La Cour rappelle par ailleurs qu'une donnée a un caractère « personnel » dès lors qu'elle se rapporte à une personne identifiée ou identifiable (*Amann c. Suisse* [GC], no 27798/95, § 65, CEDH 2000-II). Elle touche alors à la vie privée d'un individu, peu important qu'elle soit conservée sous une forme codée intelligible uniquement à l'aide de l'informatique et ne pouvant être interprétée que par un nombre restreint de personnes (*S. et Marper c. Royaume-Uni* [GC], nos 30562/04 et 30566/04, § 67 et 75, CEDH 2008, et *Big Brother Watch et autres*, précité, § 330). Or, en l'espèce, il est clair que les données captées se rapportaient à des utilisateurs d'EncroChat et qu'elles étaient de nature à permettre leur identification (paragraphes 35, 38 et 39 ci-dessus). Dès lors, la circonstance que les utilisateurs d'EncroChat localisés au Royaume-Uni n'ont été identifiés qu'après l'exécution de la DEE n'ôte rien au caractère personnel des données transmises et n'affranchit pas la France de son obligation de respecter les droits des personnes concernées.

104. Il résulte de tout ce qui précède que la juridiction de la France est établie et que l'exception préliminaire tirée de l'incompétence de la Cour *ratione personae* doit être rejetée.

105. La Cour note, au demeurant, que cette conclusion se concilie avec la jurisprudence de la CJUE selon laquelle le principe de reconnaissance mutuelle des jugements et des décisions judiciaires interdit aux autorités ayant émis une DEE aux fins de transmission de ces données à titre de preuve de contrôler la régularité de la procédure distincte par laquelle ces preuves ont été collectées dans l'État membre d'exécution (arrêt *M.N. (EncroChat)*, cité au paragraphe 74 ci-dessus).

b) Sur la qualité de victime des requérants

i. Thèses des parties

α) Le gouvernement défendeur

106. Le Gouvernement sollicite le rejet des requêtes pour défaut de qualité de victime. Il souligne que les requérants ne reconnaissent pas l'utilisation

d'EncroChat, que ce soit dans le cadre du procès pénal dont ils font l'objet au Royaume-Uni ou devant la Cour. Dans ces conditions, il soutient que leurs requêtes s'apparentent à une *actio popularis*.

107. S'il ne conteste pas que les requérants se voient imputer l'utilisation d'EncroChat par l'accusation devant les juridictions britanniques, le Gouvernement fait observer que cette imputation ne résulte pas du fait des autorités françaises et que la France n'a pas à en répondre devant la Cour.

108. Il soutient par ailleurs qu'il n'y a pas lieu d'appliquer les tempéraments à la preuve de la qualité de victime de prévus en matière de surveillance secrète (*Roman Zakharov c. Russie* [GC], n° 47143/06, §§ 164-179, CEDH 2015), dans la mesure où la captation de données litigieuse a été opérée dans le cadre d'une enquête judiciaire et sous le contrôle d'un juge indépendant.

β) Les requérants

109. Les requérants font valoir que les autorités de poursuite britanniques les désignent comme des utilisateurs d'EncroChat et produisent à leur encontre des données issues de l'opération de captation à titre de preuves, et estiment que ces éléments suffisent à leur conférer la qualité de victime. Ils soulignent qu'ils ne peuvent revendiquer l'utilisation d'EncroChat sans s'exposer à ce que cette allégation soit retenue à leur encontre devant les juridictions britanniques.

ii. Observations du gouvernement intervenant

110. Le Gouvernement britannique confirme que les requérants se voient reprocher l'usage d'EncroChat dans des poursuites pendantes à leur encontre au Royaume-Uni.

iii. Appréciation de la Cour

111. Selon la jurisprudence constante de la Cour, la Convention ne reconnaît pas l'*actio popularis* et la Cour n'a pas normalement pour tâche d'examiner dans l'abstrait la législation et la pratique pertinentes, mais de rechercher si la manière dont elles ont été appliquées au requérant ou l'ont touché a donné lieu à une violation de la Convention (*Roman Zakharov*, précité, § 164, et *Verein KlimaSeniorinnen Schweiz et autres c. Suisse* [GC], n° 53600/20, § 460, 9 avril 2024). Pour pouvoir introduire une requête en vertu de l'article 34, une personne doit pouvoir démontrer qu'elle a « subi directement les effets » de la mesure litigieuse. Cette condition est nécessaire pour que soit enclenché le mécanisme de protection prévu par la Convention, même si ce critère ne doit pas s'appliquer de façon rigide, mécanique et inflexible tout au long de la procédure (*Centre de ressources juridiques au nom de Valentin Câmpeanu c. Roumanie* [GC], n° 47848/08, § 96, CEDH 2014, et *Kindlhofer c. Autriche*, n° 20962/15, § 26, 26 octobre 2021).

112. La Cour admet toutefois qu'un requérant puisse se prétendre victime d'une violation entraînée par la simple existence de mesures de surveillance secrète ou d'une législation permettant de telles mesures à la double condition qu'il puisse éventuellement être touché par la législation litigieuse, soit parce qu'il appartient à un groupe de personnes visées par elle, soit parce qu'elle concerne directement l'ensemble des usagers des services de communication en instaurant un système dans lequel tout un chacun peut voir intercepter ses communications, et qu'il ne dispose d'aucun recours effectif au plan interne (*Roman Zakharov*, précité, § 171, et *Centrum för rättvisa c. Suède* [GC], nº 35252/08, § 167, 25 mai 2021). Pour qu'un requérant puisse se dire victime dans une telle situation, il doit produire des preuves plausibles et convaincantes de la probabilité de survenance d'une violation dont il subirait personnellement les effets ; de simples soupçons ou conjectures ne suffisent pas à cet égard (*Senator Lines GmbH c. Autriche, Belgique, Danemark, Finlande, France, Allemagne, Grèce, Irlande, Italie, Luxembourg, Pays-Bas, Portugal, Espagne, Suède et Royaume-Uni* (déc.) [GC], nº 56672/00, CEDH 2004-IV).

113. En l'espèce, la Cour relève que la captation de données litigieuse a permis de collecter les données d'un grand nombre d'appareils connectés à EncroChat entre le 1er avril et le 2 juillet 2020 (paragraphes 26 et 33 ci-dessus). Si cette solution de communication chiffrée a compté plusieurs dizaines de milliers d'utilisateurs, elle fonctionnait en réseau fermé : les utilisateurs d'EncroChat ne pouvaient communiquer qu'entre eux, au moyen d'appareils téléphoniques dédiés fonctionnant sur abonnement (paragraphes 7, 8, 29 et 35 ci-dessus). De plus, cette solution de communication n'était pas librement commercialisée (paragraphes 8, 29 et 35 ci-dessus). Ainsi, même en prenant en compte le risque de surveillance indirecte (*Ekimdzhiev et autres c. Bulgarie*, nº 70078/12, § 263, 11 janvier 2022), la Cour constate que la mesure de captation ne pouvait donc concerner qu'un cercle de personnes déterminé, limité aux utilisateurs d'EncroChat, et non pas l'ensemble des usagers des services de communication téléphonique ou d'Internet (comparer avec *Roman Zakharov*, précité, § 175 et *Centrum för rättvisa*, précité, §§ 169-170). Il reste dès lors à déterminer si les requérants démontrent de façon suffisante qu'ils faisaient partie du groupe de personnes visé par la captation.

114. À cet égard, la Cour relève que les requérants ont été arrêtés à la suite de la captation litigieuse et que l'utilisation d'EncroChat leur est reprochée dans le cadre des poursuites dont ils font l'objet au Royaume-Uni (paragraphes 43, 44, 49 et 110 ci-dessus). Tous deux justifient de la production, par l'accusation, de preuves issues de la captation. Certes, les requérants contestent l'utilisation d'EncroChat devant les juridictions britanniques et ne se présentent pas comme des utilisateurs de cette solution de communication chiffrée devant la Cour. La Cour relève toutefois qu'une telle allégation pourrait peser lourdement dans l'appréciation de leur

culpabilité. Elle estime que les preuves qu'ils apportent suffisent à leur conférer la qualité de victime. Exiger d'eux qu'ils démontrent qu'ils étaient utilisateurs d'EncroChat à la date des faits reviendrait en effet à les contraindre à s'auto-incriminer (voir, *mutatis mutandis*, *Müdür Duman c. Turquie*, n° 15450/03, § 30, 6 octobre 2015) et constituerait un obstacle disproportionné à l'exercice efficace du droit de recours individuel prévu à l'article 34 de la Convention (voir, *mutatis mutandis*, *Vaney c. France*, n° 53946/00, § 53, 30 novembre 2004, et *Gaglione et autres c. Italie*, n°s 45867/07 et 69 autres, § 22, 21 décembre 2010).

115. En conséquence, la Cour rejette l'exception préliminaire du Gouvernement tirée du défaut de qualité de victime.

c) Sur l'épuisement des voies de recours internes

i. Thèses des parties

α) Le Gouvernement défendeur

116. Le Gouvernement excipe du non-épuisement des voies internes.

117. Premièrement, il soutient que les requérants auraient dû porter leurs contestations relatives à la transmission et à l'imputation des données devant les juridictions britanniques avant d'introduire leurs requêtes contre la France.

118. Deuxièmement, il considère que les requérants disposaient de voies de recours pouvant passer pour effectives devant les juridictions françaises, dont ils auraient dû faire usage.

119. Il fait d'abord valoir que les requérants auraient pu solliciter l'annulation de la transmission des données aux autorités britanniques aux fins de versement à des procédures pénales distinctes en tant que preuves devant la chambre de l'instruction sur le fondement de l'article 694-41 du CPP (paragraphe 76 ci-dessus). Il souligne que ce recours est ouvert à toute « personne intéressée » et qu'il aurait permis aux requérants de se prévaloir de la jurisprudence bien établie qui permet, dans une situation purement interne, de solliciter l'annulation du versement de pièces issues d'une autre procédure au motif qu'elles ont été obtenues dans des conditions contraires à l'article 8 de la Convention (paragraphes 81-82 ci-dessus). Ce faisant, les requérants auraient pu soumettre l'ensemble de leurs griefs aux juridictions internes.

120. Il fait ensuite valoir que les requérants pouvaient contester la conservation des données les concernant en exerçant leurs droits d'information, d'accès, de rectification, d'effacement et de limitation du traitement des données dans les conditions prévues par l'article 7 du décret du 18 décembre 2015 (paragraphe 69 ci-dessus). Si le Gouvernement admet que les droits des personnes concernées peuvent être restreints pour différents motifs et notamment pour éviter de gêner des enquêtes en cours, il indique que la mise en œuvre d'une telle restriction permet de saisir la CNIL aux fins

de vérification et ouvre droit à un recours juridictionnel en vertu de l'article 108 de la loi du 6 janvier 1978 (paragraphe 67 ci-dessus). Il souligne que la procureure de la République de Lille a annoncé, lors d'une conférence de presse à Eurojust, la création d'une adresse courriel dédiée permettant de solliciter l'effacement de données captées (paragraphe 34 ci-dessus). Or, il indique qu'aucune demande d'effacement n'est parvenue au responsable du traitement.

β) Les requérants

121. Les requérants soutiennent d'abord que l'exigence d'épuisement des voies de recours internes ne doit s'apprécier qu'à l'aune des voies de recours ouvertes dans l'État contractant à l'encontre duquel leurs requêtes sont dirigées. La circonstance qu'ils n'aient pas épuisé certains recours au Royaume-Uni leur parait donc indifférente. À titre subsidiaire, ils font valoir que la *High Court of Justice* a jugé, lors de l'examen d'un recours présenté par un tiers à l'encontre de la DEE émise par le Royaume-Uni le 11 mars 2020, qu'elle n'est pas compétente pour apprécier la légalité des opérations de captation et leur conformité au droit français (paragraphe 51 ci-dessus).

122. Ils relèvent ensuite qu'à défaut d'avoir la qualité de partie à la procédure pénale dans laquelle la captation a été ordonnée, ils ne peuvent accéder au dossier pénal et contester la validité des décisions de captation dans ce cadre.

123. Le premier requérant soutient par ailleurs que le recours prévu par l'article 694-41 du CPP ne lui permet de contester que la mesure aux fins de laquelle la DEE du 11 mars 2020 a été émise, à savoir la transmission des données captées aux autorités britanniques, et non la mesure de captation de données initialement ordonnée par les autorités françaises.

124. Les deux requérants contestent enfin la disponibilité et l'effectivité du recours fondé sur l'article 7 du décret du 18 décembre 2015 invoqué par le Gouvernement. À cet égard, ils font valoir que l'exercice d'un tel recours exigeait d'eux qu'ils s'identifient (paragraphe 68 ci-dessus) et qu'ils revendiquent l'utilisation d'un terminal EncroChat, en endossant le risque que cette allégation soit retenue à leur encontre sur le plan pénal. Ils ajoutent que le responsable de traitement peut restreindre le droit d'effacement ou de limitation des données captées sur le fondement de l'article 7, II du décret du 18 décembre 2015 (paragraphe 69 ci-dessus) ou encore outre s'opposer à leur effacement sur le fondement de l'article 106, II, 2° de la loi du 6 janvier 1978 (paragraphe 67 ci-dessus). Ils affirment par ailleurs que ce recours ne permet pas d'examiner la légalité des décisions de captation critiquées et soutiennent que l'effacement des données ne constitue pas un remède effectif à leurs griefs.

ii. Observations du gouvernement intervenant

125. Le gouvernement britannique expose que la légalité de la DEE émise par le Royaume-Uni est susceptible de recours devant la *High Court of Justice*, sa contrariété à la Convention pouvant être invoquée dans ce cadre.

126. Il indique qu'un tel recours a été présenté par un tiers à l'encontre de la DEE du 11 mars 2020, le second requérant étant intervenu à l'instance en qualité de partie intéressée. Notant qu'aucun moyen de conventionnalité n'a été développé a cette occasion, il indique que ce recours a été rejeté le 26 octobre 2020 (paragraphe 51 ci-dessus). Il observe en outre que le premier requérant s'est abstenu de présenter un tel recours ou d'intervenir à l'instance.

iii. Appréciation de la Cour

α) Principes généraux

127. La Cour rappelle que le mécanisme de sauvegarde instauré par la Convention revêt un caractère subsidiaire par rapport aux systèmes nationaux de garantie des droits de l'homme, ce principe étant inscrit au Préambule de la Convention depuis l'entrée en vigueur du Protocole n° 15 le 1er août 2021. La Cour a la charge de surveiller le respect par les États contractants de leurs obligations découlant de la Convention. Elle ne doit pas se substituer à eux, et il leur incombe en premier lieu de veiller à ce que les droits et libertés fondamentaux consacrés par la Convention soient respectés et protégés au niveau interne (*Vučković et autres c. Serbie* (exception préliminaire) [GC], nos 17153/11 et 29 autres, § 69, 25 mars 2014, et *Communauté genevoise d'action syndicale (CGAS) c. Suisse* [GC], n° 21881/20, § 138, 27 novembre 2023).

128. L'obligation d'épuiser les recours internes impose aux requérants de faire un usage normal des recours disponibles et suffisants pour leur permettre d'obtenir réparation des violations qu'ils allèguent. Ces recours doivent exister à un degré suffisant de certitude, en pratique comme en théorie, sans quoi leur manquent l'effectivité et l'accessibilité voulues (*Akdivar et autres*, précité, § 66, *Vučković et autres*, précité, § 71, et *Communauté genevoise d'action syndicale (CGAS)*, précité, § 139). Pour pouvoir être jugé effectif, un recours doit être susceptible de remédier directement à la situation incriminée et présenter des perspectives raisonnables de succès (*Balogh c. Hongrie*, n° 47940/99, § 30, 20 juillet 2004, *Sejdovic c. Italie* [GC], n° 56581/00, § 46, CEDH 2006-II, et *Vučković et autres*, précité, § 74).

129. Le caractère approprié et suffisant du redressement offert aux requérants dépend de l'ensemble des circonstances de la cause, eu égard en particulier à la nature de la violation de la Convention qui se trouve en jeu (*Gäfgen c. Allemagne* [GC], n° 22978/05, § 116, CEDH 2010). En matière de mesures attentatoires aux droits garantis par l'article 8 ordonnées dans le cadre de procédures pénales, l'effectivité des remèdes internes dépend essentiellement des particularités du système juridique de l'État défendeur et

des circonstances de l'affaire dont il s'agit (*Contrada c. Italie (nº 4)*, nº 2507/19, § 51, 23 mai 2024, et *Gernelle et S.A. Société d'exploitation de l'hebdomadaire Le Point c. France* (déc.), nº 18536/18, § 43, 9 avril 2024). Pour être considéré comme effectif aux fins de l'épuisement des voies de recours internes, un recours doit avant tout permettre un contrôle de la légalité et de la nécessité de la mesure attentatoire (voir, parmi d'autres, *Gutsanovi c. Bulgarie*, nº 34529/10, § 210 211, CEDH 2013 (extraits)). En outre, en cas de constat d'irrégularité, le recours doit offrir un redressement adéquat (voir, parmi d'autres, *Budak c. Turquie*, nº 69762/12, § 46, 16 février 2021).

130. Enfin, selon une jurisprudence constante, la règle de l'épuisement des recours internes doit être appliquée avec une certaine souplesse et sans formalisme excessif. Elle ne s'accommode pas d'une application automatique et ne revêt pas un caractère absolu ; en en contrôlant le respect, il faut avoir égard aux circonstances de la cause (voir, parmi beaucoup d'autres, *Gherghina c. Roumanie* (déc.) [GC], nº 42219/07, § 87, 9 juillet 2015). Rien n'impose d'user de recours qui ne sont ni adéquats ni effectifs (*Akdivar et autres*, précité, § 67, et *Communauté genevoise d'action syndicale (CGAS)*, précité, § 141). Cela étant, le simple fait de nourrir des doutes quant aux perspectives de succès d'un recours donné qui n'est pas de toute évidence voué à l'échec ne constitue pas une raison propre à justifier la non-utilisation du recours en question (*Scoppola c. Italie (nº 2)* [GC], nº 10249/03, § 70, 17 septembre 2009, *Vučković et autres*, précité, § 74 et *Communauté genevoise d'action syndicale (CGAS)*, précité, § 142). Dans un ordre juridique où les droits fondamentaux sont protégés, il incombe à l'individu lésé d'éprouver l'ampleur de cette protection en donnant aux juridictions nationales la possibilité de faire évoluer ces droits par la voie de l'interprétation (*Gherghina*, décision précitée, § 101, et *Communauté genevoise d'action syndicale (CGAS)*, précité, § 159).

β) Application en l'espèce

131. La Cour relève que les données des utilisateurs d'EncroChat ont été collectées à l'initiative des autorités françaises, au moyen d'une mesure de captation ordonnée dans le cadre d'une procédure pénale ouverte à la JIRS de Lille. Les données concernant les individus qui utilisaient EncroChat au Royaume-Uni ont ensuite été transmises, en tant qu'éléments de preuves déjà en possession des autorités françaises, en exécution d'une DEE émise par le *CPS* britannique (paragraphes 35-36 ci-dessus) en vue d'être versées à d'autres dossiers pénaux à titre de preuves, comme ce fut le cas pour les deux requérants. Rien n'indique que la mesure de captation ait été effectuée à la demande des autorités britanniques, celles-ci s'étant bornées à solliciter la transmission d'une partie des matériaux collectés.

132. Si le gouvernement défendeur soutient qu'il incombait aux requérants d'épuiser les voies de recours ouvertes au Royaume-Uni, la Cour relève qu'il résulte des termes mêmes de l'article 35 § 1 que l'exigence

d'épuisement porte sur les voies de recours « internes ». Elle rappelle que cette exigence vise à permettre aux États contractants de redresser la situation dans leur ordre juridique interne avant d'avoir à répondre de leurs actes devant un organisme international (voir, parmi beaucoup d'autres, *Akdivar et autres c. Turquie*, 16 septembre 1996, § 65, *Recueil des arrêts et décisions* 1996-IV). Pour l'application de ce texte, seules les voies de recours ouvertes dans l'État contractant à l'encontre duquel une requête individuelle a été introduite doivent donc être prises en considération. Au demeurant, ni la circonstance que les requérants résident hors du territoire français ni la circonstance qu'ils n'aient pas choisi de leur plein gré de se placer sous la juridiction de l'État défendeur ne sont de nature à les exempter de leur obligation d'épuiser les voies de recours internes ouvertes dans cet État (voir, *mutatis mutandis*, *Demopoulos et autres c. Turquie* (déc.) [GC], nos 46113/99 et 7 autres, §§ 98 et 101, CEDH 2010, et *Ukraine et Pays-Bas c. Russie* (déc.) [GC], nos 8019/16 et 2 autres, § 772, 30 novembre 2022).

133. Il reste donc à déterminer si les requérants disposaient, en France, d'un recours satisfaisant aux exigences de l'article 35.

– *Sur l'existence et la disponibilité du recours prévu à l'article 694-41 du CPP*

134. En droit français, l'article 694-41 du CPP (paragraphe 76 ci-dessus) prévoit qu'une mesure prise sur le territoire français en exécution d'une DEE peut faire l'objet d'une contestation, d'une demande de nullité ou de toute autre forme de recours dès lors qu'une telle mesure aurait pu faire l'objet d'un recours si elle avait été exécutée dans une procédure nationale. Le cas échéant, la mesure prise en exécution d'une DEE peut être contestée dans les mêmes conditions et selon les mêmes modalités qu'elle aurait pu l'être dans une situation purement interne.

135. La Cour relève que les dispositions de cet article permettent à toute « personne intéressée » d'exercer les recours qui lui seraient ouverts en France si la mesure effectuée en exécution d'un DEE avait été exécutée dans le cadre d'une procédure interne. Elles permettent donc aux requérants de se prévaloir des droits procéduraux que leur confèrerait un tel statut dans une situation purement interne.

136. Ces dispositions transposent en droit interne l'article 14 de la directive 2014/41, qui prévoit que les États membres doivent veiller à ce que des voies de recours équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire soient applicables aux mesures d'enquête indiquées dans une DEE (paragraphe 70 ci-dessus), et qui doit être lu à la lumière de son considérant 22 (paragraphe 71 ci-dessus). La Cour note qu'elles paraissent se concilier de façon cohérente avec la jurisprudence de la CJUE selon laquelle les États membres sont tenus d'assurer le respect du droit à un recours effectif consacré à l'article 47 de la Charte dans le cadre de la procédure d'émission et d'exécution d'une DEE (arrêt *Gavanozov II*, cité au paragraphe 73 ci-dessus, points 28 et 29).

137. Lorsqu'une DEE a été émise en vue d'obtenir la transmission de preuves qui se trouvent déjà en possession des autorités de l'État membre d'exécution, la CJUE juge que les autorités de l'État d'émission ne sont pas autorisées à contrôler la régularité de la procédure distincte par laquelle l'État membre d'exécution les a collectées (arrêt *M.N. (EncroChat)*, cité au paragraphe 74 ci-dessus, point 100). Compte tenu des engagements internationaux des États concernés, les recours ouverts dans l'État d'exécution revêtent, aux yeux de la Cour, une importance déterminante.

– *Sur la portée du recours prévu à l'article 694-41 du CPP*

138. La Cour constate que, dans une situation purement interne, une personne mise en examen ou renvoyée devant une juridiction pénale peut solliciter l'annulation de pièces de procédure.

139. Elle relève plus particulièrement que le versement au dossier d'une procédure pénale d'éléments de preuves obtenus dans le cadre d'une procédure distincte est un acte susceptible d'être contesté dans le cadre d'une requête en nullité (voir, déjà, *Versini-Campinchi et Crasnianski c. France*, n° 49176/11, § 29, 16 juin 2016). Selon une jurisprudence bien établie, la personne mise en examen est alors fondée à soutenir que ces preuves ont été obtenues de façon illicite et peut solliciter l'annulation des pièces issues de cette procédure distincte, en invoquant des moyens tirés de l'irrégularité des actes accomplis dans le cadre de celle-ci. En particulier, elle peut invoquer la violation des droits garantis par la Convention et ainsi contester la régularité et la nécessité de la technique d'enquête initialement mise en œuvre (paragraphe 81 ci-dessus).

140. En application de l'article 694-41 du CPP, les requérants pouvaient donc demander l'annulation de la mesure d'exécution de la DEE du 11 mars 2020 dans les mêmes conditions et selon les mêmes modalités qu'aurait pu le faire une personne mise en examen en France, en faisant valoir qu'ils se trouvaient dans une situation procédurale comparable et que les mesures de captation litigieuses étaient contraires aux exigences de l'article 8 de la Convention. Une requête en nullité pouvait ainsi être déposée devant la chambre de l'instruction, sous réserve du respect des conditions de forme et de délai prévues par le droit interne (paragraphe 78 ci-dessus).

141. La Cour constate par ailleurs que la mise en œuvre de ce recours n'exigeait pas des requérants qu'ils s'auto-incriminent, la jurisprudence interne admettant la recevabilité d'une telle requête en nullité dès lors que son auteur se voit reprocher l'usage d'EncroChat dans la procédure diligentée à son encontre (paragraphe 82 ci-dessus).

142. Le Gouvernement démontre ainsi de façon convaincante que les requérants disposaient d'une voie de recours permettant de contester la légalité et la proportionnalité de la captation des données et de leur transmission aux autorités britanniques aux fin de versement à leur dossier pénal à titre de preuves.

143. La Cour rappelle en tout état de cause que lorsqu'un doute existe quant à l'efficacité d'un recours interne, c'est là un point qui doit être soumis aux tribunaux nationaux (*Roseiro Bento c. Portugal* (déc.), nº 29288/02, CEDH 2004-XII (extraits), *Lienhardt c. France* (déc.), nº 12139/10, 13 septembre 2011, et *Thevenon c. France* (déc.), nº 46061/21, § 57, 13 septembre 2022).

– *Sur les modalités de redressement prévues par ce recours*

144. Un tel recours permet, s'il est fondé, de constater la méconnaissance de l'article 8 de la Convention et d'obtenir, en France, l'annulation de la mesure d'exécution de la DEE. En outre, l'article D47-1-16 du CPP prévoit que l'État membre d'émission est informé de l'existence et de l'issue de ce recours. Or, l'article 14 § 7 de la directive 2014/41 impose à l'État d'émission de tenir compte du fait que la reconnaissance ou l'exécution d'une DEE a été contestée avec succès, conformément à son droit national (paragraphe 70 ci-dessus). Aux yeux de la Cour, de telles modalités de redressement, qui résultent à la fois du droit de l'Union européenne et des dispositions prises pour en assurer la transposition en droit français, doivent être regardées comme appropriées. Rien n'indique que ce recours, s'il avait été exercé, aurait été privé d'effet utile dans les circonstances de l'espèce, les poursuites diligentées à l'encontre des requérants étant toujours pendantes et les juridictions britanniques étant tenues de tenir compte de son succès éventuel.

– *Conclusion*

145. Au vu de l'ensemble de ce qui précède, la Cour considère que les requérants disposaient d'une voie de recours permettant de contester de façon effective la mesure de transmission de données prise en exécution de la DEE émise le 11 mars 2020, ainsi que la mesure de captation ayant permis de les collecter. Or, les requérants n'ont exercé aucun recours devant les juridictions françaises et ne justifient d'aucune circonstance particulière qui les auraient dispensés de le faire. Les juridictions internes ont ainsi été privées de la possibilité de développer leur jurisprudence sur la question, ce qui aurait été potentiellement bénéfique à tous les autres justiciables se trouvant dans une situation similaire ou analogue (*Gherghina*, décision précitée, § 106). La Cour constate donc qu'ils n'ont pas satisfait à l'exigence d'épuisement des voies de recours internes et déclare le grief tiré de l'article 8 irrecevable en application de l'article 35 §§ 1 et 4 de la Convention.

C. Sur la violation alléguée des articles 6 et 13 de la Convention

146. Invoquant les articles 6 et 13 de la Convention, les requérants soutiennent qu'ils ne disposent d'aucun recours leur permettant de contester de manière effective la captation de données litigieuse.

147. Cependant, il résulte de ce qui précède que les requérants disposaient d'un recours effectif à l'encontre de cette mesure. Il s'ensuit que ce grief est manifestement mal fondé et doit être rejeté en application de l'article 35 §§ 3 a) et 4 de la Convention.

PAR CES MOTIFS, LA COUR, À L'UNANIMITÉ,

1. *Décide* de joindre les requêtes ;

2. *Déclare* les requêtes irrecevables.

Fait en français, puis communiqué par écrit le 17 octobre 2024, en application de l'article 77 §§ 2 et 3 du règlement.

Martina Keller Greffière adjointe	Lado Chanturia Président