# N° 110

# SÉNAT

SESSION ORDINAIRE DE 2023-2024

Enregistré à la Présidence du Sénat le 15 novembre 2023

# RAPPORT D'INFORMATION

FAIT

*au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur les* **modalités** *d'***investigation** *recourant aux* **données** *de* **connexion** *dans le cadre des* **enquêtes pénales***,*

Par Mme Agnès CANAYER et M. Philippe BONNECARRÈRE,

Sénateurs

*(1) Cette commission est composée de :* M. François-Noël Buffet*, président ;* M. Christophe-André Frassa, Mme Marie-Pierre de La Gontrie, MM. Marc-Philippe Daubresse, Jérôme Durain, Philippe Bonnecarrère, Thani Mohamed Soilihi, Mme Cécile Cukierman, MM. Dany Wattebled, Guy Benarroche, Mme Nathalie Delattre*, vice-présidents ;* Mmes Agnès Canayer, Muriel Jourda, M. André Reichardt, Mme Isabelle Florennes*, secrétaires ;* MM. Jean-Michel Arnaud, Philippe Bas, Mme Nadine Bellurot, MM. Olivier Bitz, François Bonhomme, Hussein Bourgi, Ian Brossat, Christophe Chaillou, Mathieu Darnaud, Mmes Catherine Di Folco, Françoise Dumont, Jacqueline Eustache-Brinio, Françoise Gatel, Laurence Harribey, Lauriane Josende, MM. Éric Kerrouche, Henri Leroy, Stéphane Le Rudulier, Mme Audrey Linkenheld, MM. Alain Marc, Hervé Marseille, Michel Masset, Mmes Marie Mercier, Corinne Narassiguin, M. Paul Toussaint Parigi, Mme Olivia Richard, M. Pierre-Alain Roiron, Mmes Elsa Schalck, Patricia Schillinger, M. Francis Szpiner, Mmes Lana Tetuanui, Dominique Vérien, M. Louis Vogel, Mme Mélanie Vogel.

# S O M M A I R E

Pages

**L'ESSENTIEL..... 9**

**I. LES DONNÉES DE CONNEXION, PIERRE ANGULAIRE DE L'ENQUÊTE PÉNALE .....10**

A. LES MÉTADONNÉES, DES DONNÉES SENSIBLES AUX USAGES MULTIPLES.....10

B. LA STRUCTURATION PROGRESSIVE D'UN USAGE DEVENU MASSIF.....11

**II. DES DROITS NATIONAUX BOULEVERSÉS LA JURISPRUDENCE DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE.....11**

A. UNE JURISPRUDENCE DRASTIQUEMENT LIMITATIVE.....11

B. EN EUROPE, DES ÉTATS DÉBOUSSOLÉS, UNE UNION DÉSTABILISÉE.....12

**III. LES LIMITES DES TENTATIVES FRANÇAISES DE MISE EN CONFORMITÉ ...13**

A. UNE CONSERVATION QUI DEMEURE GÉNÉRALE ET INDIFFÉRENCIÉE.....13

B. UN ACCÈS MIEUX DÉLIMITÉ MAIS TOUJOURS PAS SOUMIS À UN CONTRÔLE PRÉALABLE.....15

**IV. AGIR EN FRANCE ET EN EUROPE POUR SÉCURISER LE RECOURS AUX MÉTADONNÉES DANS L'ENQUÊTE PÉNALE.....16**

A. EN EUROPE, ASSUMER UNE POSITION FORTE.....16

B. DANS LA LOI FRANÇAISE, TROUVER LE POINT D'ÉQUILIBRE ENTRE EXIGENCE ET PRAGMATISME.....17

C. PRÉSERVER LE QUOTIDIEN DES ENQUÊTEURS ET ÉVITER LE « CHOC PROCÉDURAL ».....18

**LISTE DES PROPOSITIONS.....21**

**INTRODUCTION.....23**

**PREMIÈRE PARTIE LES DONNÉES DE CONNEXION, NOUVELLE PIERRE ANGULAIRE DE L'ENQUÊTE PÉNALE.....27**

**I. LES DONNÉES DE CONNEXION : DES INFORMATIONS SENSIBLES AUX USAGES MULTIPLES.....27**

A. LES DONNÉES DE CONNEXION : UNE NOTION TECHNIQUE SAISIE PAR LE DROIT PÉNAL.....27

*1. Une définition technique des données de connexion.....27*

*2. Une définition juridique difficile.....30*

B. UN RÔLE DÉSORMAIS CENTRAL DANS L'ÉLUCIDATION DES INFRACTIONS ...33
*1. De l'utilité des métadonnées dans l'enquête pénale* ...33
*2. L'émergence d'un monopole probatoire* ...35

**II. LA STRUCTURATION PROGRESSIVE D'UN USAGE DEVENU MASSIF ...37**

A. UN ACCÈS LARGE QUI CONCERNE PLUSIEURS CENTAINES DE MILLIERS DE DONNÉES CHAQUE ANNÉE ...37

B. LA « MISE EN ORDRE » PROGRESSIVE DES ACCÈS ...40
*1. Un accès initialement décentralisé, coûteux et peu régulé* ...40
*2. La régulation par la technique : la création de l'agence ANTENJ* ...44

C. LA PNIJ : UN SUCCÈS INDÉNIABLE, ENTRAVÉ PAR DES « ANGLES MORTS » ...46
*1. Un périmètre techniquement limité* ...47
*2. Des usages extérieurs ou parallèles à la PNIJ qui soulèvent des interrogations* ...48

**DEUXIÈME PARTIE DES DROITS NATIONAUX BOULEVERSÉS PAR LA JURISPRUDENCE DE LA CJUE ...53**

**I. UN RECOURS AUX DONNÉES DE CONNEXION PROFONDÉMENT DESTABILISÉ PAR LA JURISPRUDENCE DE LA CJUE ...53**

A. UN ENCADREMENT SCRUPULEUX DU RECOURS AUX DONNÉES DE CONNEXION ...53

B. UNE JURISPRUDENCE À L'ASSISE CONTESTABLE ...56

**II. DES INQUIÉTUDES PROFONDES QUI REJAILLISSENT SUR L'UNION EUROPÉENNE ...58**

***A. EN EUROPE, DES ÉTATS DÉBOUSSOLÉS*** ...58
***1. Le choix contraint d'un régime sans obligation légale de conservation des métadonnées, une impasse pour les autorités*** ...59
*a) Le vide juridique créé par la sanction des régimes de conservation générale et indifférenciée des données* ...60
*b) Une volonté de réforme pour combler les fragilités créées par l'absence de régime légal de conservation des données* ...61
***2. L'adoption d'un système de conservation ciblée, un faux-semblant ?*** ...63
*a) Le système de conservation ciblée applicable en Belgique et au Danemark* ...63
*b) Un ciblage contourné* ...64
***3. Les régimes de conservation proportionnée : un compromis précaire entre efficacité du système et conformité au droit de l'union*** ...66
*a) Un régime de conservation mieux encadré* ...66
*b) Des garanties supplémentaires en matière d'accès aux données de connexion en « gage » du maintien d'une conservation large* ...67

***B. DES PERSPECTIVES EUROPÉENNES INCERTAINES*** ...68
***1. La mise en suspens de négociations sur des textes-clés pour l'avenir de l'Union*** ...68
***2. Des tentatives de coordination entre États membres : le groupe d'experts de haut niveau Going dark*** ...74

**TROISIÈME PARTIE LES LIMITES DES TENTATIVES FRANÇAISES DE MISE EN CONFORMITÉ AVEC LE DROIT DE L'UNION EUROPÉENNE ..... 78**

**I. LA CONSERVATION DES DONNÉES DE CONNEXION : LA CONSTRUCTION PROGRESSIVE D'UNE CONSERVATION CIRCONSTANCIÉE ..... 78**

***A. AVANT 2021, UNE OBLIGATION DE CONSERVATION GÉNÉRALISÉE CONTRAIRE TANT AU DROIT DE L'UNION EUROPÉENNE QU'À LA CONSTITUTION*** ..... 78

***B. LA POSITION DU CONSEIL D'ÉTAT : UNE TENTATIVE DE CONSTRUCTIVISME JURISPRUDENTIEL*** ..... 79

***C. LA LOI « RENSEIGNEMENT » DE 2021 : L'INSCRIPTION LÉGISLATIVE DU MODÈLE DESSINÉ PAR LE CONSEIL D'ÉTAT*** ..... 81

***D. DES INCERTITUDES PERSISTANTES*** ..... 84

**II. L'ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES : UNE PROCÉDURE ENCORE EN SUSPENS ..... 86**

***A. LE RESPECT DES CRITÈRES PERMETTANT L'ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES : CRIMINALITÉ GRAVE, NÉCESSITÉ ET PROPORTIONNALITÉ*** ..... 86

***1. L'encadrement progressif par le législateur des infractions permettant un accès aux données de connexion dans le cadre des enquêtes pénales*** ..... 86

***2. Les arrêts de la Cour de cassation du 12 juillet 2022 : l'institution d'un faisceau d'indices pour définir la criminalité grave*** ..... 88

***3. La criminalité grave : une notion dont l'appréciation doit continuer à relever du droit national*** ..... 89

***B. LA NÉCESSITÉ D'UN CONTRÔLE PRÉALABLE ET INDÉPENDANT*** ..... 91

***1. Les exigences posées par la CJUE*** ..... 91

***2. Les conséquences qu'en a tirées la Cour de cassation*** ..... 92

***3. Une position fragile*** ..... 93

**QUATRIÈME PARTIE AGIR EN FRANCE ET EN EUROPE POUR SÉCURISER LE RECOURS AUX DONNÉES DE CONNEXION DANS L'ENQUÊTE PÉNALE ..... 94**

**I. AGIR EN EUROPE DANS LE SENS D'UN PLUS GRAND PRAGMATISME ..... 94**

A. PLAIDER POUR UNE MEILLEURE PRISE EN COMPTE DES BESOINS OPÉRATIONNELS DES SERVICES D'ENQUÊTE ..... 94

*1. Assumer une position forte dans les négociations européennes* ..... 94

*2. Renforcer la transparence du processus européen* ..... 96

B. ŒUVRER AU DÉVELOPPEMENT DES « SOUPAPES » OUVERTES PAR LA COUR DE LUXEMBOURG ET MIEUX LES INTÉGRER AU DROIT INTERNE ..... 97

**II. ADAPTER LES NORMES FRANÇAISES À L'IMPÉRATIF D'UN CONTRÔLE PRÉALABLE DES ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES ..... 98**

***A. EN FRANCE, UN FORT SENTIMENT D'INSÉCURITÉ JURIDIQUE DES ACTEURS DE L'ENQUÊTE*** ..... 98

*B. ADAPTER LES MODALITÉS DE CONTRÔLE DE L'ACCÈS AUX DONNÉES DE CONNEXION AUX CONTRAINTES DU TERRAIN*....101
*1. Un contrôle exigeant*....*101*
*2. Un contrôle pleinement conforme aux exigences de la CJUE*....*102*
*a) La piste d'un contrôle par une entité indépendante*....102
*b) La piste d'un contrôle par une juridiction*....103
*3. Des modalités de contrôle pragmatiques*....*105*

*C. UNE OPPORTUNITÉ POUR UNE REFONTE DU CADRE DE LA PREUVE*....106

**III. GARANTIR LA FLUIDITÉ DE LA CHAÎNE PÉNALE POUR PROTÉGER LES ACTEURS DE L'ENQUÊTE DU « CHOC PROCÉDURAL »....108**

A. CONFORTER LE RÔLE PIVOT DE LA PNIJ....108

B. EVITER LE « CHOC PROCÉDURAL »....111
*1. Calibrer la procédure d'autorisation pour maîtriser la charge de travail des enquêteurs*....*112*
*2. Intégrer le sujet des données de connexion aux chantiers informatiques en cours*....*116*

**EXAMEN EN COMMISSION....121**

**LISTE DES PERSONNES ENTENDUES ET DES CONTRIBUTIONS ÉCRITES....127**

**PROGRAMME DES DÉPLACEMENTS....131**

**TABLEAU DE MISE EN ŒUVRE ET DE SUIVI....133**

**ANNEXE 1 DROIT COMPARÉ - CONSERVATION ET ACCÈS AUX DONNÉES DE CONNEXION DANS L'UNION EUROPÉENNE....137**

A. L'ALLEMAGNE....137

B. LA BELGIQUE....140

C. LE DANEMARK....143

D. L'ESTONIE....146

*L'IRLANDE*....148

*L'ITALIE*....150

E. LA LETTONIE....152

F. LA LITUANIE....154

G. LES PAYS-BAS....156

H. LA POLOGNE....159

I. LA SLOVAQUIE....161

J. LA SUÈDE....163

**ANNEXE 2 ÉTUDE DE DROIT COMPARÉ - TABLEAU DE SYNTHÈSE DES RÉGIMES LÉGAUX D'ACCÈS ET DE CONSERVATION DES DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES .....167**

**LE CONTRÔLE EN CLAIR .....177**

# L'ESSENTIEL

**Présentes dans 85 % des enquêtes pénales**, les données de connexion (ou métadonnées) sont les traces techniques laissées par un terminal (appareil portable, objet connecté, ordinateur…) sur un réseau lors de sa connexion à celui-ci. Capables de révéler les déplacements d'une personne, ses interactions numériques ou téléphoniques avec des tiers ou encore la liste des sites internet qu'elle a visités, **elles jouent un rôle majeur, à charge comme à décharge, dans les investigations sur les affaires criminelles les plus lourdes** – des disparitions de la jeune Lina et du petit Émile à l'été 2023 à l'enquête ayant permis l'identification des membres du commando terroriste responsable des attentats du 13 novembre 2015. Mais **elles ont aussi une place centrale dans l'élucidation de faits plus « banals », qui relèvent de la « délinquance du quotidien »** : c'est ainsi par les données de connexion que les enquêteurs peuvent identifier d'éventuels receleurs après un vol de portable. Enfin, à l'heure où le développement du numérique va de pair avec une croissance exponentielle de la cyber-délinquance, **les données de connexion sont, pour toutes les infractions commises en ligne (cyber-harcèlement, arnaques sur internet, pédopornographie…), les seules preuves disponibles.**

Outil précieux pour les services de police et de gendarmerie et pour les magistrats qui dirigent les enquêtes, **les données de connexion ont toutefois vu leur vaste utilisation remise en cause par des arrêts de la Cour de justice de l'Union européenne** qui, depuis près de dix ans, sont venus progressivement prohiber la conservation généralisée de ces données à des fins pénales, limiter leur utilisation par les enquêteurs aux infractions relevant de la criminalité dite « grave » et imposer avant tout accès à ces données un contrôle préalable par une autorité indépendante ou par une juridiction – interdisant *de facto* que ce contrôle soit placé sous la seule autorité du parquet. Alors que le législateur est déjà intervenu par deux fois, avec la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement en ce qui concerne la conservation des métadonnées puis, en matière d'accès, avec la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire, **notre droit national n'apparaît toujours pas pleinement conforme à la jurisprudence de la Cour.**

Dans ce contexte, la commission des lois a créé en son sein, en février 2023, une mission d'information sur l'usage des données de connexion dans l'enquête pénale en chargeant Agnès Canayer, Philippe Bonnecarrère et, jusqu'en octobre 2023, Jean-Yves Leconte, des fonctions de rapporteurs.

À l'issue de ses travaux, après trois déplacements et 21 auditions ayant permis d'entendre 56 personnes, **elle formule 16 recommandations pour :**

**- assumer en Europe une position forte**, en faisant du sujet des données de connexion une priorité pour la France ;

**- faire évoluer notre droit national** pour mieux encadrer la procédure d'accès aux métadonnées tout en adoptant, en matière de conservation, une approche pragmatique ;

**- éviter que la nouvelle procédure de contrôle** des accès aux données de connexion, légitime dans son principe et incontournable pour garantir le respect du droit européen, **ne se traduise par un « choc procédural »** pour les acteurs de l'enquête.

## I. LES DONNÉES DE CONNEXION, PIERRE ANGULAIRE DE L'ENQUÊTE PÉNALE

### *A. LES MÉTADONNÉES, DES DONNÉES SENSIBLES AUX USAGES MULTIPLES*

**Les données de connexion sont de trois types** : les données d'identification (identité civile liée à un numéro de téléphone, à une adresse IP, à un numéro d'abonné, à un numéro de carte SIM…), qui sont les moins sensibles car elles ne relèvent rien de la vie privée des personnes concernées ; les données de trafic (liste des contacts téléphoniques, des SMS et courriels reçus et envoyés, ce qui couvre notamment les factures détaillées ou « fadettes ») ; les données de localisation, qui permettent de connaître plus ou moins précisément l'emplacement de l'utilisateur en identifiant l'antenne-relais à laquelle son appareil s'est connecté. Les métadonnées recouvrent donc l'intégralité des données techniques liées aux communications, à l'exception notable de celles relatives au contenu des échanges **: elles ne permettent de connaître ni le texte des messages (courriels, SMS…) envoyés ou reçus, ni la nature des propos tenus lors de conversations téléphoniques.**

Présentant de nombreux usages pour les enquêteurs (identification des protagonistes d'une infraction ; mise au jour de lignes occultes ; identification des personnes présentes sur le lieu de commission d'une infraction…), **les données de connexion sont aujourd'hui une preuve « reine » et constituent à la fois un point de départ pour les investigations**

**et une exigence des magistrats du siège comme gage de crédibilité de l'accusation.** En 2022, ce sont ainsi **près de 3 millions de données qui ont fait l'objet d'une réquisition** ; attestant du rôle central des données de connexion dans les enquêtes pénales, ce nombre est par ailleurs en hausse tendancielle de 10 % par an.

### *B. LA STRUCTURATION PROGRESSIVE D'UN USAGE DEVENU MASSIF*

Toutes les données de connexion sont conservées directement par les opérateurs de communications électroniques (OCE), notamment les opérateurs de téléphonie, les services d'enquête pouvant y accéder en tant que de besoin par le biais d'une réquisition. **Jusqu'à une période récente, l'accès à ces données était faiblement encadré par le code de procédure pénale et se faisait de manière désordonnée**. Toutefois, ces accès ont rapidement posé un lourd problème financier, chaque opérateur fixant librement le montant de la compensation financière qui devait lui être versée pour chaque accès, et de principe, puisqu'aucune traçabilité des demandes d'accès n'était assurée. Après des tentatives échouées de rationalisation technique et financière entre 2007 et 2017, une **plateforme nationale des interceptions judiciaires (PNIJ), à laquelle les principaux opérateurs sont directement reliés, a été déployée et rendue obligatoire** ; gérée par une agence dédiée, ANTENJ, elle concentre aujourd'hui la majorité des accès aux données de connexion et offre aux enquêteurs un outil ergonomique et rapide, dont l'usage est susceptible d'être contrôlé par les magistrats.

En dépit de son indéniable succès, **la PNIJ n'a pas permis de lever toutes les difficultés liées à l'accès aux données de connexion** : non seulement le « hors-PNIJ » continue d'être statistiquement important (entre 20 et 25 % des accès passent aujourd'hui par d'autres outils que la plateforme), mais surtout les enquêteurs peuvent exploiter les données recueillies *via* la PNIJ par le biais de logiciels de rapprochement judiciaire qui n'offrent pas les mêmes garanties que la plateforme.

## II. DES DROITS NATIONAUX BOULEVERSÉS LA JURISPRUDENCE DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

### *A. UNE JURISPRUDENCE DRASTIQUEMENT LIMITATIVE*

Dans ce contexte national déjà complexe, **la jurisprudence de la Cour de justice de l'Union est venue depuis 2014 limiter drastiquement la conservation des données de trafic et de localisation par les États et l'accès à ces données par les enquêteurs.** En substance, les règles posées par les juges de Luxembourg sont les suivantes :

**- la conservation générale et indifférenciée des données de trafic et de localisation ne peut être envisagée qu'en cas de menace grave, réelle ou prévisible, pour la sécurité nationale** de l'État concerné ; dans une telle hypothèse, l'accès aux données concernées n'est possible qu'aux fins de lutte contre la menace précitée ;

- l'accès, hors menace grave, aux données de trafic et de localisation **n'est possible que pour la « criminalité grave » et sous la forme d'un *quick freeze* (ou « injonction de conservation rapide ») ou d'une conservation ciblée** fondée, notamment, sur des critères géographiques ;

**- pour la délinquance ordinaire, aucun accès aux données de trafic et de localisation n'est possible,** sauf dans des cas - sur lesquels la jurisprudence de la Cour pourrait être en train d'évoluer à la suite d'une question préjudicielle liée aux compétences de l'ex-Hadopi française - liés aux infractions exclusivement commises en ligne et lorsque leur exploitation est le seul moyen d'identifier l'auteur.

**Ces positions ont été abondamment commentées, et souvent contestées**, pour deux motifs : d'une part, fondées sur la Charte des droits fondamentaux de l'Union européenne, elles donnent une portée inédite aux droits définis par la Charte, qui s'imposent sans conciliation avec d'autres impératifs de même niveau ; d'autre part, **elles constituent pour beaucoup une immixtion dans les prérogatives exclusives des États membres**, la sécurité publique et la matière pénale étant exclues du périmètre des compétences de l'Union.

### *B. EN EUROPE, DES ÉTATS DÉBOUSSOLÉS, UNE UNION DÉSTABILISÉE*

La jurisprudence de la Cour a eu deux conséquences majeures à travers l'Europe.

**Au niveau des États membres, les tentatives nombreuses de mise en conformité vis-à-vis du droit de l'Union ont été toujours fastidieuses et souvent infructueuses.** Alors que certains États ont vu « tomber » leur régime de conservation, d'autres ont tenté de mettre en place une conservation ciblée (le ciblage atteignant dans certains cas, comme en Belgique, la quasi-intégralité du territoire national). Ces initiatives ne semblent pas avoir donné satisfaction aux autorités nationales concernées, attestant du caractère peu opérationnel des exigences posées par la CJUE et, parmi les régimes de conservation ciblée instaurés par nos voisins européens, aucun ne semble suffisamment délimité pour surmonter la rigueur des arrêts de la Cour.

Au niveau de l'Union européenne, **la jurisprudence de la CJUE est venue ajouter des perturbations dans un processus décisionnel déjà difficile** au vu des divergences récurrentes d'appréciation entre le Conseil, la Commission et le Parlement européen en ce qui concerne le juste équilibre

entre la protection des données personnelles et la prévention et la répression des infractions pénales. Si certaines réglementations ont abouti après de longues et difficiles négociations, à l'instar du « paquet » *e-evidence* sur les preuves numériques, d'autres textes semblent durablement à l'arrêt. En particulier, **les discussions restent en suspens sur le futur règlement *e-privacy* 2**, qui doit impérativement être adopté pour rendre le cadre issu de la directive *e-privacy* de 2002 conforme au RGPD et, dans le même temps**, exclure l'application du texte « *aux activités menées par les autorités compétentes à des fins de prévention et de détection des infractions pénales* ».**

Par ailleurs, un groupe d'experts de haut niveau baptisé ADELE (*access to data for effective law enforcement*) a été créé sous la présidence suédoise de l'Union, témoignant de la volonté de nombreux États membres de réévaluer les contraintes générées par les arrêts de la CJUE et de proposer un nouveau cadre de réflexion.

## III. LES LIMITES DES TENTATIVES FRANÇAISES DE MISE EN CONFORMITÉ

Si le législateur est déjà intervenu par deux fois pour mettre le droit national en conformité avec les règles issues de la jurisprudence européenne, force est de constater qu'il n'y est que très partiellement parvenu.

### *A. UNE CONSERVATION QUI DEMEURE GÉNÉRALE ET INDIFFÉRENCIÉE*

Dans leur version en vigueur jusqu'en 2021, les articles L. 34-1 et R. 10-13 du code des postes et des communications électroniques mettaient en place un régime de conservation générale et indifférenciée des métadonnées, sans condition particulière. Contraire à la jurisprudence de la CJUE et à la Constitution[1], ce dispositif a été d'abord aménagé par **le Conseil d'État qui, par sa décision d'Assemblée *French data network* du 21 avril 2021, a adopté une position de constructivisme jurisprudentiel** en considérant que, si la conservation générale et indifférenciée des données de trafic et de localisation était justifiée par des menaces pour la sécurité nationale, elle était contraire au droit de l'Union européenne dans la mesure où :

[1] *Par une décision n° 2021-976/977 QPC du 25 février 2022, le Conseil constitutionnel a en effet jugé que l'article L. 34-1 précité, dans sa version antérieurement en vigueur faisant l'objet de la saisine, prévoyait une conservation qui s'appliquait « de façon générale à tous les utilisateurs des services de communications électroniques » et portait « indifféremment sur toutes les données de connexion relatives à ces personnes, quelle qu'en soit la sensibilité et sans considération de la nature et de la gravité des infractions susceptibles d'être recherchées », constituant une atteinte disproportionnée au droit au respect de la vie privée.*

- elle n'était pas explicitement justifiée par l'existence de ces menaces et que son maintien en vigueur n'était pas conditionné à l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale. Le Conseil d'État a constaté l'existence d'une telle menace, mais exigé un réexamen périodique de celle-ci pour justifier ou non le maintien d'une conservation généralisée ;

- ses finalités n'étaient pas limitées à la sauvegarde de la sécurité nationale, à rebours des exigences posées par la CJUE pour les données de trafic et de localisation. Pour autant, s'agissant de la conservation des métadonnées à des fins de lutte contre la criminalité grave, **le Conseil d'État a considéré que la conservation ciblée proposée par la Cour de Luxembourg « *se [heurtait] à des obstacles techniques qui en compromettent manifestement la mise en œuvre* »**. Il a ainsi estimé que **les données de trafic et de localisation conservées par les opérateurs pouvaient être rendues accessibles, dans un cadre pénal, par le biais d'une injonction** de procéder, pour une durée déterminée, à une « conservation rapide » de ces données dès lors que l'infraction concernée était « *suffisamment grave pour justifier [une] ingérence dans la vie privée* » : en d'autres termes, **le Conseil d'État a reconnu la possibilité d'un accès aux données conservées aux fins de la sauvegarde de la sécurité nationale pour d'autres fins.**

C'est en s'inspirant du modèle esquissé par le Conseil d'État que le législateur a modifié, dans le cadre de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, l'article L. 34-1 du code des postes et des télécommunications électroniques pour rénover l'obligation faite aux opérateurs de conserver les données de connexion en distinguant selon les catégories de données et les finalités de la conservation**. La durée de conservation est ainsi fixée à un an pour la quasi-intégralité des métadonnées** (à l'exception des données relatives à l'identité civile de l'utilisateur, conservées pendant cinq ans après l'expiration de son contrat) et la loi reconnaît la possibilité d'une telle conservation non seulement à des fins de sauvegarde de la sécurité nationale, mais aussi de la lutte contre la délinquance grave, traduction française de la « criminalité grave » mise en avant par la CJUE. L'article L. 34-1 ainsi réécrit précise par ailleurs que les données conservées par les opérateurs peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect.

**S'il a permis de préserver l'essentiel du système de conservation français, et donc de protéger les capacités opérationnelles des services d'enquête, la conformité de ce dispositif au droit européen reste douteuse**. Alors que le Président de la CJUE avait estimé, lors d'une audition de la commission des affaires européenne de l'Assemblée nationale le 18 mai 2021,

que ce système était compatible avec les arrêts de la CJUE, la Cour elle-même semble avoir adopté une position différente dans des arrêts rendus en 2022 par lesquels elle a interdit aux autorités nationales d'accéder à une donnée pour une finalité présentant un intérêt « inférieur » à celui de la finalité pour laquelle la donnée a été conservée initialement.

### *B. UN ACCÈS MIEUX DÉLIMITÉ MAIS TOUJOURS PAS SOUMIS À UN CONTRÔLE PRÉALABLE*

Parce qu'elle permet un accès aux données de connexion par le biais d'une simple réquisition judiciaire, sans considération de la nature de l'infraction et donc potentiellement hors du cadre de la délinquance et de la criminalité grave, la loi française présentait jusqu'en 2022 un second motif de non-conformité à la jurisprudence de la CJUE ; elle avait, au demeurant, été jugée contraire à la Constitution sur ce point par le Conseil constitutionnel à la fin de l'année 2021.

En conséquence, le législateur est intervenu avec la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire pour restreindre l'accès aux données de connexion aux enquêtes pénales sur les cas les plus graves. Le nouvel article 60-1-2 du code de procédure pénale introduit à cette occasion précise que **l'accès aux données de trafic et de localisation n'est possible que « *si les nécessités de la procédure l'exigent* » et dans quatre cas limitativement énumérés :**

- lorsque la procédure porte sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement ;

- lorsque la procédure porte sur un crime ou un délit puni d'au moins un an d'emprisonnement, que celui-ci a été commis par l'utilisation d'un réseau de communication électronique et que les réquisitions ont pour seul objet d'identifier l'auteur de l'infraction ;

- lorsque les réquisitions portent sur les équipements de la victime et interviennent à la demande de celle-ci, pour des délits punis d'une peine d'emprisonnement ;

- lorsqu'elles tendent à retrouver une personne disparue ou à retracer un parcours criminel.

Comme l'a depuis lors rappelé la Cour de cassation, **le quantum encouru ne suffit pas à caractériser l'inscription de l'infraction dans la « criminalité grave » au sens de la jurisprudence de la CJUE, et il convient également de tenir compte des circonstances de l'espèce.** Il en découle une exigence de motivation renforcée pour les services d'enquête qui, elle-même, génère un surcroît de formalisme et crée le risque d'une hétérogénéité des appréciations à l'échelle nationale.

En tout état de cause, cette évolution ne réglait pas la question du rôle du parquet : bien que ne pouvant être considéré comme indépendant vis-à-vis de l'enquête, celui-ci reste en effet chargé de contrôler l'accès aux données de connexion en flagrance et en enquête préliminaire, ce qui ne paraît pas répondre aux exigences de la CJUE tenant à la mise en œuvre d'un contrôle à la fois préalable et indépendant de tels accès. C'est ainsi que, **par des arrêts du 12 juillet 2022, la chambre criminelle de la Cour de cassation a jugé que le procureur de la République, qui dirige l'enquête, ne pouvait valablement contrôler l'accès aux données de connexion.** Cette décision aurait pu avoir des conséquences dévastatrices pour la conduite des enquêtes, dans la mesure où la flagrance et l'enquête préliminaire placées sous la direction du parquet représentent actuellement l'immense majorité des investigations. Toutefois, la chambre criminelle a atténué les effets de ses arrêts en jugeant que **l'absence d'un contrôle indépendant n'entraînerait la nullité de la procédure concernée que si le requérant pouvait établir l'existence d'un préjudice**, c'est-à-dire démontrer qu'un contrôle indépendant aurait conclu à l'impossibilité d'accéder aux données de connexion concernées.

Cette position, protectrice du rôle du parquet, reste cependant fragile.

## IV. AGIR EN FRANCE ET EN EUROPE POUR SÉCURISER LE RECOURS AUX MÉTADONNÉES DANS L'ENQUÊTE PÉNALE

**Les constats qui précèdent incitent à une intervention non seulement du législateur**, auquel il appartient de sécuriser l'usage des données de connexion dans l'enquête pénale, **mais aussi du Gouvernement**, chargé à la fois d'être le porte-parole des institutions françaises dans les négociations européennes et de gérer les moyens donnés à la justice, à la police et à la gendarmerie pour un exercice serein de leurs missions.

### *A. EN EUROPE, ASSUMER UNE POSITION FORTE*

Les rapporteurs appellent tout d'abord le gouvernement à assumer une position forte dans les négociations européennes pour faire du sujet des données de connexion une véritable priorité. **Ils l'invitent ainsi à œuvrer pour l'aboutissement rapide et concluant de l'examen du règlement *e-privacy* 2.** Ils estiment, par ailleurs, indispensable que le Parlement soit mieux associé aux travaux du groupe d'experts de haut niveau ADELE et que le Gouvernement rende compte régulièrement à l'Assemblée nationale et au Sénat de l'avancée de ses réflexions et des lignes de force qui s'y dessinent.

**Les rapporteurs jugent également que la loi française doit tirer un meilleur parti des « soupapes » offertes par la jurisprudence européenne.** Cette orientation incite non seulement à aménager la loi française pour faciliter l'accès aux données d'identification, pour lesquelles le juge européen offre des possibilités plus larges d'accès, et de tenir compte des arrêts futurs de la CJUE qui pourraient conduire à un assouplissement sur l'usage des adresses IP, et plus généralement sur les conditions d'accès aux métadonnées pour les infractions commises en ligne.

### *B. DANS LA LOI FRANÇAISE, TROUVER LE POINT D'ÉQUILIBRE ENTRE EXIGENCE ET PRAGMATISME*

Face au sentiment d'insécurité juridique des acteurs de l'enquête pénale, et notamment des magistrats du parquet, il convient ensuite lieu que le législateur intervienne pour clarifier le régime applicable aux données de connexion.

S'agissant du contrôle préalable et indépendant de l'accès aux métadonnées exigé par la Cour de justice, la loi devra rappeler que celui-ci n'est exigé que pour les données de trafic et de localisation : **un accès autorisé par le parquet pour les données d'identification, qui constituent une moindre atteinte à la vie privée, pourra donc être maintenu.** Ce point est loin d'être anecdotique puisque, pour 2021 et 2022, les données d'identification ont représenté environ un million d'accès.

En ce qui concerne les données de trafic et de localisation, la mission d'information a étudié toutes les pistes possibles pour la mise en place d'un contrôle conforme aux exigences de la CJUE. Elle a **écarté la piste d'un contrôle par une autorité indépendante**, qui lui a semblé soit présenter un risque trop fort de contrariété avec la jurisprudence européenne (notamment en cas de contrôle par une autorité administrative indépendante ou par une autorité rattachée au parquet), soit soulever des difficultés techniques, informatiques et de ressources humaines insurmontables (en particulier en cas de contrôle par ANTENJ ou par une autorité nationale indépendante composée de magistrats). Par conséquent, elle a privilégié la piste d'un contrôle assuré par une juridiction et a relevé que **l'hypothèse la plus pertinente, crédible et réaliste était celle d'un contrôle préalable exercé par le juge des libertés et de la détention (JLD),** qui dispose déjà de prérogatives en matière de protection la liberté individuelle. En matière de données de trafic et de localisation, le JLD serait ainsi appelé à contrôler les demandes formulées par les enquêteurs, puis validées par le parquet selon un système de « visa ».

En pratique, **le contrôle pourrait être exercé par les juges locaux de la liberté et de la détention ou par un groupement dédié de JLD placé auprès de la Cour d'appel** – cette seconde formule permettant à la fois d'exercer un roulement parmi les juges du territoire (ce qui présente des

avantages au vu du caractère massif et sans doute rébarbatif du contrôle) et d'assurer que l'interlocuteur en charge du contrôle connaisse les enjeux locaux.

En tout état de cause, cette extension des compétences du JLD, qui s'inscrirait dans le mouvement de « recentrage » impulsé par la récente loi d'orientation et de programmation du ministère de la justice 2023-2027, **supposera des créations de postes proportionnées à l'ampleur du travail à réaliser** (qui ne pourra être mesuré qu'une fois connus le périmètre et les modalités concrètes du contrôle mais pourrait s'avérer plus limité que prévu si, comme le préconisent les rapporteurs, un travail est engagé dans le même temps sur la forme et le périmètre du nouveau contrôle) **et une reconsidération du statut et des missions de ce magistrat.** Elle imposera, aussi et surtout, de se donner du temps pour construire les outils nécessaires au bon traitement de ce contrôle.

Dans tous les cas, pour ne pas dégrader les capacités d'enquête des services de police et de gendarmerie, **cette nouvelle formalité devra aller de pair avec la création d'une procédure d'urgence permettant aux enquêteurs à titre exceptionnel d'accéder sans contrôle préalable aux données de trafic et de localisation** ; dans ce cas, le contrôle aurait lieu *a posteriori* et à bref délai.

De façon plus générale, cette réflexion doit être une opportunité de remettre à plat le cadre juridique de la preuve numérique, aujourd'hui fragmenté et peu cohérent, pour **faire dépendre l'intensité du contrôle exercé par l'autorité judiciaire sur les actes d'enquête du degré d'intrusion dans la vie privée.**

### *C. PRÉSERVER LE QUOTIDIEN DES ENQUÊTEURS ET ÉVITER LE « CHOC PROCÉDURAL »*

Les rapporteurs ont également eu pour préoccupation de limiter, autant que faire se peut, l'impact sur les services d'enquête de la nouvelle procédure de contrôle des accès aux métadonnées. En d'autres termes, **outre la question du « qui contrôle ? », il leur a semblé devoir mettre au cœur de leurs travaux la question du « comment contrôler ? ».**

Ainsi, il leur a semblé essentiel que le rôle « pivot » de la PNIJ soit préservé selon deux axes : d'une part, une formation renforcée des enquêteurs pour les aider à mieux tirer profit des modules offerts par la plateforme et pour les aider à sélectionner des outils qui limitent les demandes d'accès à ce qui est strictement nécessaire à l'enquête ; d'autre part, l'encadrement renforcé du « para-PNIJ » que constitue l'usage de logiciels de rapprochement judiciaire, avec la mise en place de nouvelles vérifications en amont de leur déploiement.

Surtout, les rapporteurs estiment indispensable que, dès les premières étapes de la conception du futur contrôle des accès aux données de connexion, **une réflexion soit engagée sur ses modalités concrètes et notamment sur les outils informatiques sur lesquels il s'appuiera**. Il leur semble à cet égard nécessaire :

- de calibrer la procédure de demande d'accès aux données de trafic et de localisation pour limiter la surcharge de travail des enquêteurs, avec une **harmonisation du périmètre des autorisations d'accès** – périmètre aujourd'hui très variable, puisque certains parquets donnent des autorisations par dossier et pour six mois alors que d'autres souhaitent être saisis pour chaque nouvelle ligne identifiée ;

- de **travailler sur la forme de la demande d'accès aux données de connexion, afin que celle-ci passe par un applicatif simple, ergonomique et souple** ;

- de **relier cet applicatif à la PNIJ** pour que l'autorisation, une fois émise, emporte l'ouverture de la possibilité d'émettre une réquisition.

Enfin, les rapporteurs ont constaté que des projets informatiques majeurs ayant vocation à toucher les services d'enquête étaient en cours, à l'instar du programme « procédure pénale numérique » (PPN). Ils ont appelé à une prise en compte, par ces chantiers, des enjeux liés à la mise en place de la nouvelle procédure de contrôle des accès aux métadonnées et à la **préservation du caractère modulable des outils ainsi créés afin qu'ils puissent évoluer avec la procédure pénale comme avec les besoins des acteurs de l'enquête.**

# LISTE DES PROPOSITIONS

**Proposition n° 1 :** Lever toute ambiguïté quant à la nature des données devant être conservées par les opérateurs.

**Proposition n° 2** : Intégrer dans le code de procédure pénale le faisceau d'indices retenu par la Cour de cassation pour définir la notion de « criminalité grave ».

**Proposition n° 3** : Maintenir au niveau de chaque État membre la définition de ce que recouvre la « criminalité grave », sans en faire une notion autonome du droit de l'Union européenne.

## AGIR EN EUROPE DANS LE SENS D'UN PLUS GRAND PRAGMATISME

**Proposition n° 4** : Obtenir du Gouvernement qu'il rende compte au Parlement des échanges menés dans le cadre du groupe d'experts de haut niveau *Going dark*.

**Proposition n° 5** : Tirer profit des éventuelles évolutions de la position de la CJUE pour, d'une part, renforcer les souplesses d'accès aux données de connexion en matière de lutte contre les infractions commises en ligne et, d'autre part, envisager un assouplissement du régime d'accès aux adresses IP.

## ADAPTER LES NORMES FRANÇAISES À L'IMPÉRATIF D'UN CONTRÔLE PRÉALABLE DES ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES

**Proposition n° 6** : Permettre au parquet d'exercer le contrôle des demandes d'accès aux données de connexion aux seules fins d'identification.

**Proposition n° 7** : Attribuer la mission de contrôle des accès aux données de connexion au juge des libertés et de la détention.

**Proposition n° 8** : Prévoir, en cas d'urgence, la possibilité d'un accès aux données de connexion avec une autorisation *a posteriori*.

**Proposition n° 9** : En cas de choix du juge des libertés et de la détention pour contrôler l'accès aux données de connexion, engager une réflexion sur le statut et les missions de ce magistrat.

**Proposition n° 10** : Engager une réflexion sur la proportionnalité des actes d'enquête en fonction de leur degré d'intrusion dans la vie privée.

## GARANTIR LA FLUIDITÉ DE LA CHAÎNE PÉNALE POUR PROTÉGER LES ACTEURS DE L'ENQUÊTE DU « CHOC PROCÉDURAL »

**Proposition n° 11** : Renforcer la formation des services enquêteurs au maniement de la PNIJ.

**Proposition n° 12** : Soumettre à un contrôle renforcé l'emploi par les services enquêteurs d'outils de retraitement des données de connexion.

**Proposition n° 13** : Sécuriser l'action des services d'enquête en précisant par circulaire le périmètre des autorisations d'accès aux données de connexion.

**Proposition n° 14** : Engager un travail sur la forme de la motivation de la demande d'accès aux métadonnées visant à limiter la charge de travail supplémentaire induite par la nouvelle procédure.

**Proposition n° 15** : S'imposer, avant l'entrée en vigueur du nouveau contrôle des autorisations d'accès aux données de connexion, de mener à bien le projet procédure pénale numérique (PPN).

**Proposition n° 16** : Assurer la modularité des outils créés par les chantiers informatiques sur la procédure pénale numérique (PPN).

**INTRODUCTION**

Rares sont aujourd'hui les citoyens qui n'ont pas auprès d'eux, presque en permanence, un téléphone portable ou qui ne vont pas quotidiennement sur internet pour s'informer, se divertir, se cultiver, acheter en ligne ou communiquer avec leurs proches. **Le constat de l'omniprésence du numérique dans tous les aspects de nos vies est aussi banal que majeur**, et le recours à ce qu'on appelait au siècle dernier « les télécommunications » est devenu inévitable pour quiconque entend mener une existence normale.

Applicable au commun des mortels, **cette observation n'est pas moins vraie pour les délinquants de tous ordres qui, eux aussi, dépendent de plus en plus du numérique pour préparer et commettre des infractions.** Les réseaux les mieux organisés vont jusqu'à développer leurs propres outils, à l'image d'EncroChat, un réseau crypté transnational qui promettait à ses 60 000 utilisateurs une confidentialité absolue et dont le démantèlement sous l'égide de la gendarmerie nationale a permis le décryptage de 115 millions de conversations criminelles et l'arrestation, à travers toute Europe, de 6 500 personnes.

Il n'est pas étonnant dans ce contexte que les données numériques – et, parmi elles, les plus faciles d'accès que sont **les données de connexion – soient désormais un instrument de preuve essentiel pour les services d'enquête.** Leur usage a cependant été remis en question par des arrêts rendus depuis dix ans par la Cour de justice de l'Union européenne qui, venant limiter la conservation des données de connexion et l'accès à celles-ci au motif d'une nécessaire protection de la vie privée, ont justifié une inquiétude croissante non seulement de la part des acteurs de l'enquête pénale en France – policiers, gendarmes et magistrats du parquet –, mais aussi des forces de l'ordre dans toute l'Union. Les responsables des services de police de vingt-six États membres ont ainsi, dans une déclaration commune faite à Lisbonne le 30 mars 2023, fait le constat d'un « *déséquilibre croissant entre les outils et moyens dévoyés par des organisations criminelles et [la] capacité [des services de police] d'offrir une réponse opérationnelle et efficace* » et appelé à une évolution de la jurisprudence[1].

Ce souhait est partagé par les acteurs français de l'enquête qui, s'estimant déjà fragilisés par une complexification continue de la procédure pénale, craignent de voir se renforcer la crise des vocations qui affecte leurs métiers et, surtout, de se trouver démunis face à des délinquants de plus en plus « connectés » et insaisissables.

Les arrêts de la Cour de Luxembourg ont, par ailleurs, incité la quasi-intégralité des législateurs européens à modifier leur procédure pénale. En France, ils ont d'ores et déjà suscité deux modifications législatives en 2021 et 2022, qui n'ont pas suffi à garantir la complète conformité du droit interne au droit de l'Union.

---

[1] *Le texte de cette déclaration (en anglais) est consultable sur le site https://justica.gov.pt.*

Cette situation a incité la commission des lois du Sénat à constituer en son sein, en février 2023, dans le cadre du programme de contrôle de la Haute assemblée, une mission d'information sur l'usage des données de connexion dans l'enquête pénale, en chargeant Agnès Canayer, Philippe Bonnecarrère et, jusqu'en octobre 2023, Jean-Yves Leconte, des fonctions de rapporteurs.

**Le sujet de l'usage des données de connexion dans l'enquête pénale, aride en première approche, n'en est pas moins au cœur des préoccupations des pouvoirs publics.** Outre la mission d'information du Sénat, il fait en effet l'objet d'une mission de réflexion lancée par le Garde des Sceaux et confiée au conseiller d'État Alexandre Lallet et d'un « groupe d'experts de haut niveau » européen installé en juin 2023 et placé sous l'autorité conjointe de la Commission et du Conseil. Ces initiatives, comme celle du Sénat, visent à identifier des solutions qui, conformes au cadre juridique établi par les juges de Luxembourg et par les cours suprêmes nationales, fassent dans le même temps preuve de pragmatisme et intègrent les besoins et les contraintes du « terrain ».

Si l'objet de la présente mission suscite une telle attention, c'est parce que **la numérisation grandissante de nos vies quotidiennes donne aux données de connexion une importance majeure dans l'ensemble de nos pratiques sociales et privées** – et parce que cette importance est appelée à croître à l'heure de l'« internet des objets ». Au-delà des moments où nous utilisons un appareil, sa simple présence dans notre poche ou au fond de notre sac laisse des marques tangibles sur le réseau auquel il se connecte à chaque instant ; cette observation vaut pour nos téléphones portables comme pour les accessoires « connectés » (montres connectées, mais aussi appareils portables de santé) de plus en plus populaires et qui enregistrent en continu l'activité, les déplacements, voire les constantes vitales de leurs utilisateurs.

Formidable opportunité d'apporter aux enquêteurs de nouveaux moyens de preuve pour mieux garantir la sécurité publique, **l'importance croissante des données de connexion fait dans le même temps monter le spectre d'une surveillance de masse** qui mobilise, en France comme dans le reste de l'Europe, des associations et des citoyens. De manière paradoxale, cette crainte se concentre davantage sur les États, pourtant garants de l'intérêt général, que sur les géants du numérique dont la puissance concurrence celle des autorités publiques et qui font des données qu'ils collectent un usage extrêmement intrusif qui, loin de se cantonner à la sphère mercantile, peut avoir un impact non seulement sur les choix de consommation des individus mais aussi sur les délibérations politiques d'un pays.

Aussi ancienne que le droit pénal moderne lui-même, cette crainte doit cependant être mise en balance avec les nombreux leviers dont notre droit s'est progressivement doté pour protéger la vie privée des individus.

Alors que l'introduction du code napoléonien d'instruction criminelle de 1811 affirmait « *qu'aucune partie de l'empire n'est privée de surveillance ; qu'aucun crime, aucun délit, aucune contravention ne doit rester sans poursuite, et que l'œil du génie qui sait tout animer embrasse l'ensemble de cette vaste machine sans néanmoins que le moindre détail puisse lui échapper* »[1], l'article préliminaire de notre code de procédure pénale rappelle, avec certes moins d'emphase mais davantage d'équilibre, qu'« *au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction* ». Cette nécessaire proportionnalité, consacrée en tête du code, impose de **maintenir un juste équilibre entre les libertés individuelles et le droit à la sécurité – ou, pour l'exprimer autrement, entre la protection de l'individu et celle de la société** : c'est dans cet état d'esprit et avec la préoccupation constante de préserver cet équilibre qu'ont été établis le présent rapport et les propositions qu'il contient.

[1] *Introduction citée par Michel Foucault, « La société punitive. Cours au collège de France, 1972-1973 », EHESS Gallimard Seuil, 2013, p. 25.*

# PREMIÈRE PARTIE
# LES DONNÉES DE CONNEXION, NOUVELLE PIERRE ANGULAIRE DE L'ENQUÊTE PÉNALE

## I. LES DONNÉES DE CONNEXION : DES INFORMATIONS SENSIBLES AUX USAGES MULTIPLES

**Données personnelles sensibles, les données de connexion constituent en cas d'infraction autant de « gisements de preuves »** qui ont le pouvoir de confirmer ou d'infirmer un alibi, de mettre au jour un mobile ou de rendre visible une complicité qu'un examen de preuves matérielles n'aurait pas rendue apparente. Elles jouent aujourd'hui un rôle majeur dans l'élucidation des crimes et des délits : **on estime qu'elles apparaissent dans 85 % des dossiers, tous types d'infractions confondus, et dans l'intégralité des procédures liées à la criminalité organisée.**

### *A. LES DONNÉES DE CONNEXION : UNE NOTION TECHNIQUE SAISIE PAR LE DROIT PÉNAL*

#### 1. Une définition technique des données de connexion

Aussi appelées « métadonnées », les données de connexion sont, comme leur nom l'indique, les **données techniques produites par un appareil** (téléphone, tablette, ordinateur…) **lors de sa connexion au réseau de communications électroniques**. Elles sont traitées puis conservées par les opérateurs de communications électroniques, ou « OCE » (opérateurs de téléphonie fixe et mobile, fournisseurs d'accès à internet[1], *etc.*).

Schématiquement, on distingue **trois types de données de connexion :**

**- celles qui permettent d'identifier l'utilisateur, les « données d'identification »** : il s'agit de l'identité civile liée à des données techniques, c'est-à-dire à un numéro de téléphone, à une adresse mail, à une adresse IP, à un numéro d'abonné, ou encore à un numéro de carte SIM (IMSI) ou à un identifiant de téléphone (IMEI) ;

**- celles qui portent sur l'acheminement des communications, ou « données de trafic »**, qui concernent l'activité numérique et téléphonique de

[1] *À l'inverse, les hébergeurs de sites internet ne relèvent pas de cette catégorie.*

l'appareil : adresse IP[1], liste circonstanciée des contacts téléphoniques entrants et sortants (ce qui recouvre notamment les **factures détaillées, communément appelées « fadettes »**), des SMS et courriels reçus et envoyés, des sites internet consultés, *etc.* ;

- **celles qui portent sur la localisation de l'appareil**, *via* l'identification de l'antenne-relai par laquelle ont transité les flux issus dudit appareil. Loin de constituer une géolocalisation retraçant le parcours exact de l'utilisateur ou donnant un point exact de présence, ces données permettent toutefois une **localisation par zone** relativement précise (*a fortiori* dans les zones urbaines où de nombreuses antennes-relais sont installées).

Les métadonnées recouvrent donc l'intégralité des données techniques liées aux communications, **à l'exception notable de celles relatives au contenu des échanges : elles ne permettent de connaître ni le texte des messages (courriels, SMS…) envoyés ou reçus, ni la nature des propos tenus lors de conversations téléphoniques.**

Techniquement, il est possible d'accéder aux données de connexion non seulement **en temps réel,** mais aussi **en temps différé et de manière rétrospective** (sous réserve, évidemment, qu'elles aient été conservées par l'opérateur concerné). **L'accès en temps réel est plus intrusif que l'accès en temps différé, dans la mesure où il porte sur un périmètre plus vaste de données** : outre les données de connexion telles qu'elles ont été décrites ci-avant, **l'accès en temps réel couvre en effet les données traitées par les OCE pour des raisons techniques**, ce qui intègre *de facto* les données de localisation GPS, les données d'acheminement (qui font apparaître, le cas échéant, le recours à des techniques d'anonymisation ou à des réseaux privés virtuels (VPN)), les certificats électroniques ou encore les logins et mots de passe renseignés par l'utilisateur.

**Les rapporteurs ont concentré leurs travaux sur l'accès en temps différé**, puisqu'il s'agit du type d'accès dont la mise en œuvre est la plus mise en cause par la jurisprudence de la Cour de justice de l'Union européenne (CJUE).

De la même manière, si le présent rapport porte sur l'usage des données de connexion dans l'enquête pénale, il convient de relever que **les services enquêteurs ne sont pas les seuls à s'être vus ouvrir par la loi un droit d'accès aux données de connexion.** Alors que la loi pour la sécurité quotidienne de 2001[2] – qui a, la première, posé une base légale de conservation des métadonnées et d'accès à celles-ci – liait la conservation des métadonnées par les opérateurs aux « *besoins de la recherche, de la constatation*

---

[1] *Pour mémoire, l'adresse IP est un numéro unique attribué à un appareil par le serveur qui assure sa connexion à un réseau ; ce numéro peut être permanent ou « dynamique » et permet de retracer le « parcours » de l'appareil sur les différents noms de domaine (ce qui permet, en d'autres termes, de connaître les sites internet auxquels l'utilisateur a accédé, sans toutefois constituer un accès au contenu desdits sites).*

[2] *Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ; les dispositions en cause étaient alors codifiées à l'article L. 32-3-1 du code des postes et des communications électroniques.*

*et de la poursuite des infractions pénales* », sans distinction particulière mais avec un objectif clair de « *mise à disposition de l'autorité judiciaire d'informations* », **des textes sectoriels ont été adoptés au fil du temps pour autoriser des acteurs extra-judiciaires à accéder aux métadonnées selon des régimes spécifiques**.

Le législateur a ainsi ouvert un accès à l'ensemble des données de connexion conservées par les opérateurs aux services fiscaux et aux services des douanes dans l'exercice de leurs fonctions « judiciaires », c'est-à-dire dans le cadre de leurs prérogatives de recherche et de sanction de certaines infractions pénales, sous l'égide d'un contrôleur indépendant[1]. Il a parallèlement aménagé un accès partiel, généralement limité aux données d'identification et à certaines données de trafic, à l'inspection du travail[2] ainsi qu'à des autorités administratives indépendantes dotées d'un pouvoir répressif (Autorité de la concurrence, Autorité des marchés financiers, Hadopi – aujourd'hui intégrée à l'Arcom -, Agence nationale de la sécurité des systèmes d'information). **Il a enfin doté les services de renseignement d'un régime d'accès propre, pour les besoins de la prévention du terrorisme et pour la défense et la promotion des intérêts fondamentaux de la Nation**, avec notamment une possibilité d'accès rétrospectif aux données de connexion analogue à celle qui existe en matière pénale et aménagée par l'article L. 851-1 du code de la sécurité intérieure.

**L'accès administratif aux données de connexion des services de renseignement**

Les services de renseignement peuvent, selon les cas, recourir à quatre techniques de renseignement mobilisant les données de connexion conservées ou traitées par les opérateurs. Ils disposent ainsi :

- d'un **accès en temps différé aux données de connexion conservées par ces opérateurs** : organisé par l'article L. 851-1 du code de la sécurité intérieure, il s'apparente, sur le plan technique (mais non sur le plan juridique), à l'accès prévu pour les services d'enquête pénale ;

- d'un **accès en temps réel aux données de connexion conservées ou traitées par les opérateurs** (article L. 851-2 du même code) : cette technique, dont l'usage est limité à la prévention du terrorisme, couvre un périmètre de données plus large que les seules données conservées (voir ci-avant) ;

- de la possibilité de recourir à **un traitement algorithmique des données de connexion** qui vise, afin de prévenir le terrorisme et au-delà du suivi de « cibles » déjà repérées et identifiées, à détecter les comportements de communication en ligne susceptibles de constituer des signaux de « faible intensité » (article L. 851-3 du même code). Mis en place pour une durée de deux mois renouvelables, ce traitement n'emporte la levée de l'anonymat que s'il permet de détecter des éléments caractérisant l'existence d'une menace terroriste ;

[1] *Ces possibilités d'accès sont aujourd'hui prévues, respectivement, par les articles 96 G du livre des procédures fiscales et 65* quinquiès *du code des douanes.*

[2] *Article L. 8113-5-2 du code du travail.*

- d'une **géolocalisation en temps réel** (article L. 851-4), qui peut prendre la forme soit du suivi dynamique d'un terminal de communication, soit de l'utilisation d'une balise GSM ou GPS placée sur un objet ou un véhicule à l'insu de son utilisateur.

La mise en œuvre de ces techniques est **soumise à l'avis de la CNCTR** (Commission nationale de contrôle des techniques de renseignement) et à une autorisation du Premier ministre ; pour mémoire, si son avis défavorable n'est pas suivi, la Commission peut saisir la formation spécialisée du Conseil d'État afin d'obtenir l'interruption du recours à la technique en cause et la destruction des données ainsi collectées.

Le code de la sécurité intérieure (article L. 851-6) permet également aux services de renseignement d'utiliser un **dispositif mobile destiné à « capter » les données de connexion (appelé « IMSI *catcher* ») lorsque celles-ci sont difficiles, voire impossibles à obtenir par d'autres moyens** (notamment lorsqu'une personne utilise une ligne occulte, c'est-à-dire un téléphone acquis sous une fausse identité ou emprunté à un tiers). Le recours à cette technique est limité par la loi à la captation des données d'identification d'un terminal (numéros IMSI et IMEI) ou du numéro d'abonnement de son utilisateur, d'une part, et aux données relatives à la localisation des équipements concernés, d'autre part.

*Source : commission des lois du Sénat*

### 2. Une définition juridique difficile

S'il est relativement aisé de tracer les contours techniques des données de connexion, il est plus complexe d'en donner une définition juridique stricte. Non seulement les métadonnées, qui relèvent tout autant du droit économique que du droit pénal ou du droit public, « *mettent à l'épreuve les divisions classiques entre les différentes branches du droit* »[1], mais surtout elles peinent à s'insérer dans des cadres intellectuels qui, conçus au XIXe siècle, ne s'acclimatent que difficilement à la numérisation de nos vies quotidiennes.

En matière de procédure pénale, **les données de connexion sont ainsi le reflet d'une désorganisation générale du droit de la preuve numérique**.

En théorie, le droit de la preuve repose, comme l'ont rappelé les juristes entendus par les rapporteurs au cours d'une table ronde, sur une **catégorisation des moyens de preuve en fonction du degré d'atteinte à la vie privée induit par leur utilisation** (le principe sous-jacent étant que, plus l'infraction commise est grave, plus on peut admettre des atteintes à la vie privée pour en connaître l'auteur). Ce degré lui-même s'appuie sur une

[1] *François-Xavier Millet, Professeur à l'université des Antilles, Laboratoire caribéen en sciences sociales - Centre d'analyse géopolitique et internationale ; RFDA 2023, p .603, introduction au colloque « Les données de connexion - Quel équilibre entre droits fondamentaux et lutte contre la criminalité à l'ère du numérique ? » organisé le 16 janvier 2023 à l'Université des Antilles.*

***summa divisio*** **qui sépare, d'un côté, le contenu des échanges**, réputé sensible par définition en écho au principe constitutionnel de secret des correspondances, qui jouit d'une protection équivalente à celle dont bénéficient l'inviolabilité du domicile privé et le droit à la vie privée[1] **et, de l'autre, le contenant des communications, vu comme une information principalement technique** et donc peu intrusive.

Cette théorie, bien que pertinente dans son principe, se heurte à une double limite.

En premier lieu, la distinction entre le contenu et le contenant ne paraît pas avoir un impact systématique sur les régimes de preuves prévus par le code de procédure pénale : l'intégration de la preuve numérique à notre procédure pénale s'est effectuée dans un mouvement de pragmatisme désordonné. Elle résulte non pas d'une construction intellectuelle homogène, mais d'une **sédimentation progressive de normes adoptées en réaction à l'évolution des technologies sans vue d'ensemble** et dans laquelle « *les régimes juridiques que la loi ou la jurisprudence ont progressivement attribués aux modes de preuve numérique […] [sont] pensés* les uns après les autres *au lieu d'être pensés* les uns par rapport aux autres »[2].

Une lecture attentive du code de procédure pénale suffit à s'en convaincre : la mise en cohérence des régimes auxquels sont soumises les preuves numériques est inaboutie. En pratique, on observe ainsi une forte disparité de leurs caractéristiques, qu'il s'agisse des modalités de recours aux différentes techniques probatoires, de l'intensité du contrôle judiciaire ou du nombre des formalités à accomplir. Plus encore, il apparaît que **les modalités d'encadrement des différentes techniques probatoires n'ont qu'un lien imparfait avec nature de la donnée recueillie** (contenu ou contenant). C'est ainsi que, par exemple, **le recours aux données de connexion (qui sont théoriquement des « contenants ») est moins contraint que l'exploitation intégrale du téléphone des personnes gardées à vue** ou des ordinateurs découverts sur le lieu d'une perquisition, possible pour tout type d'infraction et sous le seul contrôle du parquet. Dans le même ordre d'idées, et bien que leur régime d'emploi présente des différences notables[3], on relèvera que depuis l'intervention du législateur en 2022 pour réguler l'accès aux données de connexion, **la géolocalisation en temps réel prévue par l'article 230-32 du code de procédure pénale a le même champ matériel d'application que l'accès rétrospectif aux métadonnées**, ces deux techniques étant utilisables pour toute infraction punie d'une peine de trois ans d'emprisonnement ou plus.

---

[1] *Voir, par exemple, la décision n° 2014-420/421 QPC du 9 octobre 2014, considérant 9 :* « au nombre de[s libertés constitutionnellement garanties] figurent la liberté d'aller et venir, l'inviolabilité du domicile, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789, ainsi que la liberté individuelle ».

[2] *Benoît Auroy, article précité.*

[3] *La géolocalisation en temps réel suppose toutefois, contrairement à l'accès aux données de connexion, l'intervention du juge des libertés et de la détention au-delà de huit jours (étant rappelé que, en-dessous de ce délai, seule l'autorisation du procureur de la République est requise).*

La deuxième limite de cette distinction entre le contenu et le « contenant » est qu'elle est **remise en question par le fonctionnement d'internet, qui génère des données dont la catégorisation est de plus en plus complexe.** Ainsi que le soulignait lors de son audition Patrick Pailloux, conseiller d'État, la notion de « données de connexion » recouvre une quantité substantielle d'informations de natures diverses ; or, si la distinction entre le contenu et le contenant est simple à appréhender lorsqu'on l'applique à un courriel (le « contenant » correspondant aux indications relatives à l'expéditeur et à son interlocuteur et le « contenu », le texte envoyé), elle perd de sa pertinence lorsqu'on tente de l'appliquer à certaines catégories de données. En témoignent les récents débats législatifs sur le statut des URL dans le cadre de l'examen du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement (devenu la loi n° 2021-998 du 30 juillet 2021), au cours duquel les rapporteurs du Sénat relevaient que **« *les URL constituent des données mixtes, comprenant à la fois des données de connexion, c'est-à-dire des éléments relatifs à l'acheminement de la communication internet, et des données de communication, c'est-à-dire des éléments fournissant des précisions sur l'objet ou le contenu du site internet consulté* »**[1] (le libellé des URL, c'est-à-dire des adresses des sites internet visités par un utilisateur, étant très souvent un révélateur direct et explicite de la nature de l'information consultée) ; malgré ce statut à part, les URL sont aujourd'hui intégrées, au même titre que les données de connexion « classiques », au champ matériel des données susceptibles d'un traitement algorithmique en application de l'article L. 851-3 du code de la sécurité intérieure comme à celui des données techniques auxquelles les services de renseignement peuvent accéder en temps réel sur le fondement de l'article L. 851-2 du même code (voir *supra*).

**La même hybridité s'applique aux données générées par les applications sur *smartphone*** : ces dernières génèrent, en effet, une très grande quantité de données qui sont développées (et traitées) librement par des acteurs privés et dont certaines ont une nature hybride ; à titre d'illustration, le numéro de compte qui sert d'identifiant pour une application bancaire peut à la fois être analysé comme une donnée de « contenant », car il s'agit fonctionnellement d'un identifiant, et comme un « contenu », le numéro de compte étant en soi une information signifiante. **La même observation vaut, peut-être encore davantage, pour des applications dont la fonction même renvoie à des éléments de la vie privée de l'utilisateur** (applications de rencontre, applications de prise de rendez-vous médical, *etc.*).

Ces éléments brouillent la prise en charge juridique des données numériques et remettent en cause la traditionnelle distinction qui présidait, bien qu'imparfaitement, à la définition des régimes probatoires.

---

[1] *Rapport n° 778 (2020-2021) d' Agnès CANAYER et Marc-Philippe DAUBRESSE, déposé le 20 juillet 2021.*

### *B. UN RÔLE DÉSORMAIS CENTRAL DANS L'ÉLUCIDATION DES INFRACTIONS*

#### 1. De l'utilité des métadonnées dans l'enquête pénale

Les métadonnées apportent aux services de police et de gendarmerie de nombreux éléments de fond pour caractériser une infraction, révéler des liens de complicité ou encore identifier des témoins. **Mais elles sont aussi utilisées à décharge**, l'alibi d'une personne pouvant être attesté par des données de connexion qui la localisent hors du secteur de commission d'une infraction au moment de celle-ci.

Selon les éléments recueillis par les rapporteurs au cours de leurs auditions et déplacements, les **principaux usages des données de connexion** sont les suivants :

– l'identification des protagonistes d'une infraction (auteurs, victimes, mais aussi témoins ou complices) grâce aux données non seulement d'identification *stricto sensu* mais aussi de trafic, avec notamment :

- l'établissement de la liste des contacts d'une victime ou d'un suspect et l'analyse des caractéristiques des messages et appels (date, horaire, durée…), ces informations étant **potentiellement révélatrices d'un environnement relationnel qui peut contribuer à l'élucidation des affaires.** Elles sont, en particulier, précieuses lorsque la ligne utilisée par un délinquant est reliée à une fausse identité ou enregistrée au nom d'un tiers qui n'en est manifestement pas l'utilisateur réel : dans une telle hypothèse, c'est par l'analyse des principaux contacts de l'utilisateur que les services de police ou de gendarmerie parviennent à attribuer la ligne à son détenteur effectif ; symétriquement, l'étude de la liste des contacts d'un suspect peut révéler l'existence d'une ligne « occulte » (comme le sont fréquemment les lignes dédiées à une activité criminelle) qui, bien qu'elle ne soit pas officiellement rattachée à une personne citée dans l'enquête, s'avérera être utilisée par celle-ci ;
- corrélativement, l'identification – grâce aux numéros contactés par un suspect – d'éventuels complices, les données d'identification permettant de faire le lien entre un numéro téléphonique et une identité civile ;
- **l'identification, grâce aux numéros IMEI, des différentes cartes SIM utilisées sur un même téléphone**, cette information étant par exemple utile en cas de vol pour identifier un receleur ;
- la découverte, pour les infractions commises en ligne ou dont la préparation s'est traduite par un échange de messages sur internet, de **l'identité réelle d'une personne qui utilise un pseudonyme** ;

– **la vérification, grâce à la localisation des téléphones portables (aussi appelée « bornage »), des déplacements d'un suspect ou d'une personne recherchée** : les données de localisation peuvent être utilisées à la fois pour estimer la localisation de l'utilisateur, par référence aux antennes-relais auxquelles il s'est trouvé relié, comme pour définir la liste des utilisateurs présents dans une même zone à un instant déterminé *via* le recueil des flux ayant transité par une ou plusieurs bornes. Elles permettent ainsi, selon la direction générale de la police nationale, « *de conforter les déclarations d'un mis en cause contestant s'être trouvé sur le lieu des faits dont on l'accuse, ou au contraire d'établir sa présence sur un site, de retrouver des personnes portées disparues ou ayant indiqué une volonté suicidaire* » ou encore, comme l'indique la conférence nationale des procureurs de la République, d'apporter « *des éléments utiles sur les déplacements des personnes suspectées et leurs habitudes de vie, afin par exemple de faciliter leur interpellation* ». Elles permettent également, par recoupement des numéros de téléphone ayant « borné » dans certains lieux au moment de la commission de plusieurs infractions, d'en identifier l'auteur ;

– la **mise au jour de l'utilité fonctionnelle d'un appareil** : comme le relève la direction générale de la police nationale, « *le type de données de trafic (voix, SMS, DATA) renseigne sur l'utilisation du terminal de communications (ligne 'de vie', ligne dédiée à un circuit fermé de terminaux, ligne associée à un* tracker*…)* », permettant par exemple d'identifier, dans une affaire de prostitution, le téléphone utilisé comme « standard » par des proxénètes (dont la nature peut être révélée par le fait qu'il reçoive un nombre important de SMS provenant d'un nombre important de numéros toujours différents) ;

– dans les formes de criminalité les plus graves et conformément aux principes de subsidiarité et de proportionnalité posés par le législateur, le **préalable à l'utilisation de techniques plus lourdes et plus intrusives.** L'un des magistrats de la section F3 du parquet de Paris (délinquance organisée et stupéfiants) soulignait ainsi devant les rapporteurs que **les données de connexion permettent de faire un « *premier tri* » avant de solliciter l'autorisation de recourir aux écoutes et/ou à la géolocalisation en temps réel** afin que l'utilisation de ces techniques soit limitée aux lignes pertinentes.

Par ailleurs et par nature, **les données de connexion sont également l'un des seuls moyens d'élucider les crimes et délits commis en ligne, ou à tout le moins le seul « point d'entrée » pour identifier les auteurs** ; elles sont donc essentielles à la lutte contre les actes de cyber-délinquance de toute nature (fraudes sur internet, cyber-attaques, menaces et appels à la violence en ligne, « rançongiciels », pédopornographie et infractions sexuelles sur mineurs en ligne…).

En bref, et comme le résumait l'un des enquêteurs que les rapporteurs ont rencontrés au commissariat central du 17e arrondissement de Paris, les données de connexion sont fréquemment le seul moyen de répondre aux questions essentielles de l'investigation pénale, à savoir le « qui ? », le « quand ? » et le « où ? ».

### 2. L'émergence d'un monopole probatoire

Mais la véritable particularité des données de connexion réside dans la **place singulière qu'elles occupent désormais dans le dispositif d'enquête, où elles ont acquis une forme de monopole probatoire.** Ainsi que le relève le criminaliste Benoît Auroy, « *Alors même qu[e la preuve numérique] n'a qu'une valeur indiciaire, la pratique lui a reconnu une remarquable force de conviction* »[1] : les données de connexion sont devenues une preuve « reine », susceptible de faire ou de défaire un dossier, de disculper comme d'inculper.

Ce rôle central s'explique par un constat : à rebours de l'image d'Épinal d'une enquête pénale se dénouant au cours des auditions grâce aux informations données par des témoins ou aux aveux d'un suspect, la présence des avocats et l'usage de plus en plus répandu du « droit au silence » seraient venus priver la garde à vue de son rôle traditionnellement central dans la conduite des investigations. De même, face aux réticences de plus en plus fortes des citoyens à voir leur nom apparaître dans des procédures pénales, et donc à apporter leur témoignage aux enquêteurs, les données de connexion deviennent le seul moyen d'établir la présence d'un suspect sur les lieux d'une infraction ou l'existence de relations entre deux personnes qui apparaissent complices mais prétendent ne pas se connaître.

Parallèlement, les délinquants aguerris semblent avoir développé des stratégies afin d'éviter de laisser des traces physiques (empreintes, ADN) sur les lieux des infractions : l'utilité des moyens d'investigation biologique et génétique serait ainsi devenue réservée aux « *primo-délinquants encore peu affûtés aux moyens de la police technique et scientifique* »[2]. À l'inverse, et comme le relevait la direction générale de la gendarmerie nationale lors de son audition par les rapporteurs, les traces numériques dépendent de tiers, les opérateurs, et ne sont pas maîtrisées par celui qui les produit : elles sont donc quasiment impossibles à effacer.

Dans ce contexte, **les métadonnées constituent souvent le seul moyen, pour les enquêteurs, de disposer d'éléments matériels susceptibles de conduire à l'élucidation d'une affaire ;** elles présentent également la particularité d'être des données objectives, ce qui les rend (contrairement à des témoignages, par exemple) difficilement contestables par les personnes mises en cause.

---

[1] *Benoît AUROY, « La preuve numérique en procédure pénale : un système à (re)construire », Recueil Dalloz, 2023, p. 697.*

[2] Ibid.

En outre, l'ensemble des personnes entendues par les rapporteurs ont rappelé que **les données de connexion permettent une accélération substantielle de l'élucidation des enquêtes, ainsi qu'un gain important en effectifs** : la découverte d'un nombre d'informations comparable à celui que permet la consultation des données de connexion supposerait, si elle était traduite en moyens humains, une « consommation » difficilement soutenable d'emplois de gendarme et de policier. Ainsi, pour connaître les déplacements d'une personne (par exemple dans le cas où les allées et venues de celle-ci révèlent des repérages avant des cambriolages, ou encore la localisent sur les lieux de commission d'infractions sérielles graves), **l'accès aux données de connexion offre une exhaustivité et une facilité qu'une surveillance humaine, bien plus coûteuse, ne saurait garantir.** Comme le synthétise le conseiller d'État Alexandre Lallet, rapporteur public de la décision *French data network* de 2021, dans ses conclusions, « *le recours exclusif à des méthodes traditionnelles d'investigation nécessiterait des moyens humains considérables que notre pays ne peut s'offrir dans les proportions qui seraient nécessaires pour compenser la perte de capacités opérationnelles enregistrées* ».

Les rapporteurs ont par ailleurs constaté que, loin de remettre en cause l'utilité des données de connexion, **la montée en puissance de technologies échappant à la téléphonie classique ne faisait qu'en renforcer l'importance pour les acteurs de l'enquête**. En effet, l'essor du chiffrement de bout en bout des échanges et du recours à des messageries cryptées rend impossible, ou presque, l'interception du contenu des communications par des voies classiques (c'est-à-dire *via* les opérateurs) : avec le cryptage, la captation des contenus suppose désormais des « chevaux de Troie », qui sont des procédés techniques lourds et coûteux. Cette évolution a eu pour effet paradoxal de rendre les métadonnées plus essentielles encore, puisqu'elles constituent dans de nombreux cas les seules données qui ont transité par le réseau cellulaire – et donc les seules indications techniquement exploitables[1]. En d'autres termes, **face à un contenu devenu inaccessible, le « contenant » est désormais la principale source d'informations des enquêteurs de la police et la gendarmerie.**

La valeur probante acquise par les données de connexion **s'est aussi progressivement diffusée auprès des magistrats du siège, qui les voient comme un gage de fiabilité de l'accusation**, même pour les infractions les plus simples et y compris, dans certains cas, pour des délits flagrants. Il a ainsi été relevé par les personnes auditionnées par les rapporteurs, et notamment par les praticiens de l'enquête pénale, que l'absence de métadonnées dans un dossier était systématiquement interprétée par les juges comme la marque d'une investigation incomplète, de nature à générer

[1] *Comme le relève la DGPN, l'utilisation de messageries cryptées, de plus en plus fréquente par les groupes organisés, réduit déjà notablement l'identification des criminels de ces réseaux. Les données de trafic et de localisation restent le seul moyen de cibler leurs déplacements, points de rencontre, présence sur le lieu des faits et les appareils utilisés.*

un doute qui devait profiter aux accusés et conduire à leur relaxe. Comme l'illustre la DGPN, « *le bornage est […] devenu un véritable élément de preuve demandé quasi-systématiquement par les magistrats pour vérifier la présence d'un suspect sur les lieux de l'infraction, y compris pour un vol à la tire ou un vol à l'arrachée* ».

Ces éléments convergent pour créer, comme le résumait le procureur général près la Cour de cassation François Molins lors son audition, une **« *dépendance* » des policiers et gendarmes envers les métadonnées.**

Les rapporteurs estiment, plus largement, que **cette dépendance touche – au moins autant que les enquêteurs – les autres acteurs de la chaîne pénale, ainsi que les citoyens.** Dans un contexte où le sentiment d'insécurité va croissant et où de fortes attentes s'expriment quant au maintien d'un taux élevé d'élucidation, il semble en effet illusoire de renoncer aux informations révélées par les données de connexion : **loin d'être un caprice des enquêteurs, la recherche des moyens les plus performants pour résoudre une affaire est une exigence non seulement des victimes, mais aussi et surtout du corps social dans son ensemble.**

## II. LA STRUCTURATION PROGRESSIVE D'UN USAGE DEVENU MASSIF

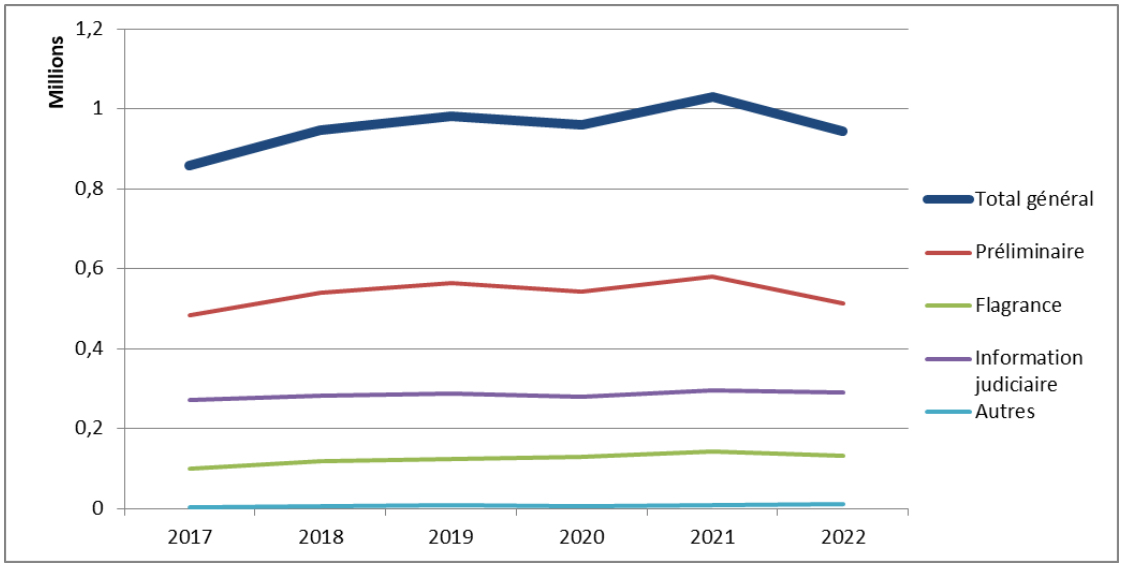
Les données de connexion présentent, pour les services enquêteurs, des avantages considérables. Outre la facilité longtemps accordée par le droit français pour y recourir, **elles sont peu onéreuses** (notamment en comparaison du coût substantiel lié à l'usage d'autres techniques) **et, depuis le milieu des années 2010 et la mise en service de la plateforme nationale des interceptions judiciaires (PNIJ), aisément accessibles**. Il n'est donc pas étonnant qu'elles soient devenues un outil de choix, **plusieurs centaines de milliers de données étant exploitées chaque année dans un cadre pénal avec une croissance annuelle de l'ordre de 10 % jusqu'en 2022.**

### *A. UN ACCÈS LARGE QUI CONCERNE PLUSIEURS CENTAINES DE MILLIERS DE DONNÉES CHAQUE ANNÉE*

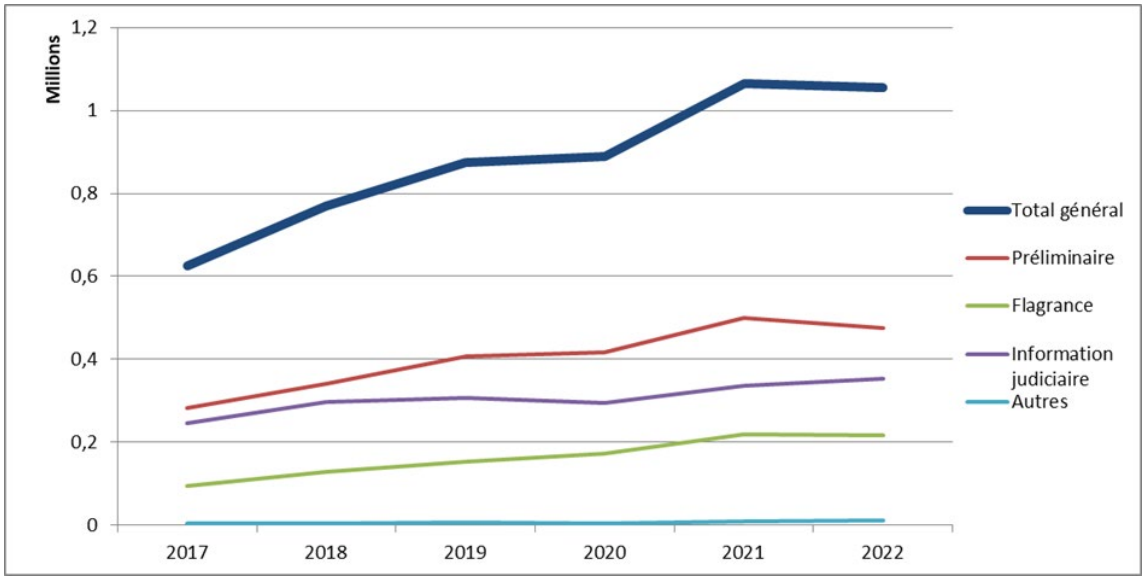
Comme le confirment les chiffres communiqués par l'Agence nationale des techniques d'enquête numériques judiciaires (ANTENJ), gestionnaire de la PNIJ, l'utilisation des données de connexion a connu une croissance continue jusqu'à l'intervention, en juillet 2022, d'arrêts de la chambre criminelle de la Cour de cassation remettant en cause le rôle du parquet et qui seront commentées plus loin. Ce sont ainsi environ un million de données d'identification et, sur la fin de la période étudiée, autant de

données de trafic et de localisation conservées par les quatre OCE dits « majeurs » (c'est-à-dire les opérateurs de téléphonie Bouygues, Free, Orange et SFR) qui ont été exploitées chaque année depuis 2017, selon l'évolution représentée par les schémas ci-dessous[1].

**Données d'identification (2017-2022), par cadre d'enquête**




**Données de trafic et de localisation (2017-2022), par cadre d'enquête**




*Source : commission des lois du Sénat*

Au-delà de ces chiffres, une analyse par nature des données de connexion utilisées par les services d'enquête témoigne de **l'importance quantitative des données d'identification, soit pour identifier l'ensemble des utilisateurs présents sur une zone par « bornage », soit pour associer**

[1] *Schémas établis par la commission des lois du Sénat sur la base des chiffres fournis par ANTENJ, hors données relatives à la recherche de personnes.*

**une identité civile à un numéro d'appel** : ces réquisitions représentent près de la moitié des accès aux données de connexion conservées par les quatre principaux opérateurs de téléphonie. Viennent ensuite les **factures détaillées, ou « fadettes »,** qui comportent à la fois l'heure et la durée des appels (donc des données de trafic), les numéros des correspondants (données d'identification) et les coordonnées spatiales de l'antenne-relai déclenchée par le terminal (données de localisation).

Il convient, toutefois, d'appréhender ces chiffres avec prudence : en effet, **plusieurs données sont parfois nécessaires à l'accomplissement d'un seul acte d'enquête** et, comme l'indique la conférence nationale des procureurs de la République, « *une seule demande de bornage visant à obtenir le trafic sur une borne de téléphonie mobile peut se traduire par la délivrance d'une dizaine de réquisitions (4 OCE ayant chacun 3 antennes pour couvrir 360° sur une borne)* ». De la même manière, plusieurs accès ayant un même objet peuvent se succéder au cours d'une enquête : lorsqu'un « bornage » permet d'identifier des terminaux nouveaux, des données complémentaires sont nécessaires pour faire le lien entre la ligne concernée et l'abonné qui y est rattaché. Les statistiques présentées, sans être négligées, doivent donc être relativisées.

Une autre grille d'analyse de ces chiffres tient à la nature des dossiers. En effet, **plus une affaire est complexe, plus elle est « consommatrice » en données de connexion**, si bien que les accès se concentrent en pratique sur les infractions les plus graves : un magistrat de la section P12 du parquet de Paris estimait ainsi que, pour les dossiers couverts par le large périmètre de compétence de son service (« Traitement en temps réel des majeurs », c'est-à-dire les infractions flagrantes), 85 % des données consultées par les enquêteurs étaient exploitées dans le cadre d'une infraction liée au trafic de stupéfiants.

Il n'en reste pas moins que ces chiffres témoignent d'un accès massif aux données de connexion par les services enquêteurs, cette situation trouvant sa source, au moins pour partie, dans la **facilité d'un tel accès jusqu'en 2022.**

En effet, et en dépit de leur spécificité, **les métadonnées ont longtemps été incluses dans le droit commun des réquisitions judiciaires**, applicable au « tout-venant » de la preuve en matière pénale. Or ce statut pose question dans un contexte où de telles réquisitions constituent un mode de preuve extrêmement général et peu contrôlé, voire une « *technique probatoire à tout faire* »[1].

Jusqu'à la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire (voir *infra*), les métadonnées étaient ainsi soumises au régime prévu par le code de procédure pénale qui permet, tant en flagrance

[1] *Pour reprendre l'expression employée par le professeur Etienne Vergès lors de son audition par les rapporteurs.*

(article 60-1) qu'en enquête préliminaire (article 77-1-1) et dans le cadre d'une information judiciaire (article 99-3), au magistrat compétent (procureur de la République ou juge d'instruction) ou aux officiers de police judiciaire (ainsi que, sous le contrôle de ces derniers et hors information judiciaire, aux agents de police judiciaire), de requérir « *par tout moyen* » et « *de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique* », des « *informations intéressant l'enquête* », quelle qu'en soit la nature et sans limitation particulière.

La réponse à de telles réquisitions est une obligation juridique pour ceux qui en sont l'objet, l'absence de suite donnée « *dans les meilleurs délais* » étant passible d'une amende de 3 750 euros (article 60-1 précité).

Sur le fondement de ce régime généraliste, **les données de connexion étaient par ailleurs exploitables pour n'importe quelle infraction**, sans critère de gravité et sans mention d'un quantum minimal de peine encourue (voir ci-après).

Dès lors, et comme l'a résumé la conférence nationale des procureurs auprès des rapporteurs, « *l'exploitation des données de connexion, de localisation était ainsi un acte d'enquête courant, quels que soient l'infraction commise et le cadre d'enquête* » ; **le choix d'y recourir ou non était dicté par des considérations d'opportunité** tenant à la fois à l'objectif de « *maîtrise des frais de justice* » - chaque réquisition auprès des opérateurs devant faire l'objet d'une compensation financière - et au respect des instructions permanentes émises par les procureurs de la République visant, par exemple, à limiter l'engagement de moyens techniques et humains en cas de préjudice faible.

### *B. LA « MISE EN ORDRE » PROGRESSIVE DES ACCÈS*

#### 1. Un accès initialement décentralisé, coûteux et peu régulé

Pour qu'elles puissent être consultées en temps différé, encore faut-il que les données de connexion aient été préalablement conservées.

C'est au début des années 2000, déjà sous l'effet d'une directive européenne, que la loi a posé le principe et défini les modalités de la conservation des données de connexion par les OCE[1], apportant une base juridique à une pratique d'enquête émergente sur internet, mais déjà bien établie en matière de téléphonie.

---

[1] *Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, et loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. Il est intéressant de noter que, résultant d'un amendement déposé en lecture définitive à l'Assemblée nationale par le rapporteur sur le projet de loi relatif à la sécurité quotidienne, Bruno Le Roux, les dispositions relatives aux données de connexion et à leurs modalités de conservation ont été adoptées sans aucun débat.*

Ce principe de conservation est, en réalité, **une dérogation à un impératif plus large, lui aussi inscrit dans le droit européen comme dans la loi, à savoir celui de l'anonymisation ou de l'effacement des données liées aux communications électroniques** : en d'autres termes, hors des hypothèses dans lesquelles la conservation est prescrite ou autorisée[1] par la loi, elle est strictement interdite.

Le système ainsi instauré repose sur l'obligation d'une **conservation effectuée directement par les opérateurs**, en contrepartie d'une compensation financière[2] ; cette conservation est **à la fois générale et indifférenciée, ce qui signifie qu'elle touche l'ensemble des données de connexion et l'intégralité des lignes et des abonnés**.

Codifiée depuis 2001 au sein du code des postes et télécommunications, la conservation présente une durée variable en fonction de la nature des métadonnées en cause. Jusqu'à l'intervention de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, qui a modifié en profondeur le régime de conservation des données de connexion pour l'adapter aux arrêts de la Cour de justice de l'Union européenne (voir *infra*), les opérateurs devaient ainsi conserver, **pour une durée d'un an** :

– des données d'identification : les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication utilisés (numéro IMEI, par exemple) ; les données permettant d'identifier le ou les destinataires de la communication ;

– des données de trafic : les caractéristiques techniques ainsi la date, l'horaire et la durée de chaque communication (donc des données de trafic) ; les données relatives aux services complémentaires demandés ou utilisés et à leurs fournisseurs ;

– des données de localisation : les données permettant d'identifier l'origine et la localisation des communications téléphoniques.

Avant 2021, le code des postes et communications électroniques donnait à cette conservation un périmètre fonctionnel singulièrement large, puisqu'il la liait aux « *besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle* [i.e. *la prévention du téléchargement illicite d'œuvres protégées par le droit d'auteur ou un droit voisin] ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du*

[1] *Outre l'obligation de conservation liée aux besoins de la puissance publique, les opérateurs bénéficient d'une autorisation de conserver des données techniques utiles à la sécurité des réseaux ou des installations ou nécessaires à la facturation (article R. 10-14 du code des postes et des communications électroniques).*

[2] *Cette compensation est forfaitaire pour les investissements en équipements (notamment de stockage et de traitement des données) réalisés par les opérateurs, mais « à l'acte » pour l'accès effectif aux données de connexion.*

*code pénal* ». Le code précise que la conservation s'effectue conformément aux principes fixés par la loi n° 78-17, dite « informatique et libertés » du 6 janvier 1978, ce qui constitue de toute évidence un garde-fou important et un gage de protection pour les droits et libertés des utilisateurs.

Depuis 2000[1], des règles analogues existent s'agissant des données devant être conservées par les fournisseurs d'accès à internet ; elles sont, depuis 2004, intégrées au cadre général de la loi n° 2004-575 pour la confiance en l'économie numérique.

Sous l'effet d'une démocratisation de l'usage des téléphones portables et des accès à internet, le recours aux données de connexion dans l'enquête pénale s'est développé dès le début des années 2000 ; il passait alors par **l'envoi aux opérateurs de réquisitions de droit commun sous format « papier »**, avec des délais de traitement souvent longs, et **supposait l'intervention de sociétés tierces fournissant des équipements techniques aux services de police et de gendarmerie** et intervenant à ce titre pour des prestations spécifiques et sensibles (à l'instar des interceptions de sécurité), mais aussi pour le traitement des réquisitions de données de connexion adressées aux opérateurs.

Cette évolution a généré un **surcoût important qui, initialement décentralisé et géré individuellement par chaque juridiction et par chaque opérateur** (avec des pratiques tarifaires libres jusqu'en 2006[2] et des délais de réponse variables), **est rapidement venu saturer les frais de justice**. La Cour des comptes indiquait ainsi[3] que, pour 2015, le coût des interceptions judiciaires (très majoritairement constitué par les frais relatifs à l'accès aux données de connexion) s'élevait à 122,55 M €, dont plus de 110 M € sur frais de justice, et constituait une dépense cumulée d'environ 1 Md € sur dix ans.

Le Gouvernement avait souhaité, dès 2007, simplifier l'architecture technique d'accès aux données de connexion en créant une plateforme *ad hoc* destinée à recevoir les données issues non seulement de la conservation effectuée par les opérateurs, mais aussi des interceptions judiciaires de toute nature[4]. Cette solution technique devait offrir une double facilité aux services d'enquête et aux OCE : d'une part, l'accès s'en trouvait pour une large partie automatisé, limitant les interventions humaines et centralisant les investissements techniques, et donc réduisant les coûts ; d'autre part,

---

*[1] Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.*

*[2] À titre d'illustration, on notera que la régulation tarifaire instaurée par un arrêté du 22 août 2006 a permis de faire passer les frais de justice associés aux données de connexion de 69 millions d'euros en 2005 à 38,28 millions d'euros en 2006 (source : avis n° 106 (2009-2010) sur le projet de loi de finances pour 2010 présenté, au nom de la commission des lois, par Yves Détraigne et Simon Sutour).*

*[3] Référé S 2016-0336-1 en date du 18 février 2016.*

*[4] Décret n° 2007-1145 du 30 juillet 2007 instituant un système de traitement automatisé de données à caractère personnel (dénommé « système de transmission d'interceptions judiciaires »). En 2007, étaient notamment conservés, pendant 30 jours, les SMS interceptés.*

elle permettait de **mettre en place un format standardisé en lieu et place de demandes ponctuelles écrites** (donc des fax ou des courriels) à la fois fastidieuses à traiter et susceptibles d'être falsifiées.

C'est dans le prolongement de cette initiative qu'a été **décidée la création d'une plateforme nationale des interceptions judiciaires (PNIJ) qui**, instituée par un décret n° 2014-1162 du 9 octobre 2014, **devait répondre à un triple défi** :

– premièrement, celui de la responsabilisation financière, le système préexistant conduisant à imputer aux frais de justice (et donc à faire porter par le ministère de la justice) des dépenses trouvant leur origine dans les choix effectués par les officiers de police judiciaire ;

– ensuite, celui d'une **meilleure maîtrise de l'écosystème des données de connexion et d'un « recentrage » sur les OCE**, dans un contexte où l'intervention de sociétés privées d'appui technique aux côtés des opérateurs posait des difficultés certaines[1] ;

– enfin et surtout, celui de la **traçabilité des accès aux données de connexion**, le dispositif technique antérieur ne permettant le suivi par les magistrats ni des réquisitions formulées par la police et la gendarmerie, ni des réponses apportées par les opérateurs[2].

**La chronologie du projet témoigne par elle-même des difficultés rencontrées par l'État dans la mise en œuvre de la plateforme**. La création par décret du traitement de données personnelles qui sert de support à celle-ci est en effet intervenue en 2014 soit presque dix ans après la décision gouvernementale de centraliser l'accès aux données, sept ans après la création d'une plateforme embryonnaire et cinq ans après l'attribution à Thalès du partenariat public-privé qui devait faire naître la PNIJ. Le projet n'avait toujours pas abouti en 2016, date à laquelle la Cour des comptes a rendu public un référé mettant en évidence des défaillances dans le pilotage du projet[3]. Ce référé a eu l'effet d'un coup de semonce ; il a incité, après une décennie d'errements, à une salutaire reprise en main du dossier.

---

[1] *Le référé précité de la Cour des comptes relevait que, du fait notamment des tarifs pratiqués par ces intermédiaires, les coûts supportés par l'État avaient longtemps été supérieurs aux frais exposés par les acteurs privés ; plus encore, il considérait que* « la place prise par les sociétés privées d'appui technique aux interceptions [avait] soulevé, au moins jusqu'en 2015, des interrogations quant […] aux garanties de protection du secret de l'instruction ».

[2] *Cette absence de traçabilité pouvait donner lieu à des pratiques illégales dont la presse se faisait régulièrement l'écho et dénommées « écoutes-taxis », ce terme désignant le fait, pour un enquêteur, d'ajouter manuellement une ligne sur la liste des écoutes autorisées par un magistrat.*

[3] *Référé S 2016-0336-1 précité.*

### 2. La régulation par la technique : la création de l'agence ANTENJ

C'est sous l'effet de ce référé, et dans un contexte *a minima* dégradé, que **le recours à la PNIJ a été rendu obligatoire par voie réglementaire en 2014[1] puis que le pilotage de celle-ci a été confié, en 2017, à un service de l'État à compétence nationale dédié :** l'Agence nationale des techniques d'enquête numériques judiciaires **(ANTENJ)**.

**L'agence ANTENJ**

Créée par un décret n° 2017-614 du 2017, l'Agence nationale des techniques d'enquête numériques judiciaires est un service à compétence nationale notamment chargé de **veiller au bon fonctionnement de la PNIJ**. Le code de procédure pénale précise que le service est dirigé par un magistrat de l'ordre judiciaire et rattaché au secrétaire général du ministère de la justice (article R. 40-51) et que l'ensemble de ses personnels sont habilités au niveau « secret » et soumis au secret professionnel (article R. 40-52). Pour 2024, les crédits prévus par le projet de loi de finances pour l'action d'ANTENJ en matière de développement des techniques d'enquêtes numériques judiciaires, incluant notamment la PNIJ, se montent à 32,7 M€ en AE et à 50 M€ en CP ; l'Agence disposera, par ailleurs, de 73,3 ETPT.

À titre principal, **ANTENJ exerce trois missions : l'infogérance et la maintenance corrective des services** (cette tâche n'étant pas la moindre au vu de la complexité du système d'information associé et de ses interconnexions avec les opérateurs et les utilisateurs) ; le **développement de nouveaux outils** d'exploitation des données pour répondre aux besoins des usagers ; **l'assistance aux utilisateurs**.

Par ailleurs, ANTENJ communique avec la **personnalité qualifiée en charge du contrôle de la PNIJ** (article R. 40-53 du code de procédure pénale) ainsi qu'avec les autres entités appelées à effectuer des contrôles sur la PNIJ, comme la Cnil (dont le dernier contrôle a eu lieu en 2022-2023) ou l'ANSSI (qui a mené un audit en 2016).

**Ses compétences s'exercent en parallèle de celles du Commissariat aux communications électroniques de défense (CCED)**, autre service à compétence nationale rattaché au chef du service de l'économie numérique de la direction générale des entreprises. Le CCED « *coordonne les relations avec les opérateurs en matière de déploiement d'équipements d'interception et de mise à disposition de données* » (article 2 de l'arrêté du 29 décembre 2017 érigeant le commissariat aux communications électroniques de défense en service à compétence nationale). Auditionné par les rapporteurs, Didier Vidal, administrateur interministériel des communications électroniques de défense, a rappelé qu'en matière de données de connexion, **le CCED joue un rôle de supervision technique** (définition des spécifications techniques des équipements déployés par les opérateurs pour mettre en œuvre leurs obligations légales, mise en place des liaisons entre les opérateurs et les plateformes, vérification de leur bon fonctionnement et du respect des normes de sécurité informatique…) qui ne touche pas à l'exploitation des données, mais à la mise en place d'outils communs pour **rationaliser les dépenses de l'État comme des opérateurs et garantir le meilleur niveau de « service » possible**. Le CCED travaille actuellement sur un nouvel outil, appelé PHENOMENE, qui doit permettre à terme d'automatiser encore davantage les réquisitions.

*Source : commission des lois du Sénat*

[1] *Décret n° 2014-1162 du 9 octobre 2014 ; l'obligation de recourir à la PNIJ résulte depuis 2017 d'une disposition législative (article 230-45 du code de procédure pénale, introduit par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*

La PNIJ centralise les réquisitions liées non seulement aux accès aux données de connexion, mais aussi aux autres techniques d'enquête prévues par le code de procédure pénale, notamment pour la lutte contre la criminalité organisée, qui reposent sur la téléphonie, à l'instar des interceptions judiciaires et de la géolocalisation en temps réel. **Elle offre un lien direct entre les services enquêteurs et une vingtaine d'opérateurs, couvrant à la fois les principaux opérateurs de téléphonie**, dits « historiques » (aujourd'hui Bouygues Télécom, Free, Orange et SFR[1]) et d'autres acteurs qui, moins connus du grand public, comptent un nombre important d'utilisateurs (comme par exemple La Poste Mobile, avec environ 2 millions d'abonnés). Il conviendra d'y ajouter, à court terme, une dizaine d'opérateurs virtuels en cours de raccordement à la plateforme.

**La PNIJ constitue, en outre, un gage de réactivité** : selon les informations transmises par ANTENJ lors de l'audition de son directeur et de l'adjoint de ce dernier, le recours à des formulaires de réquisition **permet de traiter environ 90 % des demandes *via* des automates**, ce qui représente un gain de temps considérable pour les OCE comme pour les enquêteurs.

En 2022, la PNIJ comptait plus de 63 000 utilisateurs (magistrats, gendarmes et policiers, mais aussi agents des douanes et des services fiscaux judiciaires)[2] : **elle constituait donc le principal système d'information utilisé par les services d'enquête initiale** (exception faite des simples fichiers). Elle assure, en parallèle, une **fonction de « coffre-fort numérique »** qui non seulement garantit l'intégrité des informations recueillies, mais aussi permet une traçabilité des actions effectuées par les OPJ pendant trois ans pour prévenir ou détecter les cas de mésusage de la plateforme.

Concrètement, pour des affaires simples (et hors instruction), le fonctionnement de la plateforme peut être résumé de la manière suivante :

– après un appel téléphonique au parquet (ou au juge d'instruction) pour obtenir l'autorisation d'accéder aux données de connexion, l'officier de police judiciaire s'identifie sur la PNIJ, celle-ci n'étant utilisable (et cette caractéristique est une garantie essentielle de sécurité des données et de traçabilité des accès) **que depuis un poste informatique relié au réseau interne des forces de sécurité intérieure et avec l'utilisation d'une carte professionnelle qui authentifie son détenteur**, cette authentification étant renforcée par l'utilisation d'un code d'accès[3] ;

---

[1] *Ce raccordement constitue un point essentiel pour l'efficacité du système puisque, à l'exception des hypothèses techniques qui seront développées* infra *(opérateurs OTT, opérateurs satellitaires…) et qui restent à date numériquement marginales, la couverture de ces quatre acteurs permet de toucher par « ricochet » les opérateurs numériques dont les données transitent par les installations physiques des OCE précités.*

[2] *Selon les documents annexés au projet de loi de finances pour 2024 pour la mission « Justice », la PNIJ comptait précisément 63 107 utilisateurs en 2022 : 33 915 au sein de la gendarmerie, 28 101 au sein de la police, 812 magistrats et 279 enquêteurs du service des enquêtes judiciaires des finances (SEJF).*

[3] *Article R. 40-47. La chambre criminelle de la Cour de cassation a récemment (23 mai 2023, pourvoi n° 22-83.462) rappelé que l'accès à la PNIJ était ouvert à l'ensemble des officiers de police judiciaire de la police et de la gendarmerie, sans habilitation ou sans désignation hiérarchique particulière.*

– l'utilisateur remplit ensuite un certain nombre de champs relatifs à l'enquête et à ses caractéristiques : son cadre juridique (flagrance, enquête préliminaire, sur commission rogatoire, liée à une recherche de personne…), la désignation du magistrat compétent (son identité, sa fonction, son tribunal de rattachement), le numéro de la procédure, *etc*. Les champs nominatifs sont contraints (ils sont reliés aux systèmes d'information des ministères de l'intérieur et de la justice, rendant impossible la saisie d'une identité fictive) et d'autres font l'objet d'un remplissage automatique (à l'instar de la fonction du magistrat compétent et de sa juridiction, renseignées directement par la plateforme par association avec le nom) ; en revanche, l'ensemble est déclaratif, ce qui veut dire que **la PNIJ ne contrôle ni la cohérence des informations saisies par l'OPJ** (par exemple, en vérifiant que le magistrat désigné comme ayant autorisé l'accès aux données exerce bel et bien dans le même ressort que l'OPJ qui y accède), **ni *a fortiori* leur véracité** ;

– l'OPJ peut ensuite sélectionner la nature des données de connexion qu'il souhaite requérir auprès de l'opérateur et la période concernée, selon un **système de « panier » qui fait apparaître le coût de chaque « prestation »**[1], un écran « prestations courantes » permettant un accès aisé aux données de connexion les plus fréquemment requises ;

– la réponse de l'opérateur s'affiche sur la PNIJ, dans un **délai généralement très court** (compris entre quelques minutes et une heure, en fonction du type de données et de l'opérateur) ;

– les informations restent accessibles à l'OPJ et au magistrat compétent pendant toute la durée de l'enquête, étant relevé que les accès de magistrats semblent rares en pratique : ils seraient en effet limités aux cas où un usage disproportionné est invoqué par la défense au cours de la procédure.

### *C. LA PNIJ : UN SUCCÈS INDÉNIABLE, ENTRAVÉ PAR DES « ANGLES MORTS »*

Malgré ses débuts chaotiques et une mise en service qui aura duré près de dix ans, **la PNIJ est aujourd'hui un outil ergonomique et performant, qui donne pleine satisfaction à ses utilisateurs**. Certains des représentants des services de police et de gendarmerie rencontrés par les rapporteurs ont même décrit la plateforme comme l'un des seuls outils dont ils disposent à fonctionner de manière fluide et à faire l'objet d'améliorations techniques régulières visant à tenir compte de leurs besoins et de leurs attentes.

---

[1] *Les rapporteurs ont constaté lors de leurs déplacements que, si le coût induit par les réquisitions apparaissait sur le poste informatique des enquêteurs (à la fois pendant la « commande », pour chaque prestation, et sous forme récapitulative en fin d'opération), aucune indication financière n'est visible sur l'interface informatique utilisée par les magistrats du parquet.*

Toutefois, **la plateforme présente des « angles morts »** qui soit nuisent à son efficacité dans le cadre des enquêtes, soit soulèvent des questions quant à la bonne protection des données personnelles sensibles que sont les données de connexion.

### 1. Un périmètre techniquement limité

La PNIJ présente tout d'abord, par nature, des limites périmétriques.

Pour certaines, **ces limites ne sont pas l'apanage de la plateforme** : elles découlent de l'intervention sur le marché français d'opérateurs auxquels la loi nationale apparaît *de facto* difficilement opposable, soit pour des raisons juridiques (donc pour les opérateurs extra-communautaires et ne disposant pas de représentation légale en France), soit pour des raisons techniques.

En effet, **le raccordement à la PNIJ d'une vingtaine d'opérateurs est à rapprocher du nombre total d'opérateurs sur le territoire français, estimé par ANTENJ à 1 800.** Si le raccordement des OCE dits « historiques » permet, *via* les installations physiques de ces derniers, de collecter une partie des données gérées par des acteurs tiers, ces chiffres attestent d'un bouleversement technique et économique : la dérégulation du secteur des communications électroniques complexifie la centralisation des accès aux données de connexion et, plus largement, rend illusoire la perspective d'une gestion exhaustive de ces données à l'échelle nationale. À cet égard, et en dépit de son apport majeur dans la téléphonie traditionnelle, il convient de rappeler que **la PNIJ ne couvre ni les fournisseurs d'accès à internet, ni les opérateurs non-traditionnels** comme les opérateurs satellitaires ou les opérateurs *over-the-top* (OTT) qui opèrent par « contournement » du réseau.

De la même manière, la PNIJ ne peut par nature toucher que des acteurs disposant d'une existence légale en France, obligeant les services d'enquête à faire des réquisitions *ad hoc* pour solliciter les opérateurs ou les fournisseurs qui ne répondent pas à ce critère. Or, si elles sont théoriquement soumises aux dispositions nationales applicables aux autres opérateurs dès lors qu'elles interviennent en France, les entités étrangères peuvent en pratique échapper aux sanctions en cas de non-respect des obligations fixées par le droit français ; ainsi, **certains acteurs (et notamment les principaux OTT américains, à savoir Google et Meta pour Facebook et WhatsApp) refusent de déférer aux réquisitions qui leur sont adressées par les services d'enquête français** et vont parfois, selon les informations recueillies par les rapporteurs, jusqu'à opérer un véritable contrôle de l'opportunité de la demande sur le fond. Ainsi, et comme l'a résumé ANTENJ auprès des rapporteurs, « *la question relève aujourd'hui davantage de l'effectivité des obligations faites aux opérateurs, notamment extra-européens, que de la production de nouvelles normes* ».

D'autres difficultés affectent spécifiquement la PNIJ ; elles tiennent au degré de coopération des opérateurs de téléphonie.

En effet, les quatre opérateurs dits « historiques » (Bouygues, Free, Orange et SFR) semblent avoir adopté des **pratiques hétérogènes et ne pas accorder la même portée à l'obligation de conservation fixée par la loi.** Des différences d'interprétation existent ainsi quant au sort des données de localisation prises en compte par le réseau hors de toute communication : si deux opérateurs sur quatre les rendent accessibles aux services d'enquête pendant un an, un autre ne le prévoit que pour 90 jours ; le quatrième en a exclu la possibilité.

Pour le bon fonctionnement de la PNIJ et, surtout, pour la bonne marche des enquêtes et la pleine application de la loi, **il paraît essentiel aux rapporteurs qu'une harmonisation soit effectuée, sous l'égide du CCED, quant à la nature des données de localisation devant être conservées par les OCE.**

> **<u>Proposition n° 1 :</u> Lever toute ambiguïté quant à la nature des données devant être conservées par les opérateurs.**

### 2. Des usages extérieurs ou parallèles à la PNIJ qui soulèvent des interrogations

La deuxième série de limites tient à la **rémanence de réquisitions « hors-PNIJ »,** en contrariété avec le principe posé depuis 2016 par l'article 230-45 du code de procédure pénale selon lequel « *Sauf impossibilité technique, les réquisitions et demandes adressées [aux OCE] sont transmises par l'intermédiaire de la plate-forme nationale des interceptions judiciaires qui organise la centralisation de leur exécution* ». Lors de leurs auditions et déplacements, les rapporteurs ont constaté que **des accès aux données de connexion en dehors de la plateforme continuaient à se produire, y compris dans des cas qui ne semblent pas répondre à une impossibilité technique.** Il peut ainsi arriver que des enquêteurs sollicitent directement les OCE, comme en témoigne le fait que la Fédération française des télécoms (FFT, qui représente notamment Bouygues, Orange et SFR) ait indiqué que « *Les opérateurs regrettent qu'une petite partie des réquisitions judiciaires leur arrivent encore directement par courrier, courriel ou fax* ».

Certes, et comme le relève ANTENJ, « *des enquêteurs ont recours à une solution d'interception hors-PNIJ [qui semble être distribuée par une entreprise privée, Elektron] dotée de fonctionnalités qui, jusqu'à récemment, n'étaient pas présentes sur la PNIJ (accès en mobilité, analyse des flux interne chiffrés, notamment), ou parce que certains opérateurs ne peuvent être interceptés sur la PNIJ, notamment outre-mer* ». **De tels accès représentent, toujours selon ANTENJ, 20 à 25 % des interceptions**.

**Les éléments recueillis par les rapporteurs laissent à penser que, dans certains services, le nombre de recours à des solutions d'interceptions tierces (donc au « hors-PNIJ ») est anormalement élevé. Cette situation est particulièrement préoccupante : on ne saurait exclure que de tels accès soient motivés par la volonté d'échapper aux garanties imposées par la PNIJ en termes de traçabilité.**

La troisième limite concerne **l'exploitation et le retraitement des données (nombreuses, hétérogènes et parfois livrées sous une forme « brute ») issues de la plateforme**.

Si ANTENJ œuvre à la conception de « modules » visant à doter la PNIJ de nouvelles fonctions et à rapprocher son fonctionnement des besoins des utilisateurs, comme en témoigne le déploiement récent d'une possibilité de visualisation graphique de l'évolution dans le temps des données de localisation d'un utilisateur, la plateforme n'est pas autosuffisante et, **pour faire face à la masse de données obtenues en réponse à certaines réquisitions, les OPJ utilisent des logiciels de rapprochement judiciaire.** Ceux-ci sont notamment employés pour l'analyse des données issues de la téléphonie, qui parviennent aux enquêteurs sous une forme « brute », peu lisible et qui en conséquence n'est pas directement exploitable ; ils permettent également, pour des affaires complexes nécessitant une analyse criminelle, de « croiser » ces données avec d'autres éléments de l'enquête (contenu des auditions, preuves saisies en perquisition, preuves techniques et scientifiques…).

C'est ainsi le logiciel MERCURE qui équipe tant la police que la gendarmerie pour le traitement des données de téléphonie. En sus, selon les indications transmises aux rapporteurs, la gendarmerie nationale utilise trois logiciels[1], dont deux sont « *essentiellement* » tournés vers le traitement des données de connexion : une application de traitement des relations transactionnelles (ATRT), faisant partie de l'outil plus large ANACRIM, et le logiciel *DeveryAnalytics - Telephony Data* (DA-TD). Ces outils permettent l'import et le « nettoyage » des données (y compris, voire « *essentiellement* » pour DA-TD et ATRT, celles issues de la PNIJ), puis leur exploitation.

[1] *Le troisième logiciel,* Analyst's Notebook *(ANB, qui constitue l'autre versant du logiciel ANACRIM), qui va au-delà des données de connexion puisqu'il met en relation l'ensemble des éléments d'enquête (son usage est, par voie de conséquence, réservé aux OPJ ayant suivi une formation à l'analyse criminelle et réservé aux affaires criminelles les plus complexes) est utilisé par le service central du renseignement criminel : il est donc commun à la police et à la gendarmerie.*

**Le régime juridique des logiciels de rapprochement judiciaire**

Introduits dans le code de procédure pénale par la loi n° 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) du 14 mars 2011, **les logiciels de rapprochement judiciaire ont pour principale vocation d'aider les forces de sécurité intérieure à lutter contre des infractions sérielles de petite à moyenne gravité**[1].

Par une réserve d'interprétation, le Conseil constitutionnel a précisé dans sa décision n° 2011-625 DC que **ces logiciels n'avaient « *pas pour objet et ne sauraient avoir pour effet de permettre la mise en œuvre d'un traitement général des données recueillies* *à l'occasion des diverses enquêtes mentionnées [par le code]* »** et qu'ils ne pourraient « *conduire qu'à la mise en œuvre, autorisée par ces autorités judiciaires, de traitements de données à caractère personnel particuliers, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations* » (considérant 71).

Ces logiciels répondent au cadre général, défini par les articles 230-20 à 230-27 et R. 40-39 à R. 40-41 du code de procédure pénale, qui fixe divers garde-fous pour encadrer l'utilisation de ces logiciels. Ainsi :

– seuls les enquêteurs de police, de la gendarmerie et du **SEJF individuellement désignés et spécialement habilités** par leur supérieur hiérarchique peuvent utiliser ces logiciels (article 230-25). L'usage de tels logiciels dans le cadre d'une enquête administrative est expressément exclu par la loi (article 230-26) ;

**– les données exploitées ne peuvent provenir que des pièces et documents de procédure judiciaire déjà détenus par les services d'enquête** (article 230-21) et leur nature doit être définie dans l'habilitation de l'enquêteur (article 230-25) ;

**– les données relatives à l'identité d'une personne font l'objet d'une protection spécifique** : elles ne peuvent apparaître aux enquêteurs qu'à la fin des opérations de rapprochement et en cas de rapprochement positif. En d'autres termes, ce n'est qu'une fois qu'un lien direct (et non fortuit) est établi entre une personne et une infraction que l'identité de celle-ci peut être recherchée. Ces mêmes données sont **effacées à la clôture de l'enquête** ou, au plus tard, à l'expiration d'un délai de trois ans (article 230-22).

L'usage de ces logiciels est, par ailleurs, triplement contrôlé :

**– en amont de leur utilisation, les logiciels doivent être autorisés par décret en Conseil d'État pris après avis de la Cnil** ; le décret précise notamment « *les infractions concernées, les modalités d'alimentation du logiciel, les conditions d'habilitation des enquêteurs et les modalités selon lesquelles les personnes intéressées peuvent exercer leur droit d'accès* » (article 230-27) – étant relevé que, selon la Cnil, l'exercice du droit d'accès n'est pas garanti en pratique par les principaux logiciels utilisés par la police et par la gendarmerie[2] ;

---

[1] *Selon l'article 230-20 du code de procédure pénale, ils visent en effet à «* faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs […] [et] à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires *». Le propos du présent rapport ne concerne qu'indirectement les logiciels de rapprochement aux fins d'analyse criminelle, réservés à des enquêteurs spécifiquement formés et aux affaires les plus complexes (« cold cases », meurtres et viols sériels, disparitions inexpliquées…) dont le champ est large et qui visent à traiter de nombreuses informations qui ne sont pas des données de connexion.*

[2] *Délibération de la Cnil 2011-418 du 15 décembre 2011, accessible sous le lien suivant :*

**– leur usage général est soumis au contrôle de la Cnil**, au titre de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, **ainsi que du procureur de la République et d'un magistrat hors hiérarchie** chargé de contrôler la mise en œuvre de ces logiciels et désigné à cet effet pour trois ans par le ministre de la justice auquel il remet un rapport annuel (article R. 40-41). Le procureur de la République et le magistrat chargé du contrôle disposent tous deux d'un accès direct aux logiciels (articles 230-33 et 230-34) ;

– enfin, **l'usage au cas par cas des mêmes logiciels est autorisé par le magistrat saisi de l'enquête ou chargé de l'instruction** ; en cas de flagrance, l'autorisation est réputée acquise, sauf décision contraire du procureur. Cette autorisation **fait l'objet d'une mention en procédure**, et l'exploitation des données donne lieu à un rapport joint à la procédure à la clôture de l'enquête, le magistrat compétent pouvant par ailleurs obtenir communication de l'ensemble des données et informations exploitées (article R. 40-40)

À l'occasion de l'examen du décret n° 2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle, **le ministère de l'intérieur a adressé à la Cnil un dossier de présentation de deux logiciels** : ANACRIM-ATRT (ANAlyse CRIMinelle-Application de Traitement des Relations Transactionnelles, qui permet l'exploitation de relevés bancaires et de données téléphoniques, notamment les fadettes, afin d'effectuer des recherches, des tris et des recoupements) et ANACRIM-ANB (*Analyst's NoteBook*, qui était mis en œuvre par la gendarmerie nationale avant même la demande d'avis et qui constitue un outil d'analyse et de représentation visuelle des données permettant, entre autres, de représenter des données sous forme de graphiques relationnels ou évènementiels pour imager des relations entre individus ou des enchaînements chronologiques).

*Source : commission des lois du Sénat*

Conforme au code de procédure pénale, l'usage de ces outils fait cependant naître des interrogations. **On peut tout d'abord s'interroger sur l'impact d'un retraitement qui, parce que sa vocation même est de concerner une masse conséquente de données** (à tout le moins, une quantité de données telle qu'elle ne peut que difficilement être analysée dans un délai raisonnable par un être humain) **et d'opérer entre celles-ci des rapprochements automatisés, remet en cause l'idée selon laquelle l'accès aux données de connexion ne porte qu'une atteinte limitée à la vie privée.** Loin de l'idée répandue selon laquelle les données de connexion constitueraient un « lac » d'informations, c'est-à-dire un ensemble inerte dans lequel les services d'enquête ne pourraient trouver que des indications éparses et partielles, la mise en relation des métadonnées s'inscrit dans un processus dynamique qui met à mal la distinction traditionnelle entre le « contenu » et le « contenant ». Plus encore, parce que le traitement des données de connexion s'apparente à une forme de sérendipité, **il remet en cause l'idée même d'une corrélation entre le degré d'atteinte à la vie privée et l'importance des « garde-fous » prévus par le droit** : comment, en effet, adapter le contrôle à la nature de ce qu'on recherche lorsqu'on ignore *ab initio* ce qu'on peut découvrir ?

On peut, ensuite, relever que **les modalités de fonctionnement de ces logiciels diffèrent, et sur des points qui ne sont pas anecdotiques, de celles fixées pour la PNIJ et qui constituent autant de garanties de la régularité des accès**. Ainsi, aucune mesure particulière n'est prévue pour assurer la traçabilité des actions effectuées, rendant *de facto* impossible une supervision par le magistrat (procureur de la République ou juge d'instruction) compétent pour diriger l'enquête ou par le magistrat en charge du contrôle du bon usage des logiciels[1]. Plus largement, **aucune obligation d'authentification de l'utilisateur n'est posée par le code**, ce qui constitue potentiellement une faille majeure de sécurité[2]. De même, l'exigence d'habilitation au niveau « secret » des personnels et prestataires appelés à intervenir sur la PNIJ n'est pas reproduite pour les logiciels de rapprochement judiciaire, ce qui paraît à tout le moins étonnant.

**Certaines des personnes auditionnées par les rapporteurs se sont inquiétées d'une autre source, cette fois économique, de vulnérabilité.** Ockham Solutions, société éditrice du logiciel MERCURE, a en effet été récemment rachetée par un acteur majeur dans le domaine de l'appui technique aux interceptions de sécurité, Chapsvision ; ce groupe français avait déjà acquis, en janvier 2022, l'entreprise Elektron puis, en septembre de la même année, la société Deveryware, qui interviennent toutes deux en matière d'appui technique aux interceptions de sécurité mais aussi, pour Deveryware, pour l'édition des logiciels de rapprochement judiciaire de la gendarmerie.

Si les rapporteurs se réjouissent de l'émergence d'un acteur souverain dans le traitement des données à des fins régaliennes, ils relèvent que **cette concentration peut emporter des conséquences techniques dommageables**, en particulier s'agissant de l'impact d'une éventuelle captation des données ainsi collectées par des tiers malveillants voire de la possibilité d'un mésusage « interne ». Ils invitent le Gouvernement à **prendre ces risques au sérieux et à faire sans délai l'étude des facteurs de vulnérabilité qu'ils génèrent comme des solutions qui peuvent être déployées** pour assurer l'absolue sécurité des données personnelles ainsi rassemblées.

---

[1] *Pour la PNIJ, cette traçabilité résulte de l'article R. 40-50, qui dispose que* « Toute opération relative au traitement fait l'objet d'un enregistrement comprenant l'identification de l'utilisateur, la date, l'heure et la nature de l'action. Ces informations sont conservées pendant une durée de trois ans ».

[2] *Là encore, c'est le code de procédure pénale qui pose cette exigence pour la PNIJ (article R. 40-45).*

# DEUXIÈME PARTIE
# DES DROITS NATIONAUX BOULEVERSÉS PAR LA JURISPRUDENCE DE LA CJUE

Largement utilisées par les services d'enquête et essentielles à la manifestation de la vérité, les données de connexion restent, comme on l'a vu, des données sensibles : leur conservation et leur exploitation soulèvent donc des interrogations quant au juste point d'équilibre entre la préservation de la vie privée et la nécessaire lutte contre les infractions pénales.

C'est dans ce débat qu'est intervenue, dès 2014, la Cour de justice de l'Union européenne en **posant l'exigence d'une protection maximale des données personnelles –** exigence qui, en retour, a généré des perturbations dans de nombreux États membres et qui suscite aujourd'hui des inquiétudes dans tous les services d'enquête européens, comme en atteste la déclaration de Lisbonne déjà citée.

## I. UN RECOURS AUX DONNÉES DE CONNEXION PROFONDÉMENT DESTABILISÉ PAR LA JURISPRUDENCE DE LA CJUE

### *A. UN ENCADREMENT SCRUPULEUX DU RECOURS AUX DONNÉES DE CONNEXION*

L'utilisation massive faite par les services de police et de gendarmerie des données de connexion à des fins d'élucidation et de résolution des enquêtes a été profondément déstabilisée par la position qu'a adoptée la Cour de justice de l'Union européenne (CJUE) quant à sa conformité aux textes de droit communautaire protégeant le droit à la vie privée (en particulier la directive 2002/58/CE du 12 juillet 2002, dite « vie privée et communications électroniques » ou « *e-privacy* »).

Progressivement construite à partir de l'arrêt *Digital Rights Ireland Ltd* du 8 avril 2014, et surtout des arrêts *Tele2 Sverige* AB du 21 décembre 2016 et *La Quadrature du Net et autres* du 6 octobre 2020, cette jurisprudence part du principe, réaffirmé maintes fois depuis par la Cour, **qu'une conservation généralisée et indifférenciée des données de connexion**, par le volume et le détail des informations qu'elle permet de connaître sur la vie de tout citoyen, **porte au droit au respect à la vie privée et à la protection des données personnelles une atteinte massive, qui ne peut par conséquent être admise que pour des motifs et dans des hypothèses très circonscrits**.

Il convient à cet égard de distinguer la conservation des données, d'une part, et l'accès à ces données, d'autre part.

Sur le premier point, la Cour juge en substance que **seule la sauvegarde de la sécurité nationale est susceptible de justifier une obligation généralisée et indifférenciée de conservation des données de connexion** de trafic et de localisation, considérées comme les plus sensibles. L'existence et la gravité de cette menace doivent pouvoir être constatées par un juge ou une autorité administrative indépendante.

**Une telle obligation ne peut en revanche pas être imposée en matière de lutte contre la criminalité grave et la prévention des menaces graves pour la sécurité publique.** Pour ces finalités, la Cour n'admet que la possibilité, soit d'une **conservation ciblée** sur un groupe de personnes ou un lieu déterminé, soit d'une **conservation dite « rapide »**, afin de permettre de prévenir ou de réprimer une infraction déterminée.

Enfin, en dehors de ces deux motifs – sauvegarde de la sécurité nationale et lutte contre la criminalité grave –, **aucune obligation de conservation de données de trafic et de localisation ne saurait être imposée par les États membres aux opérateurs pour des motifs liés à la lutte contre la criminalité « ordinaire »**.

À l'inverse, la Cour admet la possibilité d'une **conservation générale et indifférenciée des données d'identification**, quel qu'en soit le motif (donc à la fois pour la lutte contre la criminalité « ordinaire », contre la criminalité grave et pour prévenir les menaces graves contre la sécurité publique), puisqu'elle constitue une certes une ingérence, mais de portée réduite.

S'agissant, en second lieu, des conditions dans lesquelles les services de sécurité sont susceptibles d'accéder aux données ainsi conservées, la Cour juge **qu'un tel accès doit être obligatoirement soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante** (arrêt de grande chambre *H.K./Prokuratuur* du 2 mars 2021). En cas d'urgence, le contrôle peut intervenir *a posteriori*, mais à bref délai. En outre, il ne leur est possible d'accéder aux données **que pour le motif pour lequel elles ont été conservées** et, en tout état de cause, il leur est interdit d'accéder aux données de trafic et de localisation pour la recherche d'infractions « non graves ». Enfin, les personnes dont les données ont été ainsi consultées doivent en être informées.

Cette position est particulièrement stricte puisqu'elle **pose le principe que, par nature, les données de connexion permettent de tirer des conclusions très précises sur la vie privée des personnes concernées, si bien que tout accès à ces données constitue une ingérence grave** et que, pour « prendre le mal à la racine », il y a lieu de restreindre autant que possible la conservation des mêmes données. Pour illustrer la rigueur de la jurisprudence de la Cour, on rappellera que les faits à l'origine du procès pénal en droit national dans l'affaire précitée *H.K./Prokuratuur* portaient sur trois accès d'une durée respective d'une journée, d'un mois et de onze mois ; or tous ont fait l'objet de la même censure, alors que l'on peut émettre des

doutes légitimes sur la possibilité de connaître, pour reprendre les termes de la Cour, les « *habitudes de la vie quotidienne, les lieux de séjours permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales [des] personnes et les milieux sociaux fréquentés par celles-ci* » avec un accès limité à une seule journée.

Il convient de relever, par ailleurs, que **la position de la CJUE diffère sensiblement de celle de la Cour européenne des droits de l'homme** qui, si elle considère également la conservation de données de connexion comme une ingérence dans le droit de toute personne au respect de sa vie privée, protégé par l'article 8 de la Convention européenne des droits de l'homme, s'attache pour sa part, dans le cadre de son contrôle *in concreto*, à examiner la légalité, la légitimité et la nécessité de la réglementation en cause ainsi que les garanties dont elle est assortie[1].

Ces décisions ont provoqué un véritable **effet de sidération** dans les services d'enquête et les parquets, car non seulement elles paraissent condamner le recours aux données de connexion pour une frange très large d'infractions, notamment celles liées à la « délinquance du quotidien » pour lesquelles elles constituent un élément de preuve essentiel, mais, en outre, en posant l'exigence d'un contrôle préalable indépendant sur toute réquisition de ce type, elles portent un risque d'alourdissement et de ralentissement des enquêtes.

Sans doute cette jurisprudence de la Cour de justice n'est-elle pas encore entièrement stabilisée. La Cour est notamment appelée à se prononcer prochainement sur le droit de l'ex-Hadopi (désormais ARCOM) d'obtenir auprès des fournisseurs d'accès à Internet les données d'identité civile correspondant à une adresse IP, afin de lutter contre la reproduction et la diffusion illégale d'œuvres protégées par les droits d'auteurs, sans contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant. À cette occasion, la Cour aura notamment à se prononcer sur la possibilité ouverte, ou non, aux États-membres de prévoir une conservation généralisée et indifférenciée des adresses IP afin de permettre la prévention et la répression d'infractions pénales en ligne **lorsque l'adresse IP constitue le seul moyen d'investigation permettant d'identifier les personnes**. La Cour devra également dire si la notion de « criminalité grave » relève du droit de l'Union européenne ou si sa définition incombe à chaque État-membre, en fonction de ses traditions et de son contexte national.

Néanmoins, le nombre de décisions rendues à ce jour par la Cour de justice et la solennité de la formation qui les a rendues (la grande chambre) rendent peu probable, à court terme, un infléchissement net de sa position, au-delà de quelques aménagements ponctuels.

---

[1] *CEDH, 25 mai 2021,* Big Brother Watch et autres c. Royaume-Uni*, n° 58170/13, 62322/14 et 24960/15 ; la position de la CEDH est plus abondamment commentée ci-après, dans un encadré « Les garanties de bout en bout ».*

### *B. UNE JURISPRUDENCE À L'ASSISE CONTESTABLE*

**Les arrêts de la Cour ont fait l'objet de commentaires abondants de la doctrine et des juridictions nationales** au vu :

– en premier lieu, de leur fondement juridique ;

– en deuxième lieu, de l'immixtion qu'ils peuvent impliquer dans une compétence qui est celle des États ;

- en dernier lieu, de la philosophie qui sous-tend les positions des juges de Luxembourg.

S'agissant du premier point, l'un des éléments saillants de la jurisprudence de la CJUE est qu'elle **se fonde sur la Charte des droits fondamentaux de l'Union européenne, et plus particulièrement sur ses articles 7, 8 et 11** qui protègent respectivement le droit au respect de la vie privée et familiale, les données à caractère personnel et la liberté d'expression. En d'autres termes, à l'inverse d'une écrasante majorité de décisions dans lesquelles la Cour apprécie la conformité d'une règle nationale à un texte de droit dérivé, **elle examine en matière de données de connexion le bon respect de la Charte par des textes dont l'origine est indifféremment européenne ou nationale**.

Plus encore, et comme l'observait le rapporteur public Alexandre Lallet dans ses conclusions sur la décision du Conseil d'État *French data network* de 2021 (voir ci-après), les exigences issues de la Charte sont interprétées par la Cour comme des impératifs absolus, qu'elle ne juge pas devoir concilier avec d'autres impératifs de même niveau comme le ferait le Conseil constitutionnel français ou comme le fait la CEDH : il souligne ainsi que la Cour « *ne s'embarrasse pas d'une analyse des garanties pourtant sérieuses dont [la] conservation [des données de connexion] doit être entourée* » et que, tout en admettant l'importance des objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, elle les estime dérogatoires aux principes de la Charte et en promeut une interprétation stricte qui offre un contraste singulier avec la portée prétorienne qu'elle a souhaité accorder à la protection des données personnelles[1].

Sur le second sujet, **un nombre conséquent de juristes s'est interrogé sur la signification et la pertinence d'une jurisprudence qui semble aller au-delà du périmètre des compétences confiées à l'Union par les traités et toucher au cœur d'une prérogative nationale**, à savoir la sécurité publique et la sûreté de l'État. Certes, la directive « vie privée et communications électroniques » de 2002 est susceptible d'avoir un impact sur la conservation des métadonnées en raison du **régime de conservation choisi par les autorités publiques** : parce que cette conservation est confiée aux opérateurs, et donc à des acteurs économiques privés, elle relève au

[1] *Le texte des conclusions précitées est consultable sur le site du Conseil d'État.*

moins pour partie du marché intérieur[1] ce qui peut, sans épuiser le sujet, expliquer l'intervention en la matière de la CJUE. Pour autant, **ses décisions marquent un véritable renversement puisque la même directive excluait d'elle-même son application dans le domaine régalien** : son article 1er, paragraphe 3, dispose ainsi que « *la présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal* »[2].

Certains auteurs ont, dès lors, évoqué un « *glissement jurisprudentiel* » constituant une « *expansion des compétences de l'Union* »[3] et se sont interrogés sur « *la légitimité du juge européen à fixer unilatéralement une répartition des compétences entre l'Union et ses États membres* »[4]. Ces questionnements sont partagés par les cours suprêmes françaises, comme en témoignent les conclusions précitées d'Alexandre Lallet qui consacrent de longs développements à la **possibilité d'invoquer l'identité constitutionnelle de la France pour rejeter l'application de la jurisprudence européenne** : si cette idée a été finalement écartée par le Conseil d'État dans sa décision, le simple fait qu'elle ait été mise sur la table est loin d'être anodin et constitue de toute évidence un message envoyé aux juges de Luxembourg.

La troisième question porte sur la philosophie sous-jacente aux décisions de la Cour et sur les objectifs qu'elle a entendu poursuivre en limitant drastiquement les possibilités d'action des États dans un domaine où l'intérêt intégratif d'une harmonisation totale à l'échelle de l'Union n'apparaît pas avec clarté.

Certaines des personnes auditionnées par les rapporteurs ont estimé que ses arrêts, bien qu'applicables sans distinction, visaient certains États et faisaient écho aux craintes qui voient le jour face à la montée des démocraties illibérales à l'est de l'Europe. D'autres y ont vu, cumulativement ou alternativement avec ce qui précède, la marque d'une « *logique de méfiance à l'égard des autorités publiques, qu'il faut se garder de soumettre à la tentation, à défaut de les délivrer d'un mal qui sommeille en chacune d'elles : c'est le spectre de la surveillance de masse et de l'intrusion permanente dans la 'vie des autres', dont l'histoire a livré des manifestations durablement traumatisantes dans une partie au moins de l'Europe* »[5].

---

[1] *Ce qui pose la question, à titre subsidiaire, d'un sort juridique d'une conservation qui serait assurée directement par les États.*

[2] *Le texte de la directive est consultatble sur le site suivant : https://eur-lex.europa.eu.*

[3] *François-Xavier Millet, « Le glissement jurisprudentiel en matière de données de connexion : l'expansion des compétences de l'Union et sa réception dans les États membres », RFDA 2023, p. 606.*

[4] *Brunessen Bertrand, « La Cour de justice et les données de connexion : vers un* European Data Network *? », RFDA 2023, p. 615.*

[5] *Conclusions précitées d'Alexandre Lallet.*

Sans pouvoir trancher ce débat, les rapporteurs s'étonnent du paradoxe qui consiste à restreindre avec autant de force l'accès des autorités publiques aux métadonnées pour lutter contre la criminalité, tout en laissant de vastes marges de manœuvres aux acteurs privés pour traiter les mêmes données à des fins purement commerciales, notamment par le biais d'un profilage dont l'existence même suppose une connaissance fine de la vie privée des utilisateurs.

## II. DES INQUIÉTUDES PROFONDES QUI REJAILLISSENT SUR L'UNION EUROPÉENNE

### *A. EN EUROPE, DES ÉTATS DÉBOUSSOLÉS*

La France n'a pas été le seul État à voir son droit interne bouleversé par les arrêts de la Cour de justice de l'Union européenne : **une quinzaine[1] d'États membres se sont engagés dans une mise en conformité, totale ou partielle, de leurs régimes de conservation des données de connexion et d'accès à celles-ci**, avec parfois des conséquences importantes sur la capacité d'élucidation des infractions pour les services d'enquête. Cela étant, aucun pays ne semble faire preuve d'un enthousiasme particulier face aux arrêts de la CJUE et, si la plupart des États ne font pas mystère des difficultés qu'ils rencontrent dans l'application de la jurisprudence, les autres (à l'exception notable de l'Allemagne) se partagent entre indifférence et résignation. Tous subissent, en revanche, un **sentiment identique de « flottement » créé par l'effet conjugué du nombre substantiel de questions préjudicielles posées à la Cour sur le sujet des données de connexion (une vingtaine depuis 2014) et par l'absence d'engagement par la Commission européenne de recours en manquement**, même envers les États dont la législation est en contradiction manifeste avec les arrêts rendus par la Cour de Luxembourg.

L'approche quantitative n'épuise pas le sujet puisque, comme l'ont relevé plusieurs personnalités rencontrées par les rapporteurs, **l'impact concret, dans chaque État, des limites posées par la Cour en matière de données de connexion est extrêmement difficile à mesurer.** Il varie ainsi en fonction, d'une part, des autres outils dont disposent les États dans leur arsenal probatoire et dont l'utilisation renforcée peut « compenser » un moindre accès aux données de connexion (lecteurs automatiques de plaques d'immatriculation, système de vidéo-protection, *etc.*) et, d'autre part, du « seuil de judiciarisation » des affaires et de la frontière entre l'action des services de police judiciaire et celle des services de renseignement. Il apparaît ainsi que, chez certains de nos voisins européens, la limitation massive des possibilités de recours aux métadonnées dans un cadre pénal

[1] *Selon le Secrétariat général pour les affaires européennes (SGAE), outre la France, douze États-membres appliquent encore aujourd'hui un principe de conservation généralisée des données, soit parce qu'ils refusent de se mettre en conformité avec la jurisprudence de la CJUE, soit parce qu'ils n'ont pas été directement visés par celle-ci.*

s'est **traduite par un développement des enquêtes administratives** ou par un recours croissant à des outils plus intrusifs encore, comme les interceptions téléphoniques.

Par ailleurs, **la situation d'un même État peut faire l'objet d'analyses profondément divergentes d'un interlocuteur à l'autre, à l'instar de l'Allemagne** : alors que la direction des libertés publiques et des affaires juridiques (DLPAJ) du ministère de l'intérieur juge que les enquêteurs allemands ne peuvent plus mener à bien certaines enquêtes d'envergure, faute de disposer du matériau précieux que sont les données de connexion et de localisation, particulièrement en ce qui concerne le crime organisé ou les crimes en série, l'association *European digital rights* (EDRi) l'a au contraire présentée comme un exemple à suivre puisqu'elle aurait pu se dispenser de toute obligation légale de conservation des métadonnées sans, pour autant, dégrader la qualité de sa réponse pénale.

Sans compter les États qui ont, à ce stade, fait le choix de **maintenir inchangées leurs normes internes (comme la Pologne, la Lituanie et la Lettonie**), on peut répartir les pays européens en trois groupes principaux :

– ceux qui ont fait le choix de renoncer à toute conservation des métadonnées à des fins pénales (voire, pour certains, de renoncer à la conservation quelle qu'en soit la finalité) ;

– ceux qui ont tenté de mettre en œuvre des régimes de conservation ciblée ;

– enfin, ceux qui (comme la France) essaient de trouver des voies de compromis en instaurant des systèmes proportionnés, dont la compatibilité avec la jurisprudence de la CJUE reste toutefois à confirmer.

En tout état de cause, **aucune des initiatives mises en place dans les autres États membres ne semble de nature à surmonter la rigueur des arrêts de la Cour et à ménager, dans le même temps, un système donnant satisfaction aux services d'enquête**.

### 1. Le choix contraint d'un régime sans obligation légale de conservation des métadonnées, une impasse pour les autorités

**En Allemagne, aux Pays-Bas et en Slovaquie**, les régimes existants de conservation des données ont été rendus *ex abrupto* inapplicables par les juges nationaux au motif de leur non-conformité aux règles européennes. Les opérateurs ne sont donc plus soumis, à ce jour, à **aucune obligation légale de conservation des données de connexion,** les seules données encore conservées l'étant sur le fondement de considérations purement techniques ou commerciales.

Néanmoins, l'absence d'obligation de conservation ne semble qu'**un état de droit transitoire pour l'Allemagne et les Pays-Bas**.

*a) Le vide juridique créé par la sanction des régimes de conservation générale et indifférenciée des données*

Fondées sur des modèles relativement similaires, les lois néerlandaises de 2009 et slovaques de 2011 relatives aux données de connexion imposaient une obligation de conservation généralisée des données pour une durée de six à douze mois. Les deux régimes pâtissaient également d'un système de collecte des données peu encadré. Les autorités répressives pouvaient accéder à ces données sans contrôle préalable dans le cadre d'enquêtes sur une infraction pénale particulièrement grave, dans le cas slovaque, ou pour toute infraction passible d'une détention provisoire[1], dans le cas néerlandais. Dès 2015, ces régimes ont été **rendus inapplicables par le juge des référés du tribunal de La Haye[2] et par la Cour constitutionnelle slovaque[3]**, au motif notamment de la violation des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Le dispositif allemand de conservation des données[4] a, quelques années plus tard, subi un sort identique. Introduit en 2015, il semblait pourtant relativement exigeant, puisqu'il limitait la durée de conservation généralisée des métadonnées à **quatre semaines pour les données de localisation** et à **dix semaines pour les autres types de données**. La loi allemande imposait également un strict cahier des charges aux opérateurs afin de garantir une protection efficace des données. Enfin, la collecte de ces données était soumise au contrôle préalable d'un juge et limitée aux infractions particulièrement graves.

Cependant, le 22 juin 2017, quelques jours avant son entrée en vigueur, la Cour administrative d'appel de la Rhénanie du Nord-Westphalie rendait une ordonnance de référé dans laquelle elle déclarait le dispositif allemand de conservation des données contraire au droit de l'Union[5]. Le 28 juin suivant, dans l'attente d'une décision définitive sur cette affaire, l'Agence fédérale allemande des réseaux (*Bundesnetzagentur*), annonçait renoncer temporairement à prendre des mesures visant à faire respecter les règles de conservation des données. Le dispositif allemand était ainsi privé de tout effet contraignant et, en cela, de toute effectivité.

La ligne des juges allemands a, par la suite, été confirmée par la Cour de justice de l'Union européenne. Saisie d'une question préjudicielle sur ces mêmes affaires par le Tribunal administratif fédéral allemand,

---

[1] *Rentraient dans ce champ des infractions d'une gravité relative, comme le vol d'une bicyclette.*

[2] *Tribunal de La Haye, 11 mars 2015, C/09/480009 / KG A 14/1575.*

[3] *Cour constitutionnelle slovaque, 29 avril 2015, PL. ÚS 10/2014.*

[4] *Article 176 du Telekommunikationsgesetz (loi relative aux télécommunications).*

[5] *OVG Nordrhein-Westfalen, 22.06.2017 - 13 B 238/17 : le juge des référés de la Cour administrative d'appel de la Rhénanie du Nord-Westphalie décharge ainsi un petit fournisseur d'accès à Internet de Munich, SpaceNet, de l'obligation de conserver les données de trafic et de localisation de ses clients. Cette décision a été confirmée au fond par le tribunal administratif de Cologne, pour les entreprises SpaceNet et Deutsche Telekom (Verwaltungsgericht Köln, 20 avril 2018 - 9 K 7417/17 et 9 K 3859/16).*

la Cour a ainsi jugé **le dispositif allemand non conforme au droit de l'Union** au motif qu'il serait, indépendamment de la durée et des conditions d'accès, « *susceptible de permettre de tirer des conclusions très précises concernant la vie privée de la ou des personnes concernées* » (point 88)[1]. Par conséquent, et conformément à cette décision préjudicielle, les tribunaux nationaux et la *Bundesnetzagentur* ont définitivement écarté l'application des dispositions de la loi allemande sur la conservation des données[2].

D'effet immédiat, **ces décisions ont ainsi rendu inapplicable**, dans les pays étudiés, **toute obligation légale de conservation des données de connexion.** Seules les données conservées par les opérateurs pour répondre à leurs propres besoins techniques et commerciaux peuvent, dès lors, faire l'objet de réquisitions par les autorités répressives au titre de la lutte contre la criminalité grave. Aux Pays-Bas, 34 221 demandes ont été émises à ce titre en 2018[3].

Si cette transition a été faite sans modification législative en Allemagne et aux Pays-Bas, en Slovaquie le législateur a adopté, dès novembre 2015, une nouvelle loi qui acte la suppression de toute obligation légale de conservation généralisée des données de connexion. Elle prévoit, en compensation, la possibilité pour le juge de demander une conservation rapide des données. La réforme de 2015 a également conforté le contrôle du juge en matière d'accès aux données de connexion. L'autorisation préalable du juge est désormais systématique et les réquisitions de données ne peuvent s'exercer que pour les infractions pénales graves.

*b) Une volonté de réforme pour combler les fragilités créées par l'absence de régime légal de conservation des données*

**L'impact opérationnel d'un tel régime de conservation** et ses implications pour la résolution des enquêtes pénales ont suscité des interrogations dans les pays concernés.

L'ambassade de France en Slovaquie a ainsi indiqué aux rapporteurs que, **selon les services du ministère de la justice slovaque, le cadre législatif existant « *n'est pas suffisant pour une lutte efficace contre la criminalité grave* ».** Le poste diplomatique a rapporté, à ce titre, que de nombreuses enquêtes pénales échoueraient en raison de l'impossibilité de remonter aux communications passées des suspects, faute de conservation obligatoire des données de connexion. Le problème affecterait en particulier la majorité des enquêtes en matière de pédocriminalité.

---

[1] *CJUE, 20 septembre 2022, SpaceNet Ag et Telekom Deutschland GmbH (C-793/19, C-794/19).*

[2] *BVerwG, 14.08.2023 - 6 C 6.22 et 6 C 7.22. Notosn également le communiqué de la Bundesnetagentur d'août 2023, consultable à l'adresse suivante : https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/Ueberwachung_Auskunftsert/VDS_113aTKG/node.html*

[3] *Réponse n° 178 (2019-2020) aux questions du député Van der Graaf sur le message "Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark".*

Témoignant également de la fragilité d'un régime privé de toute obligation légale de conservation, **les gouvernements néerlandais et allemand se sont engagés dans une révision de leurs cadres juridiques.**

Aux Pays-Bas, **un projet de loi, soumis au Parlement dès 2016**, prévoyait un nouveau régime d'accès aux données de connexion, placé sous le contrôle du juge d'instruction[1]. Parce qu'elle préservait le régime de conservation générale et indifférenciée posé en 2009, cette position semblait difficile à maintenir à la suite de l'arrêt *Tele2 Sverige*[2]. Le ministre de la justice néerlandais a ainsi, en 2018, annoncé au Parlement son intention de modifier le projet de loi afin de limiter l'obligation de conservation aux seules données d'identification[3], tout en envisageant de réintroduire une obligation générale de conservation des données de trafic et de localisation « *si à l'avenir, par exemple dans le cadre des discussions au niveau européen, il s'avère qu'une [telle] obligation […] sous quelque forme que ce soit est compatible avec le droit européen* ». Ces derniers mots témoignent d'une forme de circonspection quant à l'idée qu'un modèle ne reposant sur aucune obligation légale de conservation puisse être maintenu à long terme.

**La question de l'exploitabilité d'un régime sans obligation légale de conservation tend également à diviser la coalition gouvernementale allemande**. Un avant-projet de loi a été annoncé par le ministre fédéral de la justice afin de mettre en place un dispositif fondé exclusivement sur la conservation rapide des données (*quick freeze*)[4]. Estimant que ce gel rapide « *peut être utilisé comme instrument d'accompagnement dans des applications spécifiques et fournir des résultats d'enquête importants, mais n'est pas un remplacement adéquat pour le stockage des adresses IP* », la ministre fédérale de l'intérieur soutient, de son côté, une approche qui prévoit à la fois une conservation généralisée des adresses IP et une conservation ciblée sur la base de critères géographiques[5].

**Loin de susciter l'adhésion des autorités des pays étudiés, l'absence d'obligation légale de conservation des métadonnées demeure donc controversée.** La tendance est ainsi moins à une expansion de ce modèle qu'à un réexamen des dispositifs de conservation différenciés selon les types de données.

---

[1] *Projet de loi n°34 537, déposé le 13 septembre 2016, modifiant la loi sur les télécommunications et du code de procédure pénale concernant la conservation des données traitées dans le cadre de la fourniture de services publics de télécommunications et de réseaux publics de télécommunication.*

[2] *CJUE, 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. (C-203/15 et C-698/15)*

[3] *Lettre du ministre de la Justice à la chambre des représentants du 26 mars 2018.*

[4] *Avant-projet du Ministère fédéral de la justice du 25 octobre 2022 pour l'introduction d'une ordonnance de conservation des données de trafic dans l'ordonnance de procédure pénale, avec motifs.*

[5] *Article d'Ingo Dachwitz et Andre Meister « Buschmann legt Alternative zur Vorratsdatenspeicherung vor », netzpolitik, 25 octobre 2022.*

### 2. L'adoption d'un système de conservation ciblée, un faux-semblant ?

Conformément à la jurisprudence de la CJUE[1], **un système mixte**, conciliant conservation ciblée des métadonnées dans le cadre de la lutte contre la criminalité grave et conservation généralisée à des fins plus spécifiques, a été récemment mis en place en Belgique et au Danemark.

Toutefois, l'application faite par ces États des exigences de la CJUE (avec, notamment, l'existence d'un certain nombre de contournements au principe du « ciblage ») conduit à s'**interroger sur la pertinence pratique des modèles existants de conservation ciblée.**

*a) Le système de conservation ciblée applicable en Belgique et au Danemark*

La Belgique et le Danemark ont tous deux adopté, en 2022, une nouvelle loi sur les métadonnées qui prévoit **la possibilité d'une conservation ciblée et d'un accès au « stock » ainsi constitué en cas d'infraction grave**. Ces évolutions normatives sont la conséquence, d'une part, de l'annulation de la loi alors en vigueur par la Cour constitutionnelle belge en 2021[2] et, d'autre part, de la prise en compte par le gouvernement danois de la non-conformité de la précédente loi nationale avec l'arrêt *Tele2 Sverige*[3].

Dans le cas belge, les données de connexion sont automatiquement conservées dans les **zones particulièrement exposées** à des menaces de crimes graves ou d'atteinte à la sécurité nationale (aéroports, gares, *etc.*), ainsi que dans les **arrondissements judiciaires sujets à un taux important de criminalité grave**[4].

Dans le cas danois, la conservation des données comprend des **« *zones critiques pour la sécurité* »** (palais royaux, ponts, gares, *etc.*), ainsi que les parties du territoire national où le **nombre réel d'infractions pénales graves ou le nombre de résidents condamnés pour de telles infractions** est supérieur à 1,5 fois la moyenne nationale.

En sus des critères géographiques, le système danois prévoit également une conservation ciblée **en fonction de catégories de personnes**. Elle est automatique pour les personnes condamnées pour des infractions graves, ainsi que pour les lignes de téléphone faisant l'objet d'une ordonnance d'interception.

---

[1] *CJUE, 5 avril 2022, Commissioner of An Garda Siochana (C-140/20), point 101.*

[2] *Cour constitutionnelle belge, 22 avril 2021, n°57/2021.*

[3] *CJUE, 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. (C-203/15 et C-698/15)*

[4] *Il s'agit en l'occurrence, en vertu de l'article 10 de la loi du 20 juillet 2022, des* « arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90 *ter*, §§ 2 à 4, du cCode d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours ».

**Ce dispositif de conservation automatique des données est assorti d'une procédure de conservation rapide « à la demande »**. En Belgique, l'injonction de conservation rapide est émise par le ministère public pour une durée de conservation de six mois au maximum. Au Danemark, il revient au tribunal d'enjoindre aux opérateurs ce gel rapide des données, pour une durée de conservation d'un an. Dans ce cadre, la portée du ciblage est réduite à l'échelle d'une affaire, qui doit concerner une infraction passible d'une peine d'emprisonnement d'un an ou plus, dans le cas belge, ou de trois ou plus, dans le cas danois.

Le dispositif de conservation ciblée des données s'appuie également sur une **procédure d'accès fortement encadrée** au Danemark. La demande des autorités d'enquête est soumise à l'autorisation du tribunal et ne peut concerner qu'une personne soupçonnée d'avoir commis une infraction grave, c'est-à-dire passible d'une peine d'emprisonnement de trois ans ou plus. Une procédure de contrôle préalable est également prévue, en Belgique, pour collecter les données de trafic et de localisation. Ces dernières ne sont ainsi accessibles qu'après autorisation du juge d'instruction et pour les seules infractions de nature à entraîner une peine d'emprisonnement d'un an ou plus. Les données d'identification peuvent, en revanche, être requises pour toute infraction et sans contrôle.

*b) Un ciblage contourné*

La réalité du caractère ciblé de la conservation peut, toutefois, être doublement nuancée : en effet, non seulement la Belgique et le Danemark sont tous deux régis par **un système mixte, combinant une conservation généralisée et une conservation ciblée des données selon le type de données ou la nature de l'infraction, mais surtout la définition du « ciblage » s'avère particulièrement large**, permettant *de facto* de soumettre une part substantielle des territoires et des populations à une obligation légale de conservation.

En premier lieu, donc, la Belgique et le Danemark ont intégré à leur droit des hypothèses de conservation généralisée des données de connexion :

– en Belgique, les **données de trafic et de localisation** font ainsi l'objet d'une **conservation généralisée pour la détection des fraudes ou des utilisations abusives du réseau de communication électronique**, bien que la CJUE ne réserve cette possibilité qu'aux fins de la sauvegarde de la sécurité nationale[1] ;

– au Danemark, le ministre de la justice peut ordonner la **conservation générale des données pendant un an s'il y a des raisons de croire qu'il existe des menaces graves pour la sécurité nationale.** Dans un premier temps, le gouvernement danois avait considéré que les autorités pouvaient accéder, aux fins de lutter contre les infractions graves,

[1] *CJUE, 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 168.*

aux données conservées de manière généralisée pour la sécurité nationale. À la suite de l'arrêt *Commissioner of An Garda Síochána*[1], rendu six jours seulement après l'entrée en vigueur de la nouvelle loi, les autorités danoises ont toutefois estimé nécessaire de revenir sur leur interprétation. Elles envisagent, depuis lors, de recourir exclusivement à la conservation géographique ciblée dans le cadre de la lutte contre les infractions graves. La mise en œuvre du dispositif prévu par la loi n'est toutefois pas encore achevée[2].

En second lieu, force est de constater que les larges critères géographiques retenus par la Belgique et le Danemark pour définir la conservation ciblée permettent une **couverture de la quasi-totalité de leur territoire.** Ainsi, la police nationale danoise estime que **67 % de la population sera concernée par la conservation ciblée des données**[3].

De même, si le gouvernement belge, dans l'exposé des motifs du projet de loi, considère « *qu'**il n'est pas impossible que l'entièreté du territoire national soit visée par une conservation des données*** », il ajoute, dans une figure rhétorique révélatrice, qu'il s'agira alors « *d'une conservation ciblée dans son approche mais généralisée dans ses conséquences* »[4]. Visant à ce titre les critères de ciblage excessivement larges retenus par la loi belge du 20 juillet 2022, la Ligue des droits Humains et la *Liga voor mensenrechten* ont chacune déposé un recours en annulation devant la Cour constitutionnelle de Belgique[5].

Le **calcul des taux de criminalité** utilisés pour identifier les territoires ciblés est, en effet, discutable. Au Danemark, les paramètres de mesure sont fondés sur le **nombre réel d'infractions ou de condamnation**s, sans que ce chiffre ne soit rapporté à la taille de la population locale, **de sorte que les grandes villes sont automatiquement comptabilisées.** En Belgique, le taux de criminalité grave est calculé d'après les données saisies par les officiers de police judiciaire, qui comprennent **« *de nombreuses inexactitudes et/ou erreurs* »** selon l'Organe de contrôle de l'information policière[6]. La **notion d'infractions graves** utilisée pour calculer le taux de criminalité inclut, en outre, des délits de droits communs tels que la fraude informatique, le vol avec violence ou la détention de stupéfiants[7].

---

[1] *CJUE, 5 avril 2022, Commissioner of An Garda Siochana (C-140/20).*

[2] *Réponse du ministre de la Justice à la question n° 776 posée le 7 avril 2022 par la commission des affaires juridiques du Parlement danois.*

[3] *Réponse du ministre de la Justice à la question n° 62 relative au projet de loi L. 93 posée le 25 janvier 2022 par la commission des affaires juridiques du Parlement danois.*

[4] *Exposé des motifs du projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, déposé le 17 mars 2022 à la Chambre des représentants de Belgique, DOC 55 2572/007, p. 12.*

[5] *Introduites en février 2023, ces affaires sont pendantes. Communiqués de presse du 9 février 2023 de la Ligue des droits humains et du 7 février 2023 de la Liga voor Mensenrechten.*

[6] *Organe de contrôle de l'information policière (COC), Rapport d'activité 2020, p. 18.*

[7] *Cf. article 90* ter *du code d'instruction criminelle.*

Les rapporteurs jugent que **les difficultés rencontrées par les autorités belges et danoises démontrent, au-delà des cas d'espèce, le caractère paradoxal et peu opérationnel des critères posés par la CJUE**, les États ayant tenté de se conformer à sa jurisprudence s'étant rapidement trouvés poussés à en contourner la rigueur et subissant, au niveau national, des contestations quant aux discriminations induites par la conservation ciblée.

### 3. Les régimes de conservation proportionnée : un compromis précaire entre efficacité du système et conformité au droit de l'union

Certains États membres ont fait le choix de **renforcer leur législation pour prendre en compte l'évolution de la jurisprudence** de la Cour de justice de l'Union européenne **sans remettre en cause le principe d'une conservation généralisée des données.**

Les législateurs nationaux ont opéré des choix variés pour tenter d'atteindre **un équilibre précaire entre efficacité de l'action publique et protection de la vie privée** : renforcement du contrôle de l'accès aux données de connexion (Italie, Estonie), procédure de conservation rapide dite « *quick freeze* » (Italie, Suède et Irlande), modulation de la durée de conservation des données (Suède, Irlande, Italie), réduction du champ des données conservées (Suède, Irlande), *etc.*

En l'absence de jurisprudence récente concernant ces différentes réformes, **la conformité de ces systèmes de conservation « proportionnée » au droit de l'Union pose encore question.**

*a) Un régime de conservation mieux encadré*

Les juridictions nationales suédoises, estoniennes et irlandaises ont adressé des questions préjudicielles à la Cour de justice de l'Union européenne qui a confirmé la non-conformité de leur législation nationale au droit de l'Union[1].

En conséquence, **les législateurs nationaux ont fait évoluer leur régime de conservation des données de connexion et d'accès à celles-ci dans le cadre des enquêtes pénales en 2022. Les pouvoirs publics suédois et estoniens ont explicitement refusé de recourir à un système de conservation ciblée** pour des raisons techniques et politiques liées notamment à la difficulté de définir des critères de ciblage non discriminatoires : ils ont ainsi fait le choix de mieux encadrer le recours aux

[1] *CJUE, 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. (C-203/15 et C-698/15), CJUE, 2 mars 2021, Prokuratuur, aff. (C-746/18) et CJUE, 5 avril 2022, Commissioner of An Garda Siochana (C-140/20).*

données de connexion tout en maintenant le principe d'une conservation généralisée. Ces réformes ont porté sur :

– **la modulation de la durée de conservation des données**, réduite à 12 mois en Estonie et en Irlande, sauf exceptions[1], et à deux à dix mois en Suède en fonction de la nature des données[2] ;

– **la réduction du champ des données conservées**. En Irlande, la conservation des données de trafic et de localisation est désormais cantonnée à la lutte contre une menace sérieuse et réelle, actuelle et prévisible pour la sécurité nationale. En Suède, les données relatives aux conversations transférées, aux communications fixes et à la mise à disposition d'une capacité d'accès à internet ont été exclues du champ des données à conserver ;

– **la mise en place d'une procédure de conservation rapide dite « *quick freeze* »** en Suède, en Irlande et en Italie, pour une durée de 90 jours prorogeable sous conditions, et dans des cas particuliers (lutte contre la criminalité grave en Suède et en Italie, uniquement pour les données de trafic et de localisation en Irlande) ;

– **l'amélioration de l'information du citoyen**. En Estonie, l'Autorité de la protection des consommateurs publie chaque année, sur son site internet, le nombre de requêtes et les délais de conservation des données de connexion utilisées dans le cadre des enquêtes pénales et transmet ces informations à la Commission européenne.

*b) Des garanties supplémentaires en matière d'accès aux données de connexion en « gage » du maintien d'une conservation large*

**En Italie, si le régime légal de conservation des données de connexion n'a pas évolué, l'accès à ces données a été modifié** par le décret-loi du n° 132 du 30 septembre 2021 dans le but de mieux se conformer à l'exigence d'un contrôle indépendant et impartial dégagée par la jurisprudence européenne[3]. L'accès aux données de connexion est désormais cantonné aux seuls cas de commission d'infractions graves et autorisé sur ordre motivé du juge ou, en cas d'urgence, par le procureur de la République, sous le contrôle du juge.

---

[1] *En Estonie, la durée légale de conservation peut être prorogée, pour une durée limitée, pour la sauvegarde de l'ordre public et de la sécurité nationale. En Irlande, elle peut être modulée par décision ministérielle ou judiciaire dans le cadre de la lutte contre la criminalité grave en fonction de la nature des données et de la finalité répressive.*

[2] *En Suède, les données de localisation ne sont conservées que deux mois s'il s'agit de données de téléphonie ou six mois lorsqu'elles proviennent d'internet. Les autres données de connexion sont conservées pendant six mois dans le cadre de la téléphonie et dix mois pour les données issues d'internet.*

[3] *CJUE, 2 mars 2021, Prokuratuur, aff. C-746/18.*

**Les législateurs estonien et irlandais ont choisi**, quant à eux, **de faire varier la rigueur du contrôle de l'accès aux données en fonction de la nature des données concernées.** En Estonie, l'accès à certaines données de connexion n'est autorisé que dans le cadre de la lutte contre la criminalité grave. De même, **les données de trafic et de localisation ne sont désormais accessibles que sur décision du juge compétent** en vertu du code de procédure pénale et non plus du procureur.

La législation irlandaise prévoit trois procédures distinctes :

– un **accès direct aux données d'identification des utilisateurs**, sans contrôle judiciaire ;

– un accès sur autorisation du juge du tribunal de district compétent aux **données des sources internet et de trafic** ;

– un accès autorisé par le supérieur hiérarchique de l'agent demandeur avec validation *a posteriori* par le juge des **données de localisation** de l'équipement terminal.

### *B. DES PERSPECTIVES EUROPÉENNES INCERTAINES*

La jurisprudence de la Cour de justice de l'Union européenne a fait vaciller l'équilibre préalablement établi du droit européen et la conciliation que le législateur de l'Union a tenté d'assurer entre la protection de la vie privée, d'une part, et la prérogative régalienne des États membres en tant que garants des ordres publics nationaux, d'autre part. **Elle a, en tant que telle, eu des conséquences au-delà du strict périmètre des données de connexion**, ralentissant voire mettant à l'arrêt des négociations sur des textes clés dans tout le secteur du numérique.

Dans ce contexte, **les États membres tentent actuellement de se coordonner pour proposer un raisonnement alternatif à celui de la Cour et étudier les évolutions possibles du droit de l'Union.** La présidence suédoise a ainsi installé, au premier semestre 2023, un groupe d'experts de haut niveau sur l'accès à l'information numérique en matière pénale.

#### 1. La mise en suspens de négociations sur des textes-clés pour l'avenir de l'Union

La jurisprudence de la CJUE est venue redistribuer les cartes dans un paysage institutionnel déjà fragmenté au niveau européen, accentuant les lignes de fracture préexistantes et, partant, aggravant les difficultés à bâtir un consensus sur des sujets pourtant essentiels.

En effet, les co-législateurs européens ont eux-mêmes des positions disparates, que l'on peut résumer (avec la dose de caricature qu'un tel exercice de synthèse implique) de la manière suivante :

**– le Conseil européen, émanation des États, insiste depuis plusieurs années sur l'impérieuse nécessité d'une adaptation des moyens**

**de répression aux innovations technologiques.** C'est ainsi qu'il a, dès ses conclusions du 23 juin 2017, estimé « *que l'accès effectif aux preuves électroniques est essentiel pour lutter contre les formes graves de criminalité et le terrorisme* » et que, « *sous réserve de garanties appropriées, la disponibilité des données devrait être assurée* ». La stratégie de l'UE contre le crime organisé 2021-2025 demandait, de même, « *d'adapter les services répressifs et judiciaires à l'ère numérique* ». Ces prises de position ont trouvé un prolongement opérationnel avec de vastes opérations coordonnées par Europol et associant plusieurs États, qui ont permis l'infiltration de services cryptés utilisés à des fins criminelles (ANOM, EncroChat, SKY ECC) puis le démantèlement des réseaux de criminalité organisée correspondants ;

– tout à l'inverse, **le Parlement européen fait traditionnellement preuve d'un attachement fort aux libertés publiques** – parfois au détriment des principes avec lesquelles celles-ci doivent être conciliées. Ses positions en trilogue sont marquées par une **volonté de prohiber toute atteinte, par les autorités répressives, à la confidentialité des données échangées en ligne ou *a minima* de réduire au strict minimum le niveau d'immixtion des États dans les communications privées** – ce qui peut paraître surprenant dans un contexte où les opérateurs continuent de bénéficier d'un accès faiblement régulé aux mêmes données, puisqu'ils peuvent les traiter presque sans limites pour leurs besoins commerciaux, y compris en établissant le profil des utilisateurs afin de leur proposer une publicité ciblée répondant à leur « profil » tel qu'il a été révélé par leur activité en ligne. Certains interlocuteurs des rapporteurs à Bruxelles ont ainsi jugé que les parlementaires européens faisaient preuve de défiance vis-à-vis des gouvernements nationaux, dont les positions étaient vues comme liberticides par nature, et se montraient *a contrario* particulièrement sensibles à la force de conviction déployée par les lobbies associatifs européens qui agissent pour la défense des droits individuels sur internet. **Le Parlement européen apparaît, en somme, comme le tenant d'une protection maximale des données échangées en ligne**, y compris dans les cas où un accès auxdites données est proposé à des fins de lutte contre la criminalité ;

– enfin, **la Commission européenne ne semble pas apte à parler d'une seule voix sur le sujet des données de connexion, ses différentes directions générales affichant en la matière des points de vue difficilement conciliables**. En effet, les intérêts objectifs des trois directions impliquées dans le débat, à savoir la DG Justice, la DG *Connect* et la DG Affaires intérieures (*Home*) sont divergents, la première ayant pour priorité la protection des droits et libertés fondamentaux tandis que la seconde a pour objectif de développer le marché du numérique en Europe, l'innovation et la recherche afin de renforcer la compétitivité collective des États, et que la troisième est chargée de la sécurité intérieure à l'Union et du contrôle des frontières. Comme les rapporteurs l'ont constaté, le dialogue entre ces directions peut s'avérer complexe, voire fastidieux. Dès lors, **le devenir d'un projet dépend étroitement de la DG qui a été chargée du pilotage du texte**

**au sein de la Commission**, l'identité de la direction pilote constituant par elle-même un « cadre » spécifique de réflexion et le révélateur de la priorité qui est poursuivie.

C'est dans ce contexte institutionnel qu'il faut analyser l'impact de la jurisprudence de la CJUE sur le processus normatif européen.

**Les décisions de la Cour**, de pair avec l'existence de dissensions entre les États, **ont en effet contribué à complexifier les négociations sur plusieurs textes importants**, au premier rang desquels le futur règlement dit « *e-privacy 2* » (ou « vie privée et communications électroniques » 2), *lex specialis* du RGPD (règlement général sur la protection des données) ayant vocation tant à préciser son application dans le domaine des communications électroniques qu'à apporter, le cas échéant, des dérogations ponctuelles et proportionnées aux principes qu'il fixe. Ce règlement doit à terme remplacer l'actuelle directive *e-privacy*, qui constitue à la fois le texte fondateur au niveau européen en matière de traitement des données téléphoniques internet et la base de la première censure prononcée par la Cour de Luxembourg en 2014.

**La directive *e-privacy* est en cours de renégociation depuis janvier 2017, soit depuis près de 7 ans** : après le vote par le Parlement européen de son rapport en 2018 et l'atteinte d'un accord au sein du Conseil en février 2021, **l'examen du texte est au point mort** et la phase de trilogue ne semble pas connaître d'avancées significatives. Cette lente avancée des discussions découle largement de la volonté des États de trouver, à l'occasion de l'adoption du futur règlement, une voie de contournement de la jurisprudence de la CJUE qui consisterait, en pratique, à rappeler au sein de ce texte que le principe de confidentialité des communications ne s'applique ni « *aux activités qui ne relèvent pas du champ d'application du droit de l'Union* », ni « *aux activités menées par les autorités compétentes 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, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces* »[1].

Comme le rappelle le Secrétariat général aux affaires européennes dans sa réponse écrite au questionnaire des rapporteurs, « *il est peu probable que les négociations aboutissent à moyen terme* » notamment au vu de la position allemande très protectrice sur les données de connexion et de l'émergence d'autres priorités en matière numérique (par exemple, en ce qui concerne la régulation de l'intelligence artificielle) qui occupent l'agenda des institutions européennes. **Pour autant, le maintien en vigueur de la directive *e-privacy* n'est pas une option tenable, celle-ci n'étant pas entièrement compatible avec le RGPD.** En l'état, la stratégie de la Commission ne semble pas arrêtée : celle-ci pourrait donc reprendre les discussions après les élections européennes et le renouvellement subséquent de la Commission

[1] *Texte provisoire du règlement, consultable sur le site https://eur-lex.europa.eu.*

en juin 2024, ou encore fragmenter le texte pour dégager plus facilement des accords sur certaines portions – étant relevé que ces deux options ne sont pas mutuellement exclusives.

Le texte *e-privacy 2* n'est pas le seul à s'être trouvé bousculé par la jurisprudence de la Cour, puisque **la conformité de plusieurs réglementations (ou projets de réglementations) européennes se trouve remise en question par ricochet par ses décisions sur les données de connexion.** Outre les textes qui, même au-delà du numérique, se trouvent impactés par les débats liés aux métadonnées (à l'instar du projet de législation européenne sur la liberté des médias, qui a conduit à poser la question d'une définition par le droit de l'Union de la notion de « criminalité grave »), deux exemples méritent d'être cités.

**Le premier concerne la lutte contre les abus sexuels sur mineurs**, ce sujet faisant l'objet d'un projet de règlement[1] ayant donné lieu au dépôt au Sénat d'une proposition de résolution européenne de Ludovic Haye, Catherine Morin-Desailly et André Reichardt, adoptée par le Sénat le 20 mars 2023[2]. La lutte contre la pédocriminalité en ligne est l'un des thèmes sur lesquels la tension entre la nécessaire répression des infractions, d'une part, et la protection des données personnelles, d'autre part, est la plus saillante : le projet de règlement comporte ainsi, aux côtés de propositions plus consensuelles, une mesure controversée et contestable dans son principe consistant à **obliger les fournisseurs de services de communication et d'hébergement en ligne à effectuer des analyses, y compris au sein des correspondances privées des utilisateurs et en cas de chiffrement des communications**, à la fois pour identifier des images ou des vidéos déjà répertoriées comme pédo-criminelles et disposant d'une empreinte numérique d'identification, **et pour détecter par l'utilisation d'outils prédictifs des contenus pédo-criminels ou de « pédo-piégeage » nouveaux**. L'atteinte lourde à la confidentialité des échanges et le risque élevé, dans le cas des contenus nouveaux, de « faux positifs » posent une véritable question de principe : comme le relevaient les auteurs de la proposition de résolution précitée, « *la possibilité d'émettre des injonctions de détection des contenus pédopornographiques ou de pédopiégeage est une atteinte manifeste à l'interdiction de surveillance généralisée des contenus* ». Au surplus, l'analyse demandée aux fournisseurs n'étant pas de nature à reposer sur les seuls contenus et supposant un « croisement » de ceux-ci avec les données personnelles de l'utilisateur, le projet de règlement crée le risque d'un « *'chalutage généralisé' des données par les fournisseurs que pourrait ouvrir une telle réglementation* »[3]. En d'autres termes, cette initiative, pourtant portée par la Commission européenne, soulève des problèmes de fond et **apparaît en complète incohérence avec la ligne défendue par la Cour de justice**.

---

[1] *Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants.*

[2] *Consultable sur le site du Sénat.*

[3] *Exposé des motifs de la proposition de résolution précitée.*

**Il est intéressant de constater que la jurisprudence européenne a, en l'espèce, fait office de force régulatrice**, invoquée en particulier dans l'avis conjoint du Contrôleur européen de la protection des données (CEPD) et du Comité européen de la protection des données (ECDP) dont les termes sont proches de la résolution adoptée par la Haute assemblée.

Le second exemple porte sur le **traitement des données des passagers par les transporteurs aériens (données PNR)**. Saisie d'une question préjudicielle sur ce traitement, la Cour de justice s'est appuyée[1] sur ses décisions rendues en matière de données de connexion pour considérer, d'une part, que le principe d'une conservation généralisée pouvait être admis pour autant que l'objectif poursuivi (la lutte contre le terrorisme) concernait une menace pour la sécurité nationale des États et que, d'autre part, le caractère nécessaire et proportionné de l'atteinte portée aux droits reconnus par les articles 7 et 8 de la Charte devait être apprécié en fonction des critères dégagés par elle dans des arrêts relatifs aux métadonnées (à savoir *Digital Rights* et *La Quadrature du Net*). Elle s'est donc dans ce cadre posé la question d'un éventuel traitement de ces données aux fins de lutte contre des infractions qui semblent relever non pas de la criminalité grave, mais de la délinquance ordinaire.

Plus encore, **la jurisprudence a d'ores et déjà eu un impact palpable sur des réglementations européennes définitivement adoptées, et notamment sur le contenu du « paquet » *e-evidence*, relatif aux preuves numériques**. Issus d'une réflexion lancée en 2015 après les dramatiques attentats de Paris traduite par une proposition rendue publique par la Commission en 2017, la directive et le règlement *e-evidence* ont été définitivement adoptés à l'été 2023 et sont venus inscrire dans le droit probatoire européen des règles étroitement inspirées des différents arrêts des juges de Luxembourg.

**Le « paquet » *e-evidence***

Proposée par la Commission à l'invitation du Parlement et du Conseil en avril 2018, la réglementation *e-evidence* (ou « preuve électronique »), composée d'un règlement et d'une directive, a été publiée au *Journal officiel de l'Union européenne* le 28 juillet dernier. Entrée en vigueur le 18 août 2023, elle sera applicable à compter du 18 août 2026.

***E-evidence* faisait partie des priorités identifiées par la présidence française de l'Union européenne au premier semestre 2022**, le Garde des Sceaux s'étant largement investi pour obtenir des avancées sur ce dossier. Le « paquet » *e-evidence* trouve son origine dans une volonté de rénover le cadre issu de la convention de Budapest de 2001 sur la cybercriminalité : en effet, celui-ci **échouait à permettre une coopération judiciaire fluide avec les entreprises américaines du numérique**, au premier rang desquelles Twitter, Google et Meta (Facebook, WhatsApp) –

[1] *CJUE (grande chambre), 21 juin 2022, Ligue des droits humains c. Conseil des ministres, affaire C-817/19.*

notamment pour l'obtention des données de trafic et de contenu détenues par ces dernières et susceptibles d'être requises dans un cadre pénal par un État-membre de l'Union.

*E-evidence* vise ainsi à doter les autorités judiciaires nationales d'outils leur permettant d'accéder plus facilement aux preuves électroniques et à créer un cadre normalisé dans lequel ces données peuvent être demandées aux fournisseurs de services électroniques. **Elle s'appliquera à tout fournisseur proposant des services dans l'Union, indépendamment de sa nationalité.** Les fournisseurs concernés qui ne disposeraient pas d'un établissement sur le territoire de l'Union se voient corrélativement tenus de désigner un représentant légal

**Deux nouvelles injonctions sont créées par le règlement :**

– une **injonction européenne de production**, qui permettra à une autorité judiciaire de demander des preuves électroniques à un fournisseur de services d'un autre État membre. Le fournisseur sera tenu de répondre dans un délai de dix jours, voire de huit heures en cas d'urgence ;

– une **injonction européenne de conservation, qui permettra à une autorité judiciaire d'empêcher l'effacement de données** pour une durée de 60 jours (pouvant être prolongée d'une durée complémentaire de 90 jours) et, partant, de sécuriser les injonctions de production ultérieures.

Le régime juridique des injonctions **varie selon le type de données demandées** :

– **pour les données d'identification**, une demande du procureur (ou validée par ce dernier) sera possible ; par ailleurs, les injonctions seront possibles pour toute infraction pénale et pour l'exécution d'une privation de liberté d'au moins 4 mois ;

– à l'inverse, **seul un juge du siège, une juridiction ou un juge d'instruction pourra formuler (ou valider) une injonction portant sur des données de trafic** (cette notion intégrant, dans la nomenclature européenne, les données relatives à l'emplacement du dispositif – donc à sa localisation) **ou de contenu.** De telles injonctions seront réservées aux infractions punies d'une peine d'emprisonnement de trois ans au moins et à certaines infractions si elles sont commises totalement ou partiellement au moyen d'un système d'information : fraude et contrefaçon des moyens de paiement ; pédo-criminalité ; attaques contre les systèmes d'information ; infractions liées au terrorisme...

Les autorités précitées pourront soit être à l'origine de la demande, soit valider les injonctions émises par les services d'enquête.

En cas de défaillance, **le fournisseur encourra des sanctions pouvant aller jusqu'à 2 % de son chiffre d'affaires mondial total.**

Les injonctions transiteront par un système informatique décentralisé, hébergé par la Commission européenne. **Chaque État-membre pourra, en complément, désigner une ou plusieurs autorités centrales chargées de la transmission administrative des injonctions** et de la gestion des actes s'y rattachant (notifications, correspondances administratives...).

Dans des cas d'urgence (celle-ci étant définie par le règlement comme une « *menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne ou pour une infrastructure critique* »), **les services d'enquête pourront émettre une injonction**

**sans validation préalable** ; une régularisation devra intervenir dans un délai maximal de 48 heures.

Le règlement est, enfin, assorti de divers garde-fous :

– si la personne dont les données sont demandées ne réside pas dans l'État d'émission ou si l'infraction n'y a pas été commise, **les États devront notifier leur demande à l'autorité nationale du prestataire de services** qui pourra refuser l'injonction ;

– si le pays d'émission fait l'objet d'une procédure de **sanction pour violation systémique de l'État de droit**, les notifications pourront être automatiques ;

– des **protections particulières, analogues à celles qui existent en droit français, sont prévues pour certaines professions et certaines données** (avocats, journalistes, secret médical…).

*Source : commission des lois.*

Or ces textes, s'ils constituent un mécanisme bienvenu de « rattrapage » européen face au *Cloud Act* américain et s'ils comportent des points rassurants pour les acteurs nationaux de l'enquête (notamment quant à la possibilité pour les parquets d'émettre seuls des injonctions portant sur des données d'identification, ou encore s'agissant de la reconnaissance d'un mécanisme d'accès dérogatoire en cas d'urgence), **viennent graver dans le marbre des points de la jurisprudence de la Cour non encore stabilisés.** Tel est le cas, en particulier, du principe selon lequel des données de connexion d'identification peuvent être obtenues pour une infraction sans quantum de peine minimal particulier (donc hors du champ de la criminalité « grave ») et, surtout, de l'émergence d'une appréciation autonome par le droit de l'Union de la notion de « criminalité grave » hors du cadre de la coopération européenne[1], comme en atteste la fixation d'un *quantum* à partir duquel il sera possible de requérir les données de trafic et de contenu (soit trois ans d'emprisonnement), y compris pour des enquêtes strictement nationales. Si ce seuil correspond à ce que prévoit la législation française en matière de données de connexion « classiques », **il est de nature à ouvrir la voie à une définition européenne des règles de procédure pénale, ce que les rapporteurs estiment tout à la fois inopportun et contraire à l'esprit comme à la lettre du Traité sur le fonctionnement de l'Union européenne.**

### 2. Des tentatives de coordination entre États membres : le groupe d'experts de haut niveau *Going dark*

Dans le même temps, et face aux contestations que faisait naître la jurisprudence de la CJUE comme aux défis soulevés par la montée en puissance du chiffrement des communications, la présidence suédoise a

[1] *Les seuils existants en droit européen étaient, jusqu'à ce jour, liés à la coopération européenne et aux compétences d'Europol (décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres et règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol)).*

estimé nécessaire de mettre en place une réflexion intitulée *Going dark*. Réunissant les ministres de la justice et de l'intérieur des États-membres ainsi que les délégations nationales du Conseil, elle s'appuie sur un **groupe d'experts de haut niveau** (ou « HLEG » pour *high level experts group*) dédié, placé sous l'autorité conjointe de la Commission et de la présidence tournante du Conseil et dont les travaux ont débuté en juin 2023. Ce groupe d'experts, rebaptisé ADELE (pour *access to data for effective law enforcement* – accès aux données pour l'application effective du droit), rendra ses conclusions en juin 2024.

L'objectif du HLEG, tel que résumé par la DG *Home* qui en assure le pilotage pour le compte de la Commission européenne, est de **passer d'un travail en silos à une réflexion pluridisciplinaire qui doit permettre de concilier les attentes opérationnelles des entités répressives et les principes de régulation portés par les autorités de protection des données.** Le groupe fait ainsi intervenir des praticiens de l'enquête pénale, des experts de la protection des données, des opérateurs privés et des acteurs associatifs et universitaires. D'après les éléments recueillis par les rapporteurs lors de leur déplacement à Bruxelles, le HLEG s'organise désormais en **trois sous-groupes structurés par types de données** et travaillant respectivement sur l'accès aux données stockées sur le terminal d'un utilisateur (un téléphone portable, par exemple), aux données stockées par un fournisseur (ce qui correspond au sujet de réflexion de la présente mission d'information) et aux données en transit (ce qui concerne, à titre principal, les interceptions en temps réel).

S'ils se réjouissent de cette initiative bienvenue, **les rapporteurs n'ont pu qu'être frappés par la divergence d'interprétation qui s'est exprimée au cours de leurs échanges au sein même des directions de la Commission quant aux objectifs du HLEG et à l'état de ses réflexions**. Ainsi, alors que le but affiché par la DG *Home* est d'identifier une base juridique solide permettant une conservation large des données et une exploitation de celles-ci y compris hors du périmètre de la criminalité grave – ce qui reviendrait à une remise en cause substantielle des arrêts de la CJUE[1] –, la DG Justice estime, tout à l'inverse, que les conclusions du groupe d'experts devront être en pleine conformité avec la jurisprudence actuelle. De la même manière, si la DG *Home* voit dans les dernières évolutions des travaux de la Cour (et notamment dans la réouverture de la phase orale du dossier dit « Hadopi ») un signal positif pouvant témoigner d'une ouverture nouvelle et de la possibilité d'une évolution sur le fond de la jurisprudence, la DG Justice estime que la position de la CJUE est à la fois remarquablement stable et insusceptible de faire l'objet d'un revirement, y compris à moyen terme. Enfin, là où la DG Justice s'est montrée rétive à toute réflexion

[1] *La DLPAJ estime, de même, que l'existence même du groupe d'experts et les motifs de sa création « démontrent un consensus fort entre les États membres et la Commission sur la nécessité de changer le cadre européen pour dépasser le blocage créé par la CJUE » (réponses écrites au questionnaire des rapporteurs).*

tendant à étendre les possibilités de conservation des données dans un cadre pénal et a jugé nécessaire de s'en tenir à un *quick freeze* prospectif n'ouvrant pas d'accès à des données antérieurement stockées, **la DG *Home* a au contraire envisagé un encadrement renforcé de l'accès aux données en contrepartie d'une conservation vaste**[1], sur le modèle des « garanties de bout en bout » exigées par la Cour européenne des droits de l'homme et qui donnent aux États une possibilité de choix quant aux moyens qu'ils utilisent pour garantir leur sécurité tout en les soumettant à une obligation de résultat quant à la préservation des libertés fondamentales des citoyens[2].

**Les « garanties de bout en bout »**

Par deux arrêts du 25 mai 2021, la grande chambre de la Cour européenne des droits de l'homme s'est prononcée sur les conditions dans lesquelles un régime de « *surveillance de masse des communications électroniques* » pouvait être compatible avec les articles 8 et 10 de la Convention européenne des droits de l'homme.

La Cour a en effet jugé que l'article 8 de la Convention européenne « *n'interdit pas [aux États parties] de recourir à l'interception en masse afin de protéger la sécurité nationale ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves* » et que **« *les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet* ».** En revanche, elle a examiné les « *garanties contre l'arbitraire et les abus qui […] sont prévues [dans les régimes mis en place]* », en acceptant de ne disposer en la matière que d'informations limitées par le besoin « *légitime* » des autorités nationales « *d'opérer dans le secret* ».

**La CEDH a ainsi fixé une série de critères lui permettant d'apprécier l'atteinte d'un juste équilibre entre l'objectif poursuivi et la protection des droits et libertés garantis par la Charte**, cet équilibre reposant sur les éléments suivants :

– les motifs pour lesquels l'interception en masse peut être autorisée ;

– les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;

– la procédure d'octroi d'une autorisation ;

– les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;

– les précautions à prendre pour la communication de ces éléments à d'autres parties ;

[1] *Ce qui est en cause, davantage qu'une conservation étendue, est la remise en cause de l'interdiction posée par la Cour d'une porosité des finalités – ou, en d'autres termes, la possibilité pour les États d'utiliser en matière pénale les données qu'ils ont conservées aux fins de lutter contre les menaces envers la sécurité nationale, avec des modalités adaptées et contrôlées d'accès.*

[2] *CEDH, 25 mai 2021, Big Brother Watch et autres c. Royaume-Uni, req. nos 58170/13, 62322/14 et 24960/15. La doctrine des « garanties de bout en bout », appliquée ici en matière de sécurité nationale, permet une analyse des garde-fous apportés à chaque étape du processus de gestion des données pour apprécier le caractère acceptable, ou non, de l'équilibre ainsi créé entre l'objectif sécuritaire poursuivi et la protection de la vie privée.*

– les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;

– les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;

– les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

Cette doctrine est considérée comme plus compréhensive que la jurisprudence de la Cour de Luxembourg dans la mesure où **la condamnation des deux États concernés (le Royaume-Uni et la Suède) a résulté non pas de la violation d'un impératif absolu mais de l'insuffisance du cumul des garanties apportées, à chaque étape, par les autorités nationales.**

*Source : commission des lois*

Cette ambiguïté, qui ne peut qu'être préjudiciable au déroulement des travaux du groupe d'experts comme à toute réflexion collective sur les données de connexion, témoigne de **l'absence de vision commune au niveau européen,** tant sur le **point d'équilibre entre les impératifs de sécurité et la protection de la vie privée** que sur **la répartition des compétences entre les États et l'Union** et sur les marges de manœuvre dont doivent disposer les autorités nationales en matière pénale.

# TROISIÈME PARTIE
# LES LIMITES DES TENTATIVES FRANÇAISES DE MISE EN CONFORMITÉ AVEC LE DROIT DE L'UNION EUROPÉENNE

À la suite de la jurisprudence de la Cour de justice de l'Union européenne, plusieurs décisions ont été successivement rendues par le Conseil d'État, le Conseil constitutionnel et la chambre criminelle de la Cour de cassation, qui n'ont toutefois **intégré que partiellement** les exigences posées par la Cour de justice et qui présentent entre elles **des points de divergence**, laissant ainsi peser un aléa sur la sécurité juridique des procédures malgré deux modifications législatives intervenues en 2021 et 2022. Cette situation invite à s'interroger à nouveau sur le curseur entre défense des droits et libertés, d'une part, et protection de la sécurité publique et du territoire national, d'autre part.

## I. LA CONSERVATION DES DONNÉES DE CONNEXION : LA CONSTRUCTION PROGRESSIVE D'UNE CONSERVATION CIRCONSTANCIÉE

### *A. AVANT 2021, UNE OBLIGATION DE CONSERVATION GÉNÉRALISÉE CONTRAIRE TANT AU DROIT DE L'UNION EUROPÉENNE QU'À LA CONSTITUTION*

**Le cadre juridique français de la conservation des données de connexion a été bouleversé par la jurisprudence européenne**. Comme on l'a vu, l'article L. 34-1 du code des postes et des communications électroniques **imposait jusqu'alors aux opérateurs de communications électroniques de conserver certaines catégories de données techniques pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales pendant une durée d'un an,** par dérogation à l'obligation générale d'effacer et de rendre anonyme toute donnée relative au trafic[1]. L'article 6 de la loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* prévoyait une **obligation de même nature pour les fournisseurs d'accès à internet et les hébergeurs de contenus** s'agissant des données de nature à permettre l'identification de quiconque a contribué à la création de contenu au sein des services dont ils sont prestataires.

**Cette obligation de conservation pendant une durée d'un an de l'ensemble des données de connexion –** en particulier les données relatives au trafic et les données de localisation **– a dû être aménagée pour assurer sa conformité à la jurisprudence de la Cour de justice de l'Union européenne** qui a jugé, par un arrêt du 6 octobre 2020[2] qu'**une législation française ne pouvait, sans méconnaître le droit de l'Union européenne, imposer à titre**

---

[1] *Prévue par le II du même article.*

[2] *Cour de justice de l'Union européenne, arrêt « La Quadrature du net » du 6 octobre 2020 (affaires C 511/18, C 512/18 et C 520/18).*

**préventif aux opérateurs de communications électroniques et aux fournisseurs d'accès à internet une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation** sans justifier dans le même temps d'une menace pour la sécurité nationale.

Le 25 février 2022, le Conseil constitutionnel, saisi de deux questions prioritaires de constitutionnalité[1], a estimé que **la conservation généralisée et indifférenciée des données de connexion** prévue par l'article L. 34-1 du code des postes et des communications électroniques dans sa rédaction applicable à l'époque des faits[2] **était également contraire à la Constitution** dans la mesure où elle s'appliquait « *de façon générale à tous les utilisateurs des services de communications électroniques* » et portait « *indifféremment sur toutes les données de connexion relatives à ces personnes, quelle qu'en soit la sensibilité et sans considération de la nature et de la gravité des infractions susceptibles d'être recherchées* », constituant ainsi une atteinte disproportionnée au droit au respect de la vie privée.

### *B. LA POSITION DU CONSEIL D'ÉTAT : UNE TENTATIVE DE CONSTRUCTIVISME JURISPRUDENTIEL*

L'inconventionalité du droit national a conduit le Conseil d'État, en dans sa décision d'assemblée *French data network* du 21 avril 2021[3], à **annuler la décision implicite du Premier ministre de ne pas abroger l'article R. 10-13 du code des postes et des communications électroniques** et le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Il a en effet jugé que **si, en l'état, la conservation générale et indifférenciée des données de trafic et de localisation était justifiée par des menaces pour la sécurité nationale**, les dispositions contestées relatives à la conservation des données de connexion étaient contraires au droit de l'Union européenne dans la mesure où :

- elles ne justifiaient pas la conservation des données de connexion par l'existence de ces menaces et ne subordonnaient pas le maintien en vigueur d'une conservation généralisée à l'**existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale**. Il a considéré qu'un réexamen périodique de l'existence d'une telle menace était nécessaire ;

---

[1] *Conseil constitutionnel, décision n° 2021-976/977 QPC du 25 février 2022.*

[2] *Qui correspond à la version décrite ci-avant et diffère de la version en vigueur lors de la décision du Conseil constitutionnel.*

[3] *Conseil d'État, Ass., 21 avril 2021, French Data Network et autres, n° 393099. Cette décision est consultable sur le site du Conseil d'État.*

- elles **ne limitaient pas à la sauvegarde de la sécurité nationale les finalités de l'obligation de conservation généralisée et indifférenciée des données de connexion** autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et les adresses IP, c'est-à-dire les **données de trafic et de localisation**.

S'agissant de l'obligation de **conservation des données de connexion pour les besoins liés aux procédures pénales**, le Conseil d'État a admis que, en l'état, elle n'était pas conforme au droit de l'Union européenne. Il a toutefois souligné, d'une part, que la solution de conservation ciblée proposée par la Cour de justice de l'Union européenne dans sa décision précitée « *se [heurtait] à des obstacles techniques qui en compromettent manifestement la mise en œuvre* » et « *présenterait un intérêt opérationnel particulièrement incertain, dès lors qu'elle ne permettrait pas, y compris en cas de faits particulièrement graves, d'accéder aux données de connexion d'une personne suspectée d'une infraction qui n'aurait pas été préalablement identifiée comme étant susceptible de commettre un tel acte* »[1]. Il a indiqué, d'autre part, **que les données relatives au trafic et les données de localisation conservées par les opérateurs pouvaient être accessibles aux fins de la lutte contre la criminalité grave par le biais d'une injonction de procéder, pour une durée déterminée, à une « conservation rapide » de ces données** dès lors que l'infraction concernée était « *suffisamment grave pour justifier [une] ingérence dans la vie privée* », **y compris s'agissant des données initialement conservées par les opérateurs, les fournisseurs et les hébergeurs aux fins de la sauvegarde de la sécurité nationale**.

Ce faisant, le Conseil d'État a dessiné un **schéma permettant aux autorités d'enquête d'accéder par le biais d'un mécanisme d'injonction de conservation rapide aux données de connexion conservées par les opérateurs**.

En conclusion, le Conseil d'État a enjoint au Premier ministre de procéder à l'abrogation des dispositions règlementaires contestées dans un délai de six mois à compter de la décision, soit avant le 21 octobre 2021.

---

[1] *Conseil d'État, Ass., 21 avril 2021, French Data Network et autres, n° 393099. Le Conseil d'État a, plus encore, estimé que* « ni l'accès aux données de connexion conservées volontairement par les opérateurs, ni la possibilité de leur imposer une obligation de conservation ciblée, ni le recours à la technique de la conservation rapide ne permettent, par eux-mêmes, de garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales ».

### *C. LA LOI « RENSEIGNEMENT » DE 2021 : L'INSCRIPTION LÉGISLATIVE DU MODÈLE DESSINÉ PAR LE CONSEIL D'ÉTAT*

En conséquence de ces jurisprudences, le législateur a modifié, dans le cadre de la loi n° 2021-998 du 30 juillet 2021 *relative à la prévention d'actes de terrorisme et au renseignement*, l'article L. 34-1 du code des postes et des télécommunications électroniques pour **modifier l'obligation faite aux opérateurs de conserver les données de connexion en distinguant selon les catégories de données et les finalités de la conservation**, suivant le modèle esquissé par le Conseil d'État dans sa décision précitée du 21 avril 2021.

Ainsi, le II *bis* de l'article L. 34-1 oblige désormais les opérateurs à conserver :

– les informations relatives à **l'identité civile de l'utilisateur** pendant une **durée de cinq ans** après l'expiration du contrat de la personne concernée, **pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale** ;

– **pour les mêmes finalités**, les **autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte** ainsi que les **informations relatives au paiement**, jusqu'à l'expiration d'un **délai d'un an** à compter de la fin de validité de son contrat ou de la clôture de son compte ;

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

– s'agissant des **autres données de trafic et des données de localisation** précisées par un décret en Conseil d'État, le III du même article L. 34-1 prévoit que les opérateurs sont obligés de les conserver, pendant une **durée d'un an**, pour des **motifs tenant à la sauvegarde de la sécurité nationale**, lorsqu'ils y sont enjoints par le Premier ministre dès lors que celui-ci **constate une menace grave, actuelle ou prévisible, contre la sécurité nationale**.

L'article précise que les données conservées par les opérateurs en application de ces différentes obligations peuvent faire l'objet d'une **injonction de conservation rapide** par les **autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect**, afin que ces autorités puissent accéder à ces données[1].

[1] *III* bis *du même article L. 34-1 du code des postes et des communications électroniques.*

**Obligations de conservation des données de connexion par les opérateurs instaurées par la loi n° 2021-998 du 30 juillet 2021 *relative à la prévention d'actes de terrorisme et au renseignement***

| Données conservées | Obligation de conservation | Durée de conservation des données | Finalités de l'accès |
|---|---|---|---|
| Identité civile | Permanente | 5 ans à compter de la fin de validité du contrat | Procédures pénales<br>Prévention des menaces contre la sécurité publique<br>Sauvegarde de la sécurité nationale |
| Coordonnées de contact et de paiement, données relatives aux contrats et aux comptes | Permanente | 1 an à compter de la fin de validité du contrat ou de la clôture du compte | Procédures pénales<br>Prévention des menaces contre la sécurité publique<br>Sauvegarde de la sécurité nationale |
| Adresses IP et équivalents | Permanente | 1 an à compter de la connexion ou de l'utilisation des équipements terminaux | Criminalité et délinquance grave<br>Prévention des menaces graves contre la sécurité publique<br>Sauvegarde de la sécurité nationale |
| Autres données de trafic et données de localisation | En cas de menace grave, actuelle ou prévisible contre la sécurité nationale | Un an renouvelable, sous la forme d'une injonction par décret du Premier ministre | Sauvegarde de la sécurité nationale |
| Toutes les données conservées par les opérateurs | Selon la nature de la donnée | Selon la nature de la donnée | Prévention et répression de la criminalité et de la délinquance grave ; autres manquements graves *via* une injonction de conservation rapide |

*Source : Commission des lois du Sénat*

On notera que **le Sénat, à l'occasion de l'examen de ce texte, avait souhaité que la procédure de « *quick freeze* » (l'injonction de conservation rapide) soit réservée aux données de localisation et de trafic**, ménageant un accès plus aisé aux données d'identification. **Cette position n'a pas été suivie par l'Assemblée nationale** qui, en nouvelle puis en dernière lecture, a

rétabli une rédaction imposant une injonction de conservation rapide pour l'accès des autorités d'enquête à l'ensemble des données de connexion, quelle qu'en soit la nature, alors même que cette exigence ne découle pas de la jurisprudence de la CJUE ou des décisions des cours suprêmes nationales.

**Le législateur**, suivant l'arrêt du Conseil d'État, **a écarté la mise en place d'un mécanisme de conservation « ciblée »** des données de connexion utilisables dans le cadre des enquêtes pénales. Plusieurs raisons, d'ordre tant pratique que juridique, s'opposaient en effet à un tel mécanisme :

- il semble difficile de mettre en place des critères de ciblage par personne qui soient non-discriminatoires ;

- le ciblage par zones géographiques se heurte à des obstacles techniques difficilement surmontables et générerait des surcoûts déraisonnables ;

- il n'est pas possible de connaître à l'avance le lieu de la commission d'une infraction grave ou le profil de l'auteur ;

- la conservation ciblée peut avoir pour effet pervers d'inciter les services d'enquête à se tourner vers des techniques plus intrusives ;

- une conservation ciblée inciterait les groupes criminels à développer des stratégies de contournement ;

- il n'existe pas de ligne de démarcation claire entre la criminalité grave et la sûreté de l'État, certaines infractions (comme la criminalité organisée) étant de nature à relever des deux catégories.

En application de la nouvelle rédaction de l'article L. 34-1 du code des postes et des télécommunications électroniques, par trois décrets n° 2021-1363 du 20 octobre 2021, n° 2022-1327 du 17 octobre 2022 et n° 2023-933 du 10 octobre 2023 *portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion*, le Premier ministre a ainsi enjoint aux opérateurs de communications électroniques et aux fournisseurs de services sur internet de conserver les données de connexion pendant un an.

**Les fondements des décrets portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion**

Le Conseil d'État avait indiqué, dans sa décision précitée de 2021, que « *la France est confrontée à une menace pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure* ».

Il avait décrit cette menace comme procédant « *d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Deux nouveaux attentats ont déjà été déjoués en 2021. Le plan Vigipirate a été mis en œuvre au niveau " Urgence attentat " entre le 29 octobre 2020 et le 4 mars 2021 puis au*

*niveau " Sécurité renforcée – risque attentat " depuis le 5 mars 2021, attestant d'un niveau de menace terroriste durablement élevé sur le territoire* ». Le Conseil avait par ailleurs indiqué que « *la France [était] particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique. De nombreuses entreprises françaises, tant des grands groupes que des petites et moyennes entreprises, font ainsi l'objet d'actions malveillantes, visant leur savoir-faire et leur potentiel d'innovation, à travers des opérations d'espionnage industriel ou scientifique, de sabotage, d'atteintes à la réputation ou de débauchage d'experts* » et que « *la France [était] également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes* ».

Il en avait ainsi conclu que : « *Ces menaces sont de nature à justifier l'obligation de conservation généralisée et indifférenciée des données de connexion* », et qu'« *il ne ressort pas des pièces du dossier que la durée de conservation de ces données, fixée à un an, ne serait pas strictement nécessaire aux besoins de la sauvegarde de la sécurité nationale* ».

Ces menaces sont toujours le fondement du décret enjoignant aux opérateurs de conserver certaines données de trafic et les données de localisation.

*Source : commission des lois du Sénat*

### *D. DES INCERTITUDES PERSISTANTES*

Si plusieurs auteurs ont pu noter que le Conseil d'État avait « *sauvé l'essentiel du système français* » relatif à la conservation des données[1], certaines incertitudes demeurent.

Ainsi, dans le cadre de la lutte contre la criminalité grave, **les enquêteurs émettent une réquisition aux opérateurs les enjoignant à conserver temporairement des données ciblées, déjà conservées pour un autre motif**. Peuvent être concernées les données du suspect, de son entourage, des victimes, des témoins, ou encore des zones géographique déterminées dès lors qu'elles apparaissent utiles à la manifestation de la vérité. La chambre criminelle de la Cour de cassation a estimé, dans des arrêts en date du 12 juillet 2022[2], que les réquisitions délivrées dans le cadre des enquêtes pénales « *doivent être analysées comme valant injonction de conservation rapide* », lesquelles pouvant résulter d'injonctions de produire[3].

La méthode de la conservation rapide constitue donc en pratique, comme l'a souligné la direction des affaires criminelles et des grâces aux

---

[1] *Voir notamment l'article de Marie-Christine de Montecler, « Conservation des données : la guerre des juges n'aura pas lieu », Dalloz actualité, 29 avr. 2021 à propos de l'arrêt CE 21 avr. 2021, req. n° 93099.*

[2] *Cour de cassation, arrêts de la chambre criminelle du 12 juillet 2022, pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652. Une note explicative relative à ces arrêts est consultable sur le site de la cour de cassation.*

[3] *Cour de cassation, crim., 12 juillet 2022, n° 21-83.710 (§34).*

rapporteurs dans le cadre de leurs travaux, « *une modalité d'accès aux données de connexion déjà conservées pour d'autres finalités* ».

**La conformité de cette solution avec le droit européen n'est pas tranchée par la jurisprudence de la Cour de justice de l'Union européenne**. Ainsi, si le système français a été jugé compatible avec la jurisprudence de la Cour par le Président de cette dernière lors d'une audition de la commission des affaires européenne de l'Assemblée nationale le 18 mai 2021[1], la Cour n'en a pas moins précisé, dans ses arrêts du 5 avril 2022[2] et du 20 septembre 2022[3], que « *l'accès à des données relatives au trafic et à des données de localisation […] ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs* » et « *lorsque ces données ont exceptionnellement été conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale contre une menace qui s'avère réelle et actuelle ou prévisible […], les autorités nationales compétentes en matière d'enquêtes pénales ne sauraient accéder auxdites données dans le cadre de poursuites pénales, sous peine de priver de tout effet utile l'interdiction de procéder à une telle conservation aux fins de la lutte contre la criminalité grave* ». **Il en résulte clairement que la Cour interdit d'accéder à une donnée pour une finalité présentant un intérêt « inférieur » à celui de la finalité pour laquelle la donnée a été conservée initialement**.

Par ailleurs, la notion d'injonction de conservation rapide provient de la Convention de Budapest sur la cybercriminalité[4]. Celle-ci, notamment dans ses articles 16 et 17, **ne permet pas de savoir si cette injonction permet d'accéder aux données déjà conservées** ou n'autorise qu'une conservation pour l'avenir et pour une durée limitée.

**La Cour de justice de l'Union européenne ne s'est donc pas prononcée sur la portée exacte qu'elle entend conférer à l'injonction de conservation rapide**. En résumé, si elle prohibe clairement l'accès, pour les besoins de la lutte contre la criminalité, aux données conservées pour la sauvegarde de la sécurité nationale, **elle ne dit rien sur la possibilité d'ajouter, par le biais de l'injonction de conservation rapide, les besoins des enquêtes pénales aux finalités premières ayant justifié leur conservation**.

---

[1] *Le compte rendu de cette réunion est consultable sur le site de l'Assemblée nationale.*
[2] *Affaire C-140/20, Commissioner of the Garda Síochána e.a. (Dwyer).*
[3] *Affaires jointes C-793/19 et C-794/19, SpaceNet.*
[4] *Consultable sur le site : https://www.coe.int.*

## II. L'ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES : UNE PROCÉDURE ENCORE EN SUSPENS

### *A. LE RESPECT DES CRITÈRES PERMETTANT L'ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES : CRIMINALITÉ GRAVE, NÉCESSITÉ ET PROPORTIONNALITÉ*

#### 1. L'encadrement progressif par le législateur des infractions permettant un accès aux données de connexion dans le cadre des enquêtes pénales

Comme le relevait la commission des lois du Sénat dans son rapport en première lecture sur le projet de loi *relatif à la prévention d'actes de terrorisme et au renseignement*[1], si le dispositif adopté en 2021 préserve les capacités opérationnelles des services de renseignement, **il « *peut fragiliser les pouvoirs d'enquête en matière judiciaire* » puisqu'il marque un changement de taille : l'accès aux données de connexion, par le passé possible pour tout type d'enquête, se trouve restreint par le texte à la criminalité et à la délinquance graves.**

**Appelé à se prononcer sur la conformité à la Constitution de l'accès aux données de connexion sous l'angle du cadre juridique d'enquête**, le Conseil constitutionnel a considéré, par trois décisions rendues à la suite de questions prioritaires de constitutionnalité, que :

- la **réquisition des données de connexion prévue par les articles 77-1-1 et 77-1-2 du code de procédure pénale dans le cadre d'une enquête préliminaire était contraire à la Constitution** dans la mesure où elle pouvait porter sur tout type d'infraction et n'était ni justifiée par l'urgence ni limitée dans le temps : ainsi, bien que soumises à l'autorisation du procureur de la République, chargé de contrôler la légalité des moyens mis en œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits, cette possibilité n'était pas assortie de garanties suffisantes[2] ;

- à l'inverse, **la réquisition de données prévue par les articles 60-1 et 60-2 du code de procédure pénale était conforme à la Constitution**, notamment parce qu'elle était limitée aux cas d'enquêtes portant sur un crime flagrant ou un délit flagrant puni d'une peine d'emprisonnement et parce que la durée de cette enquête était limitée à 8 jours[3], offrant des garanties suffisantes et constituant une conciliation équilibrée entre l'objectif

---

[1] *Rapport n° 694 (2020-2021) de Marc-Philippe Daubresse et Agnès Canayer sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, déposé le 16 juin 2021.*

[2] *Conseil constitutionnel, décision n° 2021-952 QPC du 3 décembre 2021.*

[3] *Cette durée est renouvelable sur décision du procureur de la République, mais seulement dans l'hypothèse où l'enquête porte sur un crime ou un délit puni d'une peine d'emprisonnement égale ou supérieure à cinq ans et si les investigations ne peuvent être différées.*

de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée[1] ;

- **la réquisition de données de connexion prévue par les articles 99-3 et 99-4 du code de procédure pénale était également conforme à la Constitution**, dans la mesure où elle intervient à l'initiative du juge d'instruction, « *magistrat du siège dont l'indépendance est garantie par la Constitution* », ou d'un officier de police commis par lui, dans un cadre clairement défini (celui de l'information judiciaire) et dans les conditions précisément fixées par une commission rogatoire[2].

**En conséquence de la première décision, le législateur est intervenu pour restreindre l'accès aux données de connexion aux enquêtes pénales sur les cas les plus graves**. C'est ainsi que la loi n° 2022-299 du 2 mars 2022 *visant à combattre le harcèlement scolaire* a introduit un nouvel article 60-1-2 dans le code de procédure pénale. Cet ajout vise à répondre à la demande de garanties formulée par le Conseil constitutionnel en décembre 2021.

Ce nouvel article 60-1-2 du code de procédure pénale précise que **l'accès aux données de trafic et de localisation n'est possible** en enquête préliminaire, en enquête de flagrance et en enquête sur commission rogatoire**, à peine de nullité, que « *si les nécessités de la procédure l'exigent* » et dans quatre cas limitativement énumérés** :

- lorsque la procédure porte sur un **crime ou sur un délit puni d'au moins trois ans d'emprisonnement** ;

- lorsque la procédure porte sur un **crime ou un délit puni d'au moins un an d'emprisonnement**, que celui-ci a été **commis par l'utilisation d'un réseau de communication électronique** et que les réquisitions ont pour seul objet **d'identifier l'auteur de l'infraction** ;

- lorsque les réquisitions portent sur les **équipements de la victime** et interviennent **à la demande de celle-ci**, pour des délits punis d'une peine d'emprisonnement ;

- lorsqu'elles tendent à **retrouver une personne disparue ou à retracer un parcours criminel** pour un crime sériel ou non-élucidé.

Le Conseil constitutionnel, dans son commentaire de la décision QPC du 20 mai 2022[3], a souligné que les modifications réalisées par la loi n° 2022-299 du 2 mars 2022 *visant à combattre le harcèlement scolaire*, « ***ont eu pour objet de renforcer les garanties entourant la réquisition de données de connexion*** ».

---

[1] *Conseil constitutionnel, décision n° 2022-993 QPC du 20 mai 2022.*
[2] *Conseil constitutionnel, décision n° 2022-1000 QPC du 17 juin 2022.*
[3] *Consultable sur le site du Conseil constitutionnel.*

### 2. Les arrêts de la Cour de cassation du 12 juillet 2022 : l'institution d'un faisceau d'indices pour définir la criminalité grave

Appelée à se prononcer, la chambre criminelle de la Cour de cassation a estimé, dans des arrêts en date du 12 juillet 2022[1], que **l'accès aux données de connexion pour les besoins des enquêtes pénales n'est possible que pour les affaires relevant de la criminalité grave**, conformément aux exigences de la Cour de justice de l'Union européenne.

La Cour de cassation a précisé qu'en l'absence de définition nationale ou européenne de la notion de « *criminalité grave* », **il revenait au juge du fond la responsabilité d'examiner, au cas par cas, si la nature de l'infraction relevait de la « *criminalité grave* » au sens de la décision de la Cour de Luxembourg** et donc si elle justifiait un accès aux données de connexion. Selon la note explicative accompagnant les arrêts du 12 juillet 2022, cette appréciation doit notamment s'effectuer « ***au regard de la nature des agissements de la personne poursuivie, du montant du préjudice qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue*** »[2].

**Ces critères, qui constituent un faisceau d'indices, ne doivent cependant pas être interprétés comme étant cumulatifs**. Dès lors, la gravité de l'infraction réalisée est appréciée :

- d'une part, au regard de l'infraction visée et de la peine d'emprisonnement encourue ;

- d'autre part, au regard des circonstances de l'espèce, appréciation qui peut être faite au cas par cas en application des principes de nécessité et de proportionnalité.

À ce jour, la chambre criminelle de la Cour de cassation a ainsi jugé qu'entrent dans le champ de la criminalité grave, par exemple, « *les faits de trafic de stupéfiants au sein d'une maison d'arrêt et de corruption de fonctionnaires* »[3] ou encore les faits de « *banditisme violent, organisé et transfrontalier, association de malfaiteurs, détentions d'armes et explosifs en lien avec la possibilité préparation d'attaques* »[4].

Cependant, comme l'a rappelé son président, Nicolas Bonnal, aux rapporteurs, en l'état, **la seule qualification des faits ne peut suffire à établir la nécessité et la proportionnalité de l'accès aux données de connexion** : il appartient aux magistrats, y compris du ministère public,

---

[1] *Cour de cassation, arrêts de la chambre criminelle du 12 juillet 2022, pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652. Une note explicative relative à ces arrêts est consultable sur le site de la cour de cassasstion.*

[2] *Ainsi, le simple* quantum *de la peine encourue ne suffit pas à qualifier l'appartenance de l'infraction à la « criminalité grave ».*

[3] *Crim., 11 octobre 2022, n° 22-81.244.*

[4] *Crim., 15 novembre 2022, n° 21-87.449.*

d'exercer un contrôle de la nécessité du recours aux données de connexion au regard des circonstances de l'espèce.

**<u>Proposition n° 2 :</u> Intégrer dans le code de procédure pénale le faisceau d'indices retenu par la Cour de cassation pour définir la notion de « criminalité grave ».**

En renvoyant au parquet ou au juge d'instruction la responsabilité de rattacher l'infraction à la criminalité grave, cette jurisprudence a eu deux conséquences principales :

- d'une part, **une absence d'harmonisation dans les critères d'accès aux données de connexion, qui peuvent ainsi varier en fonction des Parquets**, lesquels peuvent réaliser un contrôle d'opportunité et de proportionnalité différent ;

- d'autre part, **un formalisme accru pour justifier et obtenir une autorisation d'accès aux données de connexion**, les enquêteurs devant désormais justifier de la nécessité et de la proportionnalité de l'acte envisagé au regard de la gravité de l'infraction et de l'intérêt de l'enquête.

**Le cas particulier des infractions liées à la sécurité nationale**

Dans ses arrêts du 12 juillet 2022, la Cour de cassation a considéré que « *l'obligation de conservation des données de trafic et de localisation imposée aux opérateurs par l'article L. 34-1, III, du code précité […], en ce qu'elle permet notamment la recherche, la constatation et la poursuite des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, infractions incriminées aux articles 410-1 à 422-7 du code pénal, est conforme au droit de l'Union, comme poursuivant l'objectif de sauvegarde de la sécurité nationale* ». **Il découle de cette jurisprudence que les enquêtes pénales pour des faits constituant une atteinte aux intérêts fondamentaux de la Nation ou des actes de terrorisme ne relèvent pas de la catégorie de la « *criminalité grave* »**, mais de la « *sauvegarde de la sécurité nationale* ». L'accès aux données de connexion pour ces enquêtes est donc possible, et ce sans passer par le biais d'une injonction de conservation rapide.

### 3. La criminalité grave : une notion dont l'appréciation doit continuer à relever du droit national

Tout l'enjeu réside ainsi, pour les services d'enquêtes et les procureurs, dans **ce que recouvre cette notion de « criminalité et délinquance graves »**, traduction législative française de la notion de « criminalité grave » utilisée par la Cour de justice de l'Union européenne. Cette dernière avait ainsi précisé, au point 135 de son arrêt *Quadrature du*

*net*[1], que la criminalité grave « [*correspondait] à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et [incluait] la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme* ». Cette définition a été reprise par le Conseil d'État au point 42 de son arrêt *French Data Network*, en date du 21 avril 2021. La commission des lois du Sénat avait également relevé, dans son rapport sur la loi n° 2021-998 du 30 juillet 2021 *relative à la prévention d'actes de terrorisme et au renseignement*, que la directive du 27 avril 2016 *relative à l'utilisation des données des dossiers passagers (PNR)* fixait le niveau de gravité par référence à une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans.

La Cour de cassation, dans ses arrêts du 12 juillet 2022, n'a pas souhaité fixer de seuil de peine d'emprisonnement pour rattacher une infraction à la criminalité grave. Elle considère que l'appréciation de cette notion « *relève du droit national* ». Cette solution est cohérente avec la position défendue par la France au sein des instances européennes. Le Gouvernement a ainsi soutenu dans le cadre de procédures préjudicielles que **la définition de la criminalité grave relève de la compétence des États membres et qu'elle doit pouvoir être principalement opérée par l'échelle des peines**.

Pour ce faire, le Gouvernement s'appuie sur les termes de l'article 83, paragraphe 2 du Traité sur le fonctionnement de l'Union européenne, qui dispose que c'est seulement dans les cas où l'harmonisation du droit pénal des États membres « *s'avère indispensable pour assurer la mise en œuvre efficace d'une politique de l'Union dans un domaine ayant fait l'objet de mesures d'harmonisation* » que l'Union peut adopter des directives visant à « *établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine concerné* ».

**La question du bon niveau de définition de la notion de criminalité grave semble toutefois diviser la Cour de justice de l'Union européenne elle-même**. Ainsi, dans ses conclusions rendues le 8 juin 2023 dans l'affaire *Tribunale di Bolzano*, l'avocat général Collins a souligné la nécessité de laisser aux législateurs nationaux le soin de définir la notion de criminalité grave, privilégiant une approche au cas par cas dans laquelle la juridiction ou l'autorité administrative indépendante chargée d'autoriser l'accès aux données doit exercer, d'une part, un contrôle objectif de l'appartenance d'une infraction, en vertu du droit national, à la catégorie de « criminalité grave » et, d'autre part, un contrôle *in concreto* de la

[1] *Cour de justice de l'Union européenne, arrêt « La Quadrature du net » du 6 octobre 2020 (affaires C 511/18, C 512/18 et C 520/18).*

proportionnalité de l'ingérence[1]. En revanche, les conclusions de l'avocat général Szpunar présentées le 27 octobre 2022 dans l'affaire *Quadrature du net* proposent que la notion de « criminalité grave » reçoive une interprétation autonome en droit de l'Union. Selon lui, une telle notion « *ne saurait dépendre des conceptions de chaque État membre sauf à permettre un contournement des exigences de l'article 15, paragraphe 1, de la directive 2002/58 selon que les États membres adoptent une conception extensive ou non de la lutte contre la criminalité grave* »[2]. Suite à la réouverture de la phase orale, les secondes conclusions de l'avocat général Szpunar présentées le 28 septembre 2023 maintiennent cette position mais de manière plus discrète, ce point n'étant abordé que dans une note de bas de page. L'avocat général envisage cependant la possibilité que la notion soit définie par les États membres, indiquant dans cette même note que « *même si la Cour venait à juger que la définition de la notion de 'criminalité grave' est laissée aux États membres, celle-ci devrait en tout état de cause être établie dans les limites du droit de l'Union et ne pourrait être étendue au point de vider cette disposition de sa substance* »[3]. **La solution de la Cour dans chacune de ces affaires est ainsi très attendue**, compte tenu notamment des négociations législatives en cours au sein du Conseil de l'Union européenne.

**<u>Proposition n° 3 :</u> Maintenir au niveau de chaque État membre la définition de ce que recouvre la « criminalité grave », sans en faire une notion autonome du droit de l'Union européenne.**

### *B. LA NÉCESSITÉ D'UN CONTRÔLE PRÉALABLE ET INDÉPENDANT*

#### 1. Les exigences posées par la CJUE

Par ses décisions successives, la Cour de justice de l'Union européenne a jugé que toute réquisition portant sur l'accès à des données de connexion devait être soumise au **contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant**. Tout au plus admet-elle qu'en cas d'urgence, ce contrôle intervienne *a posteriori*, pourvu que cela soit à bref délai (voir *supra*).

En toute hypothèse, l'autorité chargée du contrôle doit être **distincte et indépendante** de celle qui requiert l'accès aux données. Dans son arrêt *H.K. c/ Prokuratuur* du 2 mars 2021, elle a ainsi expressément jugé que le ministère public estonien, qui dirige la procédure d'enquête et exerce, le cas

---

[1] <u>Conclusions</u> *de l'avocat général Anthony M. Collins, présentées le 8 juin 2023 sur l'affaire C-178/22.*

[2] <u>Premières conclusions</u> *de l'avocat général Maciej Szpunar, présentées le 27 octobre 2022 sur l'affaire C-470/21.*

[3] <u>Secondes conclusions</u> *de l'avocat général Maciej Szpunar, présentées le 28 septembre 2023 sur l'affaire C-470/21.*

échéant, l'action publique, ne répondait pas aux conditions posées pour autoriser l'accès d'une autorité publique aux données de connexion.

### 2. Les conséquences qu'en a tirées la Cour de cassation

Par ses arrêts du 12 juillet 2022, la Cour de cassation a été invitée à tirer les conséquences de cette jurisprudence sur la conformité de la procédure pénale française à ces exigences.

À cette aune, elle a jugé que **le juge d'instruction**, qui non seulement n'est pas une partie à la procédure mais une juridiction, et de plus n'exerce pas l'action publique mais statue de façon impartiale sur le sort de celle-ci, **pouvait valablement contrôler l'accès aux données de connexion**. Si cette position, que certaines personnes entendues par les rapporteurs ont qualifiée de discutable - dès lors qu'il pourrait être objecté que le juge d'instruction n'est pas parfaitement extérieur à l'enquête qu'il contrôle -, est conforme à la conception française de la procédure d'instruction et aux garanties d'indépendance dont celle-ci est entourée, elle ne s'applique toutefois en pratique **qu'à une part infime des enquêtes pénales**, en général les plus complexes, du fait de la marginalisation progressive du recours à l'information judiciaire dans la justice pénale depuis de nombreuses années[1].

En revanche, et sans surprise au regard des décisions précitées, la Cour de cassation n'a pu que constater que **les dispositions du code de procédure pénale relatives aux enquêtes préliminaires et aux enquêtes en flagrance**, qui sont placées sous le seul contrôle du parquet et représentent l'immense majorité des enquêtes pénales aujourd'hui, **étaient contraires au droit de l'Union européenne** en ce qu'elles ne prévoient pas un contrôle préalable par une juridiction ou une entité administrative indépendante : le procureur de la République, qui dirige l'enquête, ne peut donc pas valablement contrôler l'accès aux données de connexion requis pour les besoins de celle-ci.

La Cour de cassation a toutefois jugé que cette absence de contrôle préalable indépendant n'entraînerait la nullité de la procédure réalisée dans ces conditions irrégulières **que si le requérant établit l'existence d'une ingérence injustifiée dans sa vie privée et dans ses données à caractère personnel**, c'est-à-dire s'il démontre qu'un contrôle préalable aurait permis de constater que les conditions de fond pour l'accès à ses données n'étaient pas réunies. Dans le cas contraire, en l'absence de ce préjudice, l'acte accompli sans le contrôle préalable indépendant requis par la jurisprudence de la Cour de justice **pourra être admis par la juridiction**.

---

[1] *D'après les chiffres publiés par le ministère de la justice, les parquets ont enregistré plus de 3 millions d'affaires nouvelles en 2021, quand les juges d'instruction ont été saisis d'un peu moins de 18 000 affaires cette même année, ce qui représente moins de 1% des affaires enregistrées par les parquets (source : Chiffres clés, édition 2022, publié sur le site Internet du ministère de la justice).*

### 3. Une position fragile

Cette position, dont Nicolas Bonnal, président de la chambre criminelle de la Cour de cassation, a rappelé qu'elle n'était que la déclinaison du principe « *pas de nullité sans grief* »[1], a été décriée tant par la doctrine que par une partie des magistrats.

Les représentants de la conférence nationale des procureurs de la République ont notamment insisté sur la position délicate dans laquelle ces décisions les placent, en les autorisant implicitement à continuer à requérir des données de connexion tout en jugeant expressément qu'une telle pratique n'est pas conforme au droit. Ces magistrats y voient à la fois une **source d'insécurité juridique** et une **négation des termes de leur serment**[2].

La doctrine, quant à elle, en a appelé **à une rapide clarification du droit par le législateur**[3]**.**

Au surplus, **la question reste posée de la possibilité, aux yeux de la CJUE, pour le juge d'instruction d'assurer ce même rôle de contrôle** des accès aux données de connexion dans la mesure où, bien que rattaché au siège, il ne saurait être vu comme indépendant vis-à-vis d'une enquête qu'il dirige.

---

[1] *En l'espèce, il s'agit de nullités qualifiées « d'intérêt privé ».*

[2] *Pour mémoire, tout magistrat, lors de sa nomination à son premier poste, et avant d'entrer en fonctions, prête serment en ces termes : "Je jure de bien et fidèlement remplir mes fonctions, de garder le secret des délibérations et de me conduire en tout comme un digne et loyal magistrat."*

[3] *Voir par exemple "Procédure pénale - Contrôle de l'accès aux données de connexion devant la chambre criminelle de la Cour de cassation. - Comment reprendre d'une main ce que l'on a donné de l'autre ! - Aperçu rapide par Antoine Botton" La Semaine Juridique - Édition générale n° 38 du 26 septembre 2022. Ou « L'accès aux données de connexion : les affres du pluralisme normatif », Amane Gogorza,LexisNexis Sa – Droit pénal, n°10, octobre 2022.*

# QUATRIÈME PARTIE
# AGIR EN FRANCE ET EN EUROPE POUR SÉCURISER LE RECOURS AUX DONNÉES DE CONNEXION DANS L'ENQUÊTE PÉNALE

Les rapporteurs estiment qu'il est **aujourd'hui du devoir du législateur d'apporter une réponse aux inquiétudes légitimes des acteurs de l'enquête en remettant à plat le sujet des données de connexion.** Cette entreprise ne saurait s'apparenter à une codification docile de la jurisprudence de la CJUE, notamment au vu des incertitudes sur le devenir à terme de ses positions et de la nécessité pour l'État d'exercer pleinement les compétences qui lui sont confiées à titre exclusif par les traités européens. Ils proposent ainsi de **faire évoluer notre droit national pour mieux encadrer la procédure d'accès aux métadonnées, tout en adoptant en matière de conservation une approche réaliste et pragmatique**.

Pour autant, **le législateur n'est pas le seul à devoir intervenir pour redonner aux acteurs de l'enquête en France les moyens d'exercer sereinement leurs missions.** Le Gouvernement, en sa double qualité de porte-parole des institutions nationales auprès de l'Union européenne et de responsable de l'administration de la justice, de la police et de la gendarmerie, doit lui aussi se saisir du sujet et de tous ses enjeux.

## I. AGIR EN EUROPE DANS LE SENS D'UN PLUS GRAND PRAGMATISME

Les rapporteurs plaident, tout d'abord, pour une **action déterminée de la France à l'échelle européenne** afin d'obtenir une meilleure prise en compte des besoins opérationnels des services d'enquête – qui, eux-mêmes, sont les reflets des attentes des citoyens en matière de sécurité publique.

### *A. PLAIDER POUR UNE MEILLEURE PRISE EN COMPTE DES BESOINS OPÉRATIONNELS DES SERVICES D'ENQUÊTE*

#### 1. Assumer une position forte dans les négociations européennes

Il est, en premier lieu, essentiel que la France assume une position forte dans les négociations européennes qui portent sur l'usage des outils numériques en matière pénale. Le risque, pointé par les interlocuteurs des rapporteurs à Bruxelles comme par de nombreuses personnes auditionnées à Paris, est en effet non seulement de voir le droit européen évoluer dans le sens d'une codification de la jurisprudence actuelle de la CJUE, mais aussi que la structuration des débats dans les institutions européennes et au sein de la Cour conduise à dissocier le cadre juridique de la lutte contre la cyber-délinquance de celui applicable aux autres infractions, en prévoyant dans le premier cas un usage peu régulé des données de connexion – comme en

témoignent les derniers développements intervenus dans le dossier « Hadopi » - et, pour le second, une rigidité de plus en plus marquée en matière d'utilisation des preuves numériques.

À cet égard, les rapporteurs relèvent que, si de nombreuses personnes auditionnées ont estimé que la position de la CJUE s'expliquait par le fait que ses membres n'avaient pas été suffisamment sensibilisés par les États et par les services nationaux de police judiciaire et de renseignement aux réalités du terrain - donc *in fine* par une forme d'ignorance de la « vraie vie » des enquêteurs et des pratiques des délinquants -, cette analyse ne semble pas étayée par les faits : **en amont de chacun des arrêts les plus marquants, une vingtaine d'États membres ont formulé des observations auprès des juges de Luxembourg** afin de faire valoir les contraintes et les besoins des services nationaux d'enquête pénale.

Les arrêts de la CJUE se fondent, comme on l'a vu, sur la Charte des droits fondamentaux de l'Union européenne ; elles procèdent donc d'un texte ayant la même valeur juridique que les traités européens. Face à ce constat, **certaines des personnes entendues ont suggéré que soit adopté un protocole interprétatif** précisant que, dans l'intention des États membres, les dispositions des articles 7, 8 et 11 de la Charte en matière de protection des données personnelles doivent, en matière pénale, être conciliées avec des impératifs dont les États sont les garants et qui échappent à la compétence de l'Union, ce qui impliquerait par ailleurs de restaurer la pleine compétence des autorités nationales pour assurer cette conciliation.

**Un tel protocole supposant, de même que les traités eux-mêmes, une unanimité des États membres, cet objectif semble toutefois difficilement atteignable**.

À l'inverse, la piste consistant à faire évoluer la réglementation *e-privacy* pour exclure expressément de son champ d'application les activités de recherche et de répression des infractions pénales (voir ci-avant) doit être privilégiée : la réécriture engagée depuis 2017 est en effet de nature à faire passer un message clair et à susciter un revirement de jurisprudence. Il est également possible que, comme elle l'a fait par le passé en invalidant une directive de 2006 sur la conservation des données[1], la Cour considère que cette modification doit être censurée en raison de sa contrariété avec la Charte. Pour autant, les rapporteurs soulignent que **la nouvelle réglementation *e-privacy* est le seul vecteur disponible à ce jour pour envisager une remise à plat des principes de conservation des données de connexion et d'accès à celles-ci** : le sujet doit donc être au cœur des

[1] *L'arrêt Digital Rights ltd. de 2014, déjà abondamment cité, conclut en effet à l'invalidation de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.*

préoccupations de la France et des autres États membres qui partagent sa volonté de garantir une répression effective des infractions pénales.

Dans ce contexte, on ne saurait se contenter d'espérer que la jurisprudence connaisse une inflexion sous l'effet d'efforts supplémentaires de pédagogie ou d'une convergence naturelle des points de vue. Il appartient aux gouvernements des États concernés, et notamment aux ministres français de l'intérieur et de la justice, de **faire du sujet des données de connexion une véritable priorité dans l'agenda des négociations**. Concrètement, les rapporteurs estiment ainsi que le Gouvernement devrait œuvrer à bâtir une majorité au sein du Conseil et mener un travail d'influence auprès de la Commission et du Parlement européen pour **obtenir l'aboutissement rapide et concluant des négociations sur le texte *e-privacy* 2, en particulier pour confirmer l'exclusion du périmètre du futur règlement des données exploitées dans un cadre pénal.** Il pourrait, à cet égard, profiter de la double échéance de l'installation d'une nouvelle Commission après les élections européennes de 2024 et de l'aboutissement des travaux du HLEG sur les données de connexion en juin de la même année **pour prendre l'initiative d'une relance du trilogue au printemps prochain**.

### 2. Renforcer la transparence du processus européen

Les rapporteurs appellent également de leurs vœux un renforcement de la transparence du processus européen de décision sur les données de connexion, processus dont les parlements nationaux sont en l'état largement exclus.

Il leur semble à ce titre nécessaire que **les assemblées françaises soient mieux associées à l'établissement des observations présentées par la France dans le cadre de l'examen par la CJUE de questions préjudicielles portant sur l'usage des métadonnées en matière pénale** – et, plus largement, sur l'ensemble des thématiques ayant un impact lourd sur des sujets majeurs et de nature à se traduire par une modification de textes de niveau législatif. Cette recommandation s'inscrit dans la droite ligne du rapport sénatorial « Judiciarisation de la vie publique : le dialogue plutôt que le duel »[1], qui soulignait déjà qu'*« il serait pertinent que le Sénat - tout comme l'Assemblée nationale - puisse apporter sa contribution à la position française devant la CJUE en cas de contentieux relatif à l'interprétation d'une norme européenne dans le cadre d'un renvoi préjudiciel ou d'un recours en manquement […] afin d'éclairer la Cour sur les effets concrets de telle ou telle disposition en France et de faire entendre son point de vue dans les contentieux pendants devant la CJUE considérés comme stratégiques* ». Le même rapport proposait que la définition des contentieux stratégiques soit faite « *soit en fonction des travaux de la commission des affaires européennes du Sénat, première vigie de la Haute Assemblée sur l'actualité*

[1] Rapport d'information n° 592 (2021-2022) *de Philippe Bonnecarrère, au nom de la mission d'information sur la judiciarisation de la vie publique, déposé le 29 mars 2022.*

*européenne, soit en fonction de signalements du ministère de l'Europe et des affaires étrangères* » : cette proposition n'a rien perdu de son actualité, et il semble évident que **les données de connexion constituent un sujet « stratégique » auquel le Parlement doit être étroitement associé.**

Les rapporteurs estiment de même, indispensable **que le Gouvernement rende régulièrement compte au Parlement des échanges menés dans le cadre du groupe d'experts de haut niveau ADELE ou *Going dark*** afin de permettre aux parlementaires non seulement d'être informés de l'avancée des réflexions mais aussi (voire surtout) de se faire entendre dans ce débat crucial.

> **Proposition n° 4 : Obtenir du Gouvernement qu'il rende compte au Parlement des échanges menés dans le cadre du groupe d'experts de haut niveau *Going dark*.**

### *B. ŒUVRER AU DÉVELOPPEMENT DES « SOUPAPES » OUVERTES PAR LA COUR DE LUXEMBOURG ET MIEUX LES INTÉGRER AU DROIT INTERNE*

Si elle demeure contestée, la jurisprudence de la CJUE ménage d'ores et déjà des « soupapes » bienvenues qu'il convient de mieux intégrer à notre droit interne.

La première d'entre elles porte sur la **différence de régime juridique entre les infractions commises dans le monde physique et les infractions commises en ligne.** Déjà consacrée par le droit français, la souplesse accordée aux services d'enquête en matière d'accès aux métadonnées dans la lutte contre la cyber-délinquance (pour mémoire, l'article 60-1-2 du code de procédure pénale prévoit la possibilité d'accéder aux données d'identification pour la recherche des auteurs d'infractions dès lors que celles-ci sont passibles d'au moins un an d'emprisonnement, contre trois ans pour les autres infractions, et qu'elles ont été « *commis[es] par l'utilisation d'un réseau de communications électroniques* ») pourrait en effet se voir renforcée par l'arrêt de la CJUE dans l'affaire « Hadopi », l'avocat général Szpunar ayant plaidé, dans de nouvelles conclusions présentées le 28 septembre dernier, pour « *un développement de la jurisprudence nécessaire et limité* » consistant à autoriser une conservation générale et indifférenciée des adresses IP, notamment parce que celles-ci constituent le seul moyen d'investigation permettant l'identification des personnes auxquelles elles étaient attribuées au moment de la commission de l'infraction. Au surplus, l'avocat général a recommandé que soit reconnue la possibilité d'un accès aux adresses IP **sans contrôle préalable indépendant** et **pour « *toutes les***

***infractions commises exclusivement en ligne*** », donc y compris celles qui ne tombent pas dans la catégorie de la « criminalité grave »[1].

À supposer qu'elles soient suivies par la grande chambre de la CJUE, ces conclusions viendraient donner de nouvelles marges de manœuvre aux services d'enquête et il conviendrait de les répercuter au sein du code de procédure pénal français, puisqu'elles apparaissent ouvrir un champ d'accès plus large que celui qui a été ménagé par le législateur à compter de 2022. Plus encore, cette évolution pourrait inciter le Parlement à reconsidérer le statut des adresses IP dans la nomenclature des données de connexion, faisant de celles-ci une donnée « hybride » entre identification et trafic, permettant peut-être qu'elles soient plus facilement exploitées au cours des enquêtes pénales[2].

> **Proposition n° 5 : Tirer profit des éventuelles évolutions de la position de la CJUE pour, d'une part, renforcer les souplesses d'accès aux données de connexion en matière de lutte contre les infractions commises en ligne et, d'autre part, envisager un assouplissement du régime d'accès aux adresses IP.**

## II. ADAPTER LES NORMES FRANÇAISES À L'IMPÉRATIF D'UN CONTRÔLE PRÉALABLE DES ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES

### *A. EN FRANCE, UN FORT SENTIMENT D'INSÉCURITÉ JURIDIQUE DES ACTEURS DE L'ENQUÊTE*

**Les interrogations qui demeurent quant à la conformité du droit national au droit de l'Union européenne conduisent à un fort sentiment d'insécurité de la part de l'ensemble des acteurs de l'enquête** : policiers, gendarmes et procureurs de la République essentiellement. Ceux-ci attendent, légitimement, une stabilisation du droit européen et une intervention du législateur français afin de définir les lignes à suivre s'agissant de l'usage des données de connexion dans le cadre des enquêtes pénales.

Ainsi, à la suite des arrêts de la chambre criminelle de la Cour de cassation, la conférence nationale des procureurs de la République a dressé le constat de « *l'insécurité juridique majeure à laquelle doit faire face la*

---

[1] *Les conclusions citées sont accessibles sur l site : https://curia.europa.eu*

[2] *Cette position est celle qui semble avoir été adoptée par le Portugal, dont le Tribunal constitutionnel a jugé le 19 avril 2022 que «* la conservation des adresses IP dynamiques ne constituait pas une ingérence aussi grave que la conservation des données de trafic » *ouvrant la voie à l'aménagement de leur régime de conservation (source : réponse écrite du SGAE au questionnaire des rapporteurs).*

*lutte contre toutes les formes de délinquance* », la téléphonie étant « *un facteur central dans l'élucidation des affaires, un outil d'enquête tout autant à décharge qu'à charge […] une technique d'enquête utilisée quotidiennement par les parquets et les services enquêteurs* ». « *L'impossibilité dans laquelle se trouvent désormais les parquets et les services de police et de gendarmerie de recourir à ces investigations, en dehors du périmètre de la criminalité grave, ainsi que l'absence de définition objective de cette même notion, constituent des obstacles majeurs à l'identification des délinquants et des criminels* »[1].

**Ces inquiétudes conduisent à de grandes disparités de l'usage des données de connexion dans les enquêtes pénales**. Les procureurs de la République ont adapté leurs instructions en la matière, mais l'on remarque une absence d'harmonisation sur le territoire national. Certains magistrats du parquet refusent ainsi de se retrouver en situation d'ordonner des actes d'enquête selon une procédure déclarée contraire au droit de l'Union européenne, alors même que leur mission est d'appliquer et de faire appliquer le droit. D'autres demandent désormais aux enquêteurs de justifier davantage leurs demandes, aggravant d'autant la charge pesant sur les services exerçant des missions de police judiciaire. D'autres enfin n'ont pas modifié leurs pratiques.

Ces disparités interrogent quant à l'égalité de traitement de nos concitoyens dans le cadre des enquêtes pénales et sont source d'insécurité juridique et de complexité pour les enquêteurs qui peuvent avoir affaire à différents parquets devant lesquelles les façons de procéder divergent.

Les procureurs de la République se sentent également dépossédés, rappelant **qu'ils accomplissent au quotidien, dans leur mission de direction des enquêtes, un contrôle de nécessité et de proportionnalité sur les actes d'enquête** et qu'ils sont chargés, en vertu de l'article 39-3 du code de procédure pénale, **d'enquêter tant à charge qu'à décharge**, dans le respect des droits de la victime, du plaignant et de la personne suspectée.

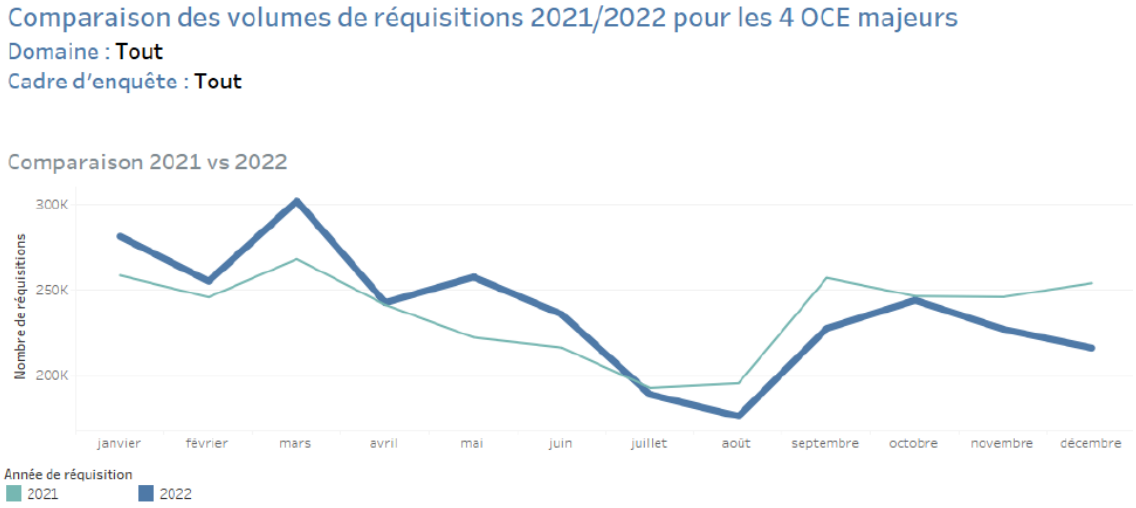
**De manière générale, les arrêts de la chambre criminelle de la Cour de cassation ont eu un effet notable sur l'évolution du nombre de réquisitions dans le cadre des enquêtes pénales**. Ainsi, alors que le nombre de réquisitions augmentait d'environ 10 % chaque année[2] et que le début de l'année 2022 suivait la même tendance, le nombre total de réquisitions portant sur les données d'identification, de trafic et de localisation s'est élevé à 2 849 125 en 2022 contre 2 838 989 en 2021, soit une hausse de 0,36 %, très

---

[1] *Communiqué de presse du conseil d'administration de la Conférence nationale des procureurs de la République, sur les conséquences des arrêts de la Cour de cassation relatifs aux donnes de connexion pour la lutte contre la délinquance, 15 juillet 2022.*

[2] *Hors crise sanitaire, les demandes de données de connexion ont ainsi connu une croissance continue au cours des dernières années. Cette croissance s'explique par le recours de plus en plus systématique à la preuve numérique dans une société elle-même numérique, et par la facilité d'usage permise par la plateforme nationale des interceptions judiciaires (PNIJ).*

éloignée des hausses constatées les années précédentes[1]. Depuis juillet 2022, le nombre de réquisitions a toujours été inférieur à celui des années précédentes.




*Source : direction des affaires criminelles et des grâces*

Conscient de ces difficultés, le Gouvernement a chargé Alexandre Lallet, rapporteur public du Conseil d'État sur la décision *French data network* du 21 avril 2021, d'une mission sur les conditions d'accès aux données de trafic et de localisation par les acteurs de l'enquête pénale. Ce dernier devra rendre ses conclusions d'ici au début de l'année 2024.

Les rapporteurs considèrent que **ces incertitudes et disparités plaident pour une évolution de la législation française afin d'y mettre fin et de définir des lignes claires d'usage des données de connexion dans les enquêtes pénales.** La question principale est celle de la **temporalité de cette évolution**. Celle-ci devra être suffisamment rapide au regard des risques que fait actuellement peser sur les procédures l'existence d'un contrôle seulement *a posteriori*, tout en s'inscrivant dans un temps suffisamment long afin que l'institution d'un nouveau contrôle, cette fois *a priori*, puisse être rendue réalisable par le déploiement d'outils informatiques permettant d'en limiter les effets pratiques pour les enquêteurs. Les rapporteurs estiment ainsi **réaliste et souhaitable une évolution de la législation à un horizon de deux ou trois ans**.

**L'évolution de la législation sur ce sujet gagnerait de fait à s'inscrire dans le cadre de la clarification et la restructuration du code de procédure pénale** envisagée par le projet de loi *d'orientation et de programmation du ministère de la justice 2023-2027*. Les rapporteurs considèrent en effet nécessaire qu'une véritable évolution du code de procédure pénale intervienne, ce qui revient à s'inscrire dans un mouvement de réforme et non une simple refonte.

[1] *Selon les informations transmises par la direction des affaires criminelles et des grâces aux rapporteurs dans le cadre de leurs travaux.*

### *B. ADAPTER LES MODALITÉS DE CONTRÔLE DE L'ACCÈS AUX DONNÉES DE CONNEXION AUX CONTRAINTES DU TERRAIN*

#### 1. Un contrôle exigeant

La jurisprudence de la Cour de justice de l'Union européenne exige qu'un contrôle préalable aux demandes d'accès aux données de connexion dans le cadre des enquêtes pénales soit réalisé. **Elle réserve cependant aux demandes d'accès aux données de trafic et de localisation l'exigence d'un contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant**.

Dans ces conditions, et par analogie avec le règlement *e-evidence*[1], il semble possible de permettre au parquet d'exercer le contrôle des demandes d'accès aux données d'identification. Ces accès, dont le nombre s'est élevé à 945 432 en 2022 contre 1 029 153 en 2021[2], présentent en effet une atteinte moindre à la vie privée puisqu'ils **ne permettent pas de retracer les contacts et les trajets des personnes**.

De la même manière, et sous réserve de l'arrêt qui sera rendu en fin d'année 2023 ou en début d'année 2024 par la Cour de justice de l'Union européenne dans le cadre de l'affaire dite « Hadopi », il paraît possible de **prévoir le même mécanisme de contrôle par le Parquet pour l'accès aux adresses IP dans le cadre d'infractions commises en ligne, dès lors que l'accès à ces données est le seul moyen d'identifier l'auteur de l'infraction**. Cette solution suivrait les préconisations de l'avocat général Szpunar dans ses conclusions rendues le 28 septembre 2023[3].

> **Proposition n° 6 : Permettre au parquet d'exercer le contrôle des demandes d'accès aux données de connexion aux seules fins d'identification.**

---

[1] *Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale.*

[2] *Selon la direction des affaires criminelles et des grâces.*

[3] *Secondes conclusions de l'avocat général M. Maciej Szpuna, présentées le 28 septembre 2023 sur l'affaire C-470/21.*

### 2. Un contrôle pleinement conforme aux exigences de la CJUE

La Cour de justice de l'Union européenne esquisse deux pistes dans l'élaboration d'un contrôle *a priori* pour l'accès aux données de connexion dans le cadre des enquêtes pénales : un contrôle par une autorité indépendante dotée d'un pouvoir contraignant. Cette autorité de contrôle serait chargée de vérifier *a priori* que l'accès à ces données s'effectue bien dans le respect des critères définis par la Cour, c'est-à-dire qu'il concerne des affaires liées à la « criminalité grave », et qu'il est nécessaire et proportionné aux exigences de l'enquête.

Les rapporteurs ont souhaité explorer l'ensemble des pistes envisagées par la Cour de justice afin de déterminer laquelle était la mieux adaptée à notre système juridique et judiciaire.

*a) La piste d'un contrôle par une entité indépendante*

S'agissant du contrôle exercé par une autorité indépendante, plusieurs hypothèses ont été évoquées à l'occasion des travaux des rapporteurs.

La première est celle d'une autorité **administrative** indépendante, qui serait chargée de rendre des avis sur les demandes d'accès aux données de connexion dans le cadre des enquêtes pénales. **En raison du principe de séparation des pouvoirs, seule une procédure d'avis serait juridiquement envisageable,** sur le modèle de la commission nationale de contrôle des techniques de renseignement. En cas d'avis favorable, l'autorisation serait réputée accordée. En cas de doute ou d'avis défavorable à l'inverse, la demande serait transmise à un juge chargé d'effectuer un contrôle et d'autoriser ou de refuser l'accès demandé. Cette solution présente toutefois une faiblesse insurmontable : son **absence probable de conformité à la jurisprudence de la Cour de justice de l'Union européenne** qui exige un contrôle préalable obligatoire et systématique. Par ailleurs, une telle solution souffrirait sans doute d'une faible acceptabilité de la part des magistrats.

La seconde piste de réflexion évoquée est celle d'une **autorité nationale indépendante, composée de magistrats** et éventuellement rattachée à la Cour de cassation. Les rapporteurs ont cru devoir également éloigner cette solution. Celle-ci ne serait pas opérationnellement viable en raison, d'une part, des moyens à engager pour mettre en œuvre une telle proposition, s'agissant tant des effectifs que des moyens informatiques et, d'autre part, de la nécessité de conserver une proximité dans la connaissance des dossiers entre l'autorité de contrôle, les services d'enquête demandeurs et les autorités de direction d'enquête.

Une troisième piste de réflexion consiste à rattacher ce contrôle à l'**agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ)**, déjà chargée de la mise en œuvre de la plate-forme nationale des interceptions judiciaires (PNIJ). Cette agence pourrait en effet intégrer un

contrôle au sein de la mise en œuvre de la plateforme. Cette solution se heurte cependant aux mêmes objections que la précédente, et fait également peser des risques organisationnels, informatiques et techniques sur la plateforme elle-même alors que le bon fonctionnement de l'outil est aujourd'hui salué par l'ensemble des services d'enquête.

Enfin, une dernière piste de réflexion évoquée a été celle d'une **autorité indépendante locale rattachée au parquet** – par exemple au procureur général qui est chargé de par la loi de la surveillance des enquêtes. Si cette solution a l'avantage de maintenir une certaine proximité entre l'autorité de contrôle et le service demandeur, elle se heurte au **risque de contrariété à la jurisprudence de la Cour de justice de l'Union européenne**. En étant rattachée au parquet en effet, qui a un rôle soit de direction des enquêtes soit de surveillance des enquêtes – selon qu'il s'agit du procureur de la République ou du procureur général –, les rapporteurs considèrent qu'il existe une forte probabilité que la Cour considère cette autorité comme étant impliquée dans la conduite de l'enquête pénale en cause, alors que la non-implication dans l'enquête est une condition posée par sa jurisprudence[1].

*b) La piste d'un contrôle par une juridiction*

Les rapporteurs considèrent en conséquence **plus pertinente, crédible et réaliste la piste d'un contrôle préalable exercé par une juridiction**. Dans le système judiciaire français, un juge, le juge des libertés et de la détention, dispose déjà de prérogatives en matière de protection la liberté individuelle. Il est ainsi chargé, dans la procédure pénale, d'autoriser certaines mesures d'enquêtes particulièrement attentatoires aux libertés.

**Ajouter le contrôle des autorisations d'accès aux données de connexion, en particulier aux données de trafic et de localisation, aux compétences du juge des libertés et de la détention s'inscrirait ainsi dans la logique des prérogatives déjà attribuées à cette entité**. Cette solution paraît aux rapporteurs être la réponse la plus forte quant aux exigences de la jurisprudence de la Cour de justice de l'Union européenne et la plus conforme avec notre logique judiciaire nationale.

Elle s'inscrirait en sus dans le mouvement actuel de **recentrage du juge de la liberté et de la détention sur ses compétences en matière de procédure pénale**. Le projet de loi *d'orientation et de programmation du*

[1] *Dans son arrêt dit « Prokuratuur » du 2 mars 2021 (C-746/18), la Cour indique en effet que* « l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable […] impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique […] que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale ».

*ministère de la justice 2023-2027* a ainsi transféré les compétences civiles exercées par le juge des libertés et de la détention en matière de contentieux des étrangers et d'hospitalisations sous contrainte à un magistrat du siège du tribunal judiciaire.

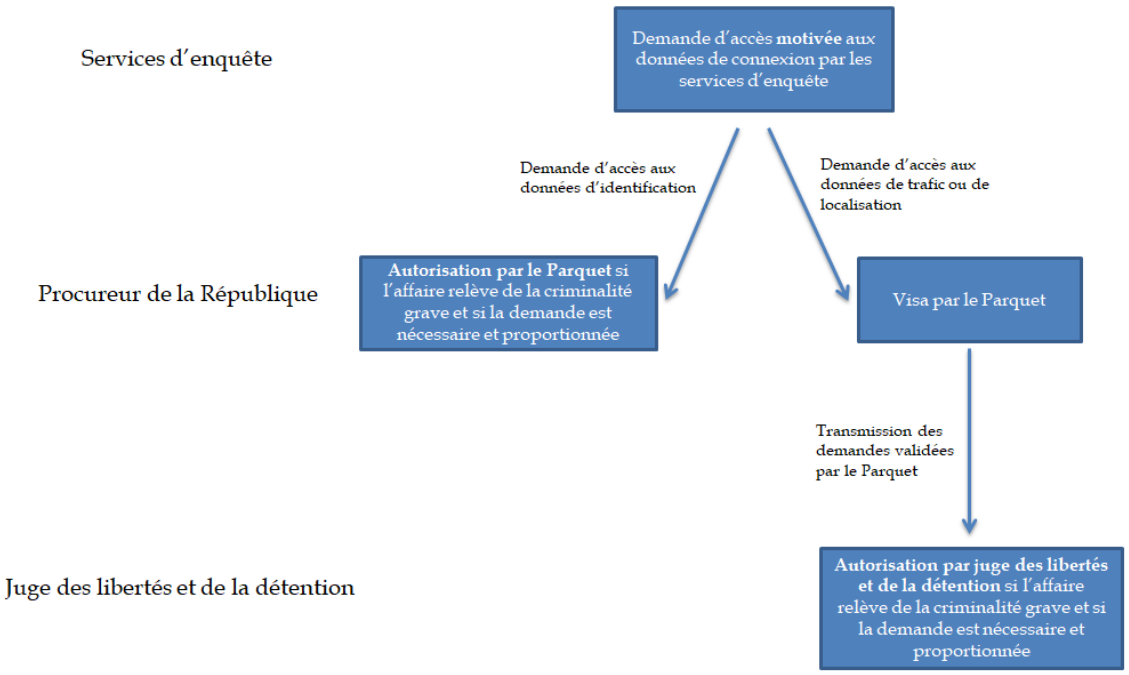
**Cette solution n'est cependant pas sans soulever de nombreuses questions**. Toutes ont trait à la capacité des juges des libertés et de la détention à faire face à ce nouveau contrôle, qui s'annonce massif, dans un contexte de désaffection de cette fonction : même si le présent rapport comporte des pistes pour limiter la charge induite par le contrôle de l'accès aux données de connexion, celui-ci demeurera une mission nouvelle qui viendra s'ajouter aux tâches déjà exercées par les magistrats et se traduira inévitablement par un besoin en effectifs qu'il sera nécessaire de quantifier en fonction des arbitrages finalement rendus.

Il convient ainsi de **se donner le temps de construire les outils nécessaires au bon traitement de ce contrôle** par les juges des libertés et de la détention, en lien avec le parquet et les services d'enquête.

De nombreuses réponses devront encore être apportées, s'agissant du **périmètre du contrôle effectué** (étendu à l'ensemble des demandes d'accès aux données de connexion ou restreint aux demandes d'accès aux données de trafic et de localisation), **de celui des autorisations** (données par ligne ou par enquête, voire les deux) ou encore du **système informatique pouvant être adopté**. S'agissant de ce dernier point, les rapporteurs considèrent que le plus efficace et adapté serait la conception d'un système informatique reliant services d'enquête, procureurs et juges des libertés et de la détention, dans lequel les services d'enquêtes effectueraient une demande motivée d'accès aux données de connexion qui serait transmise au parquet. Ce dernier l'autoriserait dans le cas des demandes d'accès à des données d'identification, tandis qu'il donnerait un avis sur les demandes d'accès aux données de trafic et de localisation. Les demandes validées par le parquet seraient alors transmises au juge des libertés et de la détention qui se chargerait de les autoriser.

**Ce système informatique de visas** (dont les modalités de fonctionnement concret et l'interaction avec d'autres applicatifs ou d'autres chantiers informatiques en cours sont détaillées dans le III ci-après) **aurait deux avantages principaux** : la rapidité et **l'allègement de la charge procédurale**, d'une part, et la **traçabilité des demandes et autorisations accordées**, d'autre part. Cela représenterait en effet un véritable gain de temps pour les parquets, temps qui pourrait être réinvesti dans leurs missions de direction et de contrôle des enquêtes.

**Schéma du système proposé de demandes d'accès aux données de connexion dans le cadre des enquêtes pénales**




*Source : Commission des lois du Sénat*

**De ces réponses dépendra le nombre de juges des libertés et de la détention à mobiliser et l'organisation qui devra être choisie pour assurer ce contrôle massif**.

Dans l'attente, les rapporteurs n'ont pas souhaité trancher pour une organisation particulière, plusieurs solutions étant envisageables. La première est d'**attribuer cette mission aux juges locaux des libertés et de la détention**, la seconde consiste à **créer un groupement dédié de juges des libertés et de la détention placé auprès de la Cour d'appel**. Ce rattachement permettrait d'exercer un roulement parmi les juges des libertés et de la détention du ressort, tout en assurant que l'interlocuteur exerçant le contrôle des demandes connaisse les enjeux locaux.

> **<u>Proposition n° 7 :</u> Attribuer la mission de contrôle des accès aux données de connexion au juge des libertés et de la détention.**

### 3. Des modalités de contrôle pragmatiques

**Quelle que soit l'organisation retenue, les modalités de contrôle devront être pragmatiques**. En particulier, et compte tenu des délais nécessairement plus longs qu'aujourd'hui dans lesquels s'inscrira la procédure d'autorisation d'accès aux données de connexion, les rapporteurs considèrent qu'**une procédure d'urgence devra être préservée**.

Ainsi, **en cas d'urgence, les services d'enquêtes devront pouvoir obtenir un accès aux données de connexion après autorisation du Parquet, le contrôle par l'autorité compétente** – dans le schéma défini par les rapporteurs, par le juge des libertés et de la détention – **étant réalisé *a posteriori*.** Si le contrôle réalisé *a posteriori* devait conclure à l'absence de correspondance de la demande aux critères gouvernant l'accès aux données de connexion – criminalité grave, nécessité et proportionnalité –, l'accès devrait être interrompu et les données obtenues supprimées sans délai.

Il convient de souligner que cette possibilité d'accès en urgence, conduisant à ce que le contrôle soit réalisé *a posteriori*, est ouverte en matière de preuve numérique par le projet de règlement européen *e-evidence* précité et est prévu par de nombreux États membres.

Les rapporteurs considèrent que **la définition de l'urgence devrait se rapprocher de sa définition nationale**[1], c'est-à-dire « *résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens* »[2].

**<u>Proposition n° 8 :</u> Prévoir, en cas d'urgence, la possibilité d'un accès aux données de connexion avec une autorisation *a posteriori*.**

### *C. UNE OPPORTUNITÉ POUR UNE REFONTE DU CADRE DE LA PREUVE*

De façon plus générale, plusieurs personnes entendues par la mission ont souhaité rappeler que les données de connexion, si elles font l'objet d'un cadre juridique spécifique posé par la Cour de justice, ne sont pour autant qu'une catégorie parmi d'autres de preuves numériques (réquisitions de téléphones, perquisitions informatiques, recours à des « *IMSI catchers* », *etc.*), lesquelles ne sont elles-mêmes qu'un sous-ensemble dans l'ensemble des modes de preuves admis par le code de procédure pénale. Soulignant la montée en puissance du recours aux preuves numériques, au détriment des preuves « physiques » (recueil de témoignages, analyses ADN, aveux, *etc.*), Benoît Auroy, en particulier, a regretté l'absence de régime juridique unifié et plaidé pour la mise en œuvre, *a minima*, **d'un régime commun applicable à l'ensemble des preuves numériques**.

Cette fragmentation du régime juridique de la preuve pénale doit être mise en rapport avec la multitude de réformes intervenues depuis une quinzaine d'années pour adapter au coup par coup les dispositions du

---

[1] *Par opposition à la définition européenne,* « en cas de menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne ou d'une infrastructure critique, ou en cas de risque pour l'intégrité des données », *définition présente dans* e-evidence.

[2] *Article 230-35 du code de procédure pénale.*

code de procédure pénale aux exigences posées par la Cour européenne des droits de l'homme, la Cour de justice de l'Union européenne et le Conseil constitutionnel s'agissant du contrôle des enquêtes par le ministère public. Ces réformes ont conduit à confier le contrôle ou la validation d'un nombre croissant de décisions **au juge des libertés et de la détention**, sans vision globale sur les tâches dévolues à ce dernier. Tout au plus le projet de loi *d'orientation et de programmation du ministère de la justice 2023-2027* a-t-il prévu, suivant la recommandation formulée par le rapport du comité des États généraux de la justice[1], de recentrer les missions du juge des libertés et de la détention sur le pénal.

Comme l'a souligné Nicolas Bonnal, président de la chambre criminelle de la Cour de cassation, peut-être est-il temps de replacer le sujet des données de connexion dans une approche plus globale d'une procédure pénale fondée, pour ce qui ne concerne pas les informations judiciaires, **sur une articulation mieux établie entre le ministère public, directeur de l'enquête, d'une part, et le juge des libertés et de la détention, chargé du contrôle des actes les plus intrusifs ou attentatoires aux libertés, d'autre part**, et de passer ainsi de ce qu'il a appelé « une logique de guichet » à « une logique de cabinet ». Les rapporteurs n'ignorent pas que cette perspective rejoint la réflexion, engagée de longue date[2] mais à ce jour inaboutie, **sur la création d'un véritable juge de l'enquête et des libertés**, dont la commission des lois, dans un rapport co-signé par Jean-René Lecerf et Jean-Pierre Michel en décembre 2010, avait tracé les contours[3].

> **Proposition n° 9 : En cas de choix du juge des libertés et de la détention pour contrôler l'accès aux données de connexion, engager une réflexion sur le statut et les missions de ce magistrat.**

De même, la réflexion actuelle autour de l'encadrement de l'accès aux données de connexion dans le cadre des enquêtes pénales représente une opportunité de revoir l'équilibre actuel de la législation entre protection de la vie privée et recherche des auteurs d'infractions, afin de conserver une graduation dans les procédures en fonction du degré d'intrusivité des actes autorisés. **Les rapporteurs considèrent qu'il pourrait être opportun, dans le cadre de la réforme du code de procédure pénale, d'engager une réflexion sur l'encadrement des actes d'enquête afin de faire dépendre l'intensité de cet encadrement de l'ampleur effective de l'impact sur la vie privée**.

---

[1] https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/285620.pdf

[2] *En particulier par le rapport de la commission Justice pénale et droits de l'homme présidée par Mireille Delmas-Marty de juin 1990 ou encore celui de la commission de réflexion sur la justice pénale présidée par Philippe Léger en 2009.*

[3] https://www.senat.fr/rap/r10-162/r10-162_mono.html

**Proposition n° 10 :** **Engager une réflexion sur la proportionnalité des actes d'enquête en fonction de leur degré d'intrusion dans la vie privée.**

## III. GARANTIR LA FLUIDITÉ DE LA CHAÎNE PÉNALE POUR PROTÉGER LES ACTEURS DE L'ENQUÊTE DU « CHOC PROCÉDURAL »

Au-delà des questions liées à l'adaptation de nos normes internes, la refonte du régime d'accès aux données de connexion doit tenir compte de la « vraie vie » des enquêteurs. **L'un des principaux enjeux est ainsi que les inévitables réformes à venir ne viennent pas aggraver la crise des vocations dans les services d'enquête** et qu'elles ne se fassent pas au prix d'une dégradation des conditions de travail des policiers, des gendarmes et des magistrats. Comme l'a relevé Alexandre Lallet au cours de son audition, **la question du « comment contrôler » est au moins aussi importante, voire plus essentielle encore, que celle du « qui contrôle »** sur laquelle les débats se sont longtemps concentrés : les rapporteurs, partageant ce constat, appellent ainsi le Gouvernement à anticiper la mise en œuvre concrète de la réforme et à engager dès maintenant une réflexion dont ils souhaitent qu'elle s'appuie sur les orientations qui suivent.

### *A. CONFORTER LE RÔLE PIVOT DE LA PNIJ*

Comme la première partie du présent rapport le souligne, la PNIJ joue aujourd'hui un rôle pivot dans la pratique de l'enquête pénale. Son utilité fonctionnelle n'est pas son seul atout : elle constitue aussi un garde-fou juridique et elle est, tout autant qu'un outil au service des enquêteurs, un levier de régulation des accès aux données de connexion qui en assure la traçabilité et en garantit la supervision par l'autorité judiciaire.

Dans ce contexte, **les rapporteurs estiment nécessaire de conforter ce rôle singulier et de tirer les conséquences de la place centrale que la PNIJ occupe dans le quotidien des services d'enquête.**

Cet objectif implique, en premier lieu, de **renforcer les actions de formation déployées par ANTENJ auprès des enquêteurs** et ce, pour deux raisons complémentaires. La première tient à l'ampleur de la « gamme » de prestations offertes par la PNIJ : le nombre important de types de données accessibles par le biais de la plateforme ainsi que les développements nouveaux qui sont régulièrement apportés à celle-ci impliquent, en effet, un **accompagnement des utilisateurs pour expliquer le fonctionnement de l'outil et pour rappeler la manière dont les différentes données peuvent être utilisées, indépendamment ou par « croisement ».** Les formations permettront ainsi aux services d'enquête de tirer profit de toutes les

potentialités offertes par la PNIJ et de mieux « cibler » les données qui peuvent contribuer à l'élucidation des affaires.

La seconde raison tient, symétriquement, à la nécessité de préserver le principe d'un accès proportionné aux données de connexion. La sensibilité des informations contenues dans la PNIJ doit faire l'objet de rappels clairs et réguliers, et **ce constat doit conduire les enquêteurs à limiter leurs accès aux données qui ne sont pas seulement utiles, mais bien nécessaires à la manifestation de la vérité.** Si les rapporteurs sont conscients des efforts déjà déployés par les policiers et par les gendarmes pour respecter ce principe, ils relèvent néanmoins que l'habitude semble avoir été prise de **demander « en première intention » les factures détaillées d'un suspect**, alors même que ces documents, très exhaustifs, font partie de ceux qui révèlent le plus de données de connexion – et, partant, le plus d'éléments sur la vie des personnes concernées, y compris ceux qui n'ont pas de lien avec l'infraction sur laquelle porte l'enquête. Des formations contribueraient indéniablement à faire cesser ce réflexe et à « recentrer » les réquisitions sur des données significatives, sans pour autant obérer les capacités d'enquête des OPJ.

Les rapporteurs rappellent que, pour que de telles formations portent leurs fruits, **il est indispensable que les moyens dont dispose ANTENJ soient mis à la hauteur de cette ambition**.

**Il est, de la même manière, essentiel que les services d'enquête prennent toute leur part au bon fonctionnement de l'Agence.** Or, si la gendarmerie est dûment représentée au sein de l'équipe de direction de l'Agence, tel n'est pas le cas de la police, faute de candidat au poste d'officier de liaison : celui-ci est vacant depuis le début de l'année 2021. **Les rapporteurs appellent la direction générale de la police nationale à faire en sorte qu'un effectif dédié soit, sans délai, affecté au sein d'ANTENJ** pour y jouer le rôle de correspondant auprès de la police, cette interface étant particulièrement précieuse non seulement pour permettre à l'Agence de communiquer de manière fluide avec les services de terrain, mais aussi pour permettre à ces derniers de faire remonter leurs besoins et leurs attentes auprès d'ANTENJ.

**<u>Proposition n° 11 :</u> Renforcer la formation des services enquêteurs au maniement de la PNIJ.**

L'affirmation du rôle éminent de la PNIJ passe, par ailleurs, par un meilleur encadrement des usages hors- et para-PNIJ décrits en première partie.

**S'agissant du « hors-PNIJ », les rapporteurs rappellent que, sauf impossibilité technique, toutes les demandes d'accès aux données de connexion doivent passer par la plateforme** ; les usages contraires doivent, en toute logique, être refusés par le parquet dans son rôle de direction des

enquêtes et se traduire par une renonciation à tenir compte des éléments révélés par les données ainsi collectées – et, *a fortiori*, par un refus de leur mise au dossier.

Pour les demandes qui ne sont pas susceptibles de passer par la PNIJ pour des raisons techniques, et afin d'éviter un mésusage (voire l'envoi aux opérateurs de faux, cette hypothèse n'étant pas un cas d'école comme l'ont révélé les auditions menées dans le cadre de la présente mission), **les rapporteurs appellent à la mise en place d'un circuit informatique traçable et standardisé permettant tout à la fois d'authentifier et de contrôler le « hors-PNIJ ».**

**S'agissant, cette fois, du « para-PNIJ » que constituent les logiciels de rapprochement judiciaire**, les rapporteurs, s'ils en reconnaissent l'utilité, estiment toutefois que leur usage devrait être mieux encadré. Certes, ces logiciels font déjà l'objet d'un contrôle *ex ante* par la Cnil, prévu par le code de procédure pénale et qui permet d'attester d'une gestion des données personnelles conforme au RGPD comme à la loi « informatique et libertés ». En complément, et au vu du rôle majeur de ces outils dans la conduite des enquêtes, les rapporteurs estiment nécessaire que des vérifications complémentaires soient menées sur les autres aspects du fonctionnement de tels logiciels. Ils jugent ainsi indispensable que **des contrôles soient mis en place pour attester, d'une part, de la conformité des usages projetés et réalisés au code de procédure pénale et, d'autre part, de l'existence de protections adéquates des données vis-à-vis du risque de cyberattaque.**

L'ANSSI semble une candidate naturelle pour exercer le second de ces contrôles, en pleine cohérence avec son périmètre de compétences. Pour le premier contrôle, et à l'image de ce qui est prévu par le code pénal en matière d'interceptions de sécurité et de géolocalisation, le déploiement de logiciels de rapprochement judiciaire touchant les données de connexion devrait, pour l'avenir, **supposer l'avis conforme d'un comité consultatif composé *a minima* de représentants du ministère de l'intérieur** (par exemple, la nouvelle Agence du numérique des forces de sécurité intérieure) **et du ministère de la justice** (en envisageant, en particulier, l'association à ce processus d'ANTENJ).

À l'image de ce qui est prévu pour la PNIJ, une habilitation adaptée pour les personnes ayant accès aux données personnelles exploitées par ces logiciels devrait également être envisagée.

**Proposition n° 12 : Soumettre à un contrôle renforcé l'emploi par les services enquêteurs d'outils de retraitement des données de connexion.**

Enfin, les travaux des rapporteurs ont mis en lumière les **enjeux créés par l'existence de masses importantes de données personnelles conservées par les opérateurs** sous l'effet de l'obligation posée par le code des postes et des communications électroniques. Leur réflexion a, par conséquent, également porté sur les données collectées par les OCE qui viennent « nourrir » la PNIJ.

Si la vulnérabilité face aux attaques venues de l'extérieur des systèmes d'information de tous les opérateurs « historiques » est auditée par l'ANSSI au titre de sa compétence à l'égard des opérateurs d'importance vitale (OIV), et s'ils sont tenus à la mise en œuvre de mesures diverses – et notamment de procédés d'architecture informatique – visant à limiter l'impact d'éventuels incidents[1], **il n'apparaît pas que l'ANSSI dispose à date d'une pleine compétence de contrôle et de supervision de l'action des opérateurs en matière de données de connexion.** Comme le relevait lors de son audition Didier Vidal, administrateur interministériel des communications électroniques de défense, il existe un cadre pénal, fixé par l'article R. 226-1 du code, pour réguler l'emploi de dispositifs techniques permettant les interceptions judiciaires et les géolocalisations en temps réel, ceux-ci devant être autorisés par le Premier ministre assisté par une commission consultative *ad hoc* dont le secrétariat est confié à l'ANSSI. Or, **il n'existe pas de régime analogue pour les dispositifs qui permettent, du côté des opérateurs, la conservation des données et l'accès des enquêteurs à celles-ci.**

Selon les rapporteurs, **il serait judicieux de renforcer le contrôle de l'ANSSI sur le matériel utilisé par les OCE pour le fonctionnement de leurs « entrepôts » de données** afin que l'État puisse s'assurer, *a minima* avec une procédure d'homologation des équipements mis en œuvre, de la sécurité des données de connexion.

### *B. EVITER LE « CHOC PROCÉDURAL »*

**Le deuxième enjeu de mise en œuvre de la future réforme est, indéniablement, celui de la charge de travail qu'il induira sur les services d'enquête.** En effet, le contrôle de l'accès aux données de connexion supposera que les demandes soient dûment motivées, et aura en tant que tel

---

[1] *Il apparaît, sur ce terrain, que les mesures mises en œuvre par les OCE, bien qu'elles puissent être améliorées, sont d'ores et déjà robustes : comme le relevait la FFT lors de la séance orale d'instruction organisée par la 10ème chambre du Conseil d'État en amont de la décision* French data network *de 2001, les différents types de données sont stockés dans des bases distinctes, le rapprochement n'ayant lieu que pour les besoins des réquisitions. En outre,* « Les mesures de sécurisation peuvent être auditées par l'ANSSI, et leur insuffisance peut justifier le prononcé par la CNIL d'une amende pouvant atteindre 2 % du chiffre d'affaires mondial du responsable de traitement, à laquelle s'ajoute, en France, la sanction pénale prévue à l'article 226-17 du code pénal, soit cinq ans d'emprisonnement et 300 000 euros d'amende » *(conclusions précitées d'Alexandre Lallet).*

pour corollaire un formalisme renforcé. Dès lors, les officiers de police judiciaire connaîtront, de la même manière que l'instance en charge du contrôle (juge des libertés et de la détention ou autorité indépendante spécifique), un accroissement de leur quantité de travail.

Les rapporteurs préconisent donc une série de mesures visant à limiter le « choc procédural ». Ces recommandations sont d'autant plus importantes dans un contexte où des inquiétudes fortes sont relayées, depuis déjà plusieurs années, sur la crise des vocations dans la police judiciaire sous l'effet, notamment, de la complexification et de l'alourdissement de la procédure pénale. **Légitime dans son principe, indispensable pour assurer la conformité de notre droit interne aux règles européennes, la mise en place d'un contrôle indépendant de l'accès aux données de connexion ne doit pas se faire « sur le dos » des services d'enquête** : ceux-ci doivent, tout au contraire, être associés à cette réforme dès sa conception et bénéficier, en contrepartie du surplus de travail que tout nouveau contrôle suppose, d'une amélioration des moyens techniques leur permettant de récupérer ailleurs du temps à consacrer à leur cœur de métier.

Le système bâti par le Conseil d'État et la Cour de cassation permet de faire « tenir » provisoirement le dispositif juridique français et de donner au législateur et au Gouvernement un délai bienvenu pour concevoir la future réforme. Ce temps ne doit pas être gaspillé et c'est sans attendre qu'une réflexion doit être engagée pour trouver une formule adaptée tant aux exigences de la CJUE qu'aux légitimes attentes des acteurs de l'enquête pénale.

**Les rapporteurs appellent de leurs vœux un approfondissement des réflexions qui figurent dans le présent rapport à l'occasion de la refonte du code de procédure pénale** lancée par le projet de loi d'orientation et de programmation du ministère de la justice 2023-2027 qui devra, outre le travail de clarification à droit constant mené par le Gouvernement, s'accompagner – comme le relevait la commission des lois lors de l'examen du texte[1] - d'une « *simplification de la procédure pénale, qui est attendue par l'ensemble des acteurs* » et notamment par les officiers de police judiciaire de la police et de la gendarmerie nationales.

### 1. Calibrer la procédure d'autorisation pour maîtriser la charge de travail des enquêteurs

Le premier levier pour limiter le surplus de travail engendré par la mise en place d'un contrôle de l'accès aux données de connexion est celui d'une clarification du périmètre de l'autorisation. **En l'état, les pratiques semblent très disparates d'un parquet à l'autre** : certains accordent des autorisations par dossier et pour six mois, donnant de larges marges de

[1] *Rapport n° 660 (2022-2023) d'Agnès Canayer et Dominique Vérien, déposé le 31 mai 2023.*

manœuvre aux enquêteurs, tandis que d'autres privilégient l'émission d'une autorisation par ligne téléphonique et/ou par individu. **D'un extrême à l'autre, la charge de travail induite varie dans des proportions importantes.** De manière similaire, **dans un même ressort, les pratiques varient selon le cadre de l'enquête** : la direction générale de la police nationale a ainsi souligné auprès des rapporteurs que « *les politiques 'parquet' ou 'instruction', sont différentes selon les juridictions concernant l'autorisation d'accès aux données et sa portée (environnement personnel, lieu, ou individus ciblés visés par l'autorisation plus ou moins restrictive), ayant un impact sur l'accès aux données et les nécessités d'autorisations successives* ».

Aux yeux des rapporteurs, **il est indispensable d'harmoniser rapidement les pratiques dans un double objectif de standardisation** (celle-ci étant le préalable à la construction d'une politique publique homogène et à la mise en place d'outils informatiques adaptés) **et, surtout, de sécurité juridique**, la volatilité des doctrines apparaissant comme un facteur de variations dans la conduite des enquêtes, parfois au détriment du justiciable, mais aussi comme un **risque supplémentaire pesant sur les procédures** *a fortiori* au vu des modalités de contrôle *ex post* dégagées par la Cour de cassation dans ses arrêts précités du 12 juillet 2022.

**Le vecteur législatif paraît d'une excessive rigidité pour résoudre cette difficulté** : il paraît en effet impossible d'inscrire « en dur » dans la loi le juste périmètre des autorisations d'accès aux données de connexion, tant est élevé le nombre de cas particuliers et tant la situation varie entre une affaire simple dans son déroulement, avec un nombre faible de protagonistes, et un dossier de délinquance organisée mettant au jour l'existence d'un vaste réseau criminel avec des modes opératoires complexes. Il semble cependant que **la conformité à la jurisprudence de la CJUE de la pratique « une autorisation par dossier » n'est pas acquise** et que, à l'autre bout du spectre, le précepte selon lequel les enquêteurs doivent solliciter une autorisation par ligne va au-delà de ce qui est exigé par les juges de Luxembourg comme des nécessités d'une gestion raisonnable des enquêtes pénales.

**Les rapporteurs préconisent ainsi la publication, par la direction des affaires criminelles et des grâces du ministère de la justice, d'une circulaire permettant d'homogénéiser les pratiques des parquets** (ceux-ci ayant vocation à garder, conformément à leur mission de direction des enquêtes, un rôle de validation des demandes d'accès avant leur transmission à l'entité compétente pour le contrôle). Si cette solution présente l'inconvénient de ne pas purger complètement le problème, une telle circulaire n'étant par nature pas opposable aux juges du siège, elle permettra néanmoins **l'émergence d'une doctrine valable à l'échelle nationale qui, elle-même, rendra plus simple et plus lisible le travail des services d'enquête.**

**<u>Proposition n° 13 :</u> Sécuriser l'action des services d'enquête en précisant par circulaire le périmètre des autorisations d'accès aux données de connexion.**

Par ailleurs, **il est indispensable qu'une réflexion soit engagée sans délai par les ministères de l'intérieur et de la justice sur la forme de la demande d'accès aux données de connexion**. Aux yeux des rapporteurs, il est essentiel que cette demande puisse faire l'objet d'un traitement informatique ergonomique et suffisamment souple pour supporter au moins deux possibilités :

– une **motivation de la demande par le biais d'une application *ad hoc*, avec un système intuitif permettant une saisie rapide** de l'ensemble des éléments à prendre en compte pour apprécier la nécessité et la proportionnalité de l'accès (cases à « cocher » et/ou menu déroulant, auxquels pourrait s'ajouter un champ de saisie libre pour les affaires complexes ou présentant des spécificités particulières), ce qui contribuera tant à simplifier le travail des enquêteurs qu'à développer une nomenclature commune qui rendra plus lisibles les critères d'autorisation et harmonisera les pratiques ;

– **une motivation par référence à une pièce existante** (un procès-verbal, par exemple), une telle pratique paraissant aujourd'hui mise en œuvre par de nombreux services d'enquête et acceptée par les parquets.

Ce système n'interdirait pas les contacts de vive voix entre les différentes parties prenantes : pour les affaires complexes ou sensibles, il restera loisible aux parquetiers comme aux personnes chargées du contrôle de la demande de prendre directement l'attache de l'OPJ compétent pour obtenir des précisions sur les circonstances des faits, la personnalité des suspects, *etc*.

**Certaines des personnes auditionnées par les rapporteurs ont envisagé que soit mis en place un système d'autorisation « prospective »** par lequel un enquêteur pourrait, par exemple, être autorisé à accéder aux fadettes d'un suspect puis, dans un second temps mais sur la même base juridique, aux données d'identification des personnes avec lesquelles celui-ci est en contact (voire, au-delà d'une certaine intensité de contacts qu'il appartiendrait au juge de définir, aux fadettes des correspondants de la « cible » initiale ou à d'autres données de connexion relevant de tiers mais nécessaires à la manifestation de la vérité) et dont l'identité n'est pas encore connue à la date de la demande. À supposer qu'une telle possibilité soit compatible avec la jurisprudence de la CJUE et avec l'exigence d'un contrôle préalable des accès par une entité indépendante, elle devra être intégrée au système informatique décrit ci-avant et être ouverte non seulement aux enquêteurs, mais aussi aux parquets qui pourraient (avant transmission de la

demande à l'entité indépendante choisie) enrichir la demande initiale des OPJ en y ajoutant une demande d'accès futur sous conditions.

Il conviendrait également **que ce système ne limite pas l'action du validateur (donc des parquets) et des décideurs finaux (le JLD ou l'autorité d'autorisation) à l'acceptation ou au refus de la demande** : afin d'éviter toute perte de temps préjudiciable à la bonne gestion des enquêtes et des « allers-retours » fastidieux entre les protagonistes, la future application devra permettre aux magistrats de modifier la demande faite par les enquêteurs, notamment pour en restreindre ou en étendre le périmètre.

Dans tous les cas, **l'application ainsi déployée devra être reliée à la PNIJ afin que l'autorisation emporte l'ouverture automatique de la possibilité d'émettre une réquisition**.

Les rapporteurs relèvent que **le déploiement d'un tel outil, qui fluidifiera le lien entre les parquets et les enquêteurs, est de nature à générer des gains de temps non-négligeables.** En effet, en l'état, la demande d'accès aux données de connexion auprès des parquets repose sur un système quelque peu artisanal, puisqu'elle se fait (de même que d'autres demandes liées à la conduite de l'enquête) par téléphone. Or, comme l'ont constaté les rapporteurs lors de leur déplacement au commissariat central du 17e arrondissement de Paris, **le niveau élevé d'activité des parquets expose les OPJ à une longue attente avant d'entrer en communication avec le parquetier de permanence** (le délai peut, selon les éléments recueillis sur place, atteindre plusieurs heures dans les journées les plus chargées).

Si les enquêteurs ont pris l'habitude de gérer d'autres tâches pendant ce temps d'attente, cette solution n'est guère satisfaisante : inconfortable pour les policiers et gendarmes comme pour le parquet, **elle constitue par ailleurs un « doublon » puisque, à l'issue de cette conversation téléphonique, un écrit est établi** (le plus souvent, sous la forme d'un courriel) pour formaliser la demande de l'OPJ comme l'accord du parquet. Elle rend, au surplus, nécessaire la mise en place de mesures fastidieuses pour assurer la traçabilité des demandes, le parquetier se trouvant tenu de prendre des notes au cours de la communication pour garder la trace de ses échanges oraux avec les enquêteurs.

> **Proposition n° 14 : Engager un travail sur la forme de la motivation de la demande d'accès aux métadonnées visant à limiter la charge de travail supplémentaire induite par la nouvelle procédure.**

Les rapporteurs s'interrogent, plus largement, sur la mise en œuvre d'un dispositif informatique se substituant pour partie aux communications téléphoniques qui constituent à ce jour l'essentiel du lien entre les enquêteurs et le parquet, y compris pour des actes basiques et quotidiens. **Cette interrogation concerne en réalité l'avenir du système « traitement en**

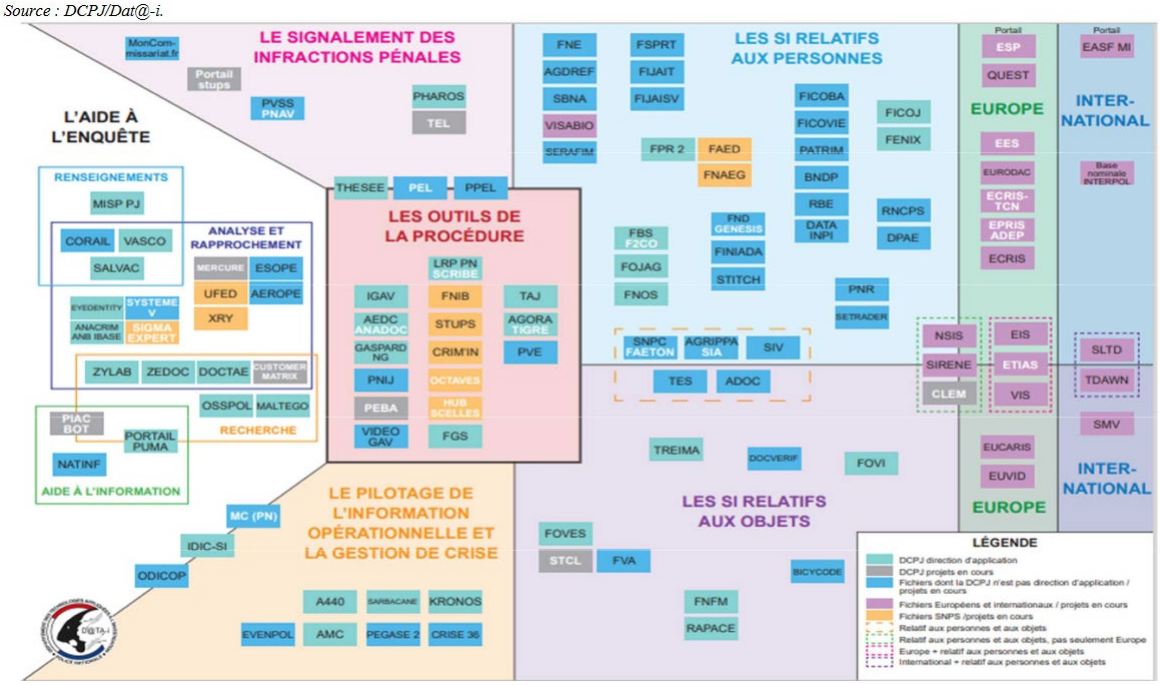
**temps réel » (TTR) mis en place par les parquets pour orienter les enquêtes** : celui-ci repose actuellement sur des outils peu performants et qui ne sont pas communs entre les forces de sécurité intérieure et les juridictions si bien qu'il s'apparente souvent, dans les faits, à un centre d'appels téléphoniques accompagné de logiciels de suivi dans lequel les informations sont « re-saisies ».

Les rapporteurs estiment ainsi que, pour les demandes simples pour lesquelles un contact oral n'a qu'une faible valeur ajoutée, une dématérialisation des échanges doit être envisagée. **Ils déplorent que ce sujet ait été laissé hors du périmètre du projet « procédure pénale numérique »** (PPN), alors même qu'il constitue un enjeu majeur d'efficacité.

### 2. Intégrer le sujet des données de connexion aux chantiers informatiques en cours

Les enquêteurs de la police et de la gendarmerie nationales interviennent dans un environnement informatique complexe, comme en atteste le schéma ci-dessous qui cartographie la « *boîte à outils numériques de l'enquêteur* ».

*Source : DCPJ/Dat@-i.*




*Source : Cour des comptes*[1]

Cette cartographie n'est pas simplifiée par la mise en œuvre du projet « procédure pénale numérique », ou « PPN », qui vise à mettre en place une procédure pénale numérique dès son origine non pas par création d'un nouvel outil unifié, mais par interconnexion des outils informatiques existants.

[1] *Cité par le rapport « Les moyens affectés aux missions de police judiciaire » publié le 11 mars 2023 et accessible sur le site de la Cour des comptes.*

**Le projet PPN**

Le programme PPN, codirigé par les ministères de l'intérieur et de la justice, consiste à définir, à droit constant, une procédure pénale intégralement numérique dès son origine. Il prévoit que les actes sont signés et transmis électroniquement aux juridictions par les forces de sécurité intérieure (police nationale et gendarmerie), depuis l'acte d'enquête initiale, réalisé par les forces de sécurité intérieure (ministère de l'intérieur), jusqu'à l'exécution de la peine et l'archivage (effectué par les juridictions). Toutes les procédures sont concernées, à l'exception des contraventions des quatre premières classes et des crimes. Sont aussi concernés les délits relatifs aux affaires d'atteintes aux biens de faible gravité d'auteurs inconnus, dits « petits X », qui n'étaient pas enregistrés auparavant, mais simplement transmis au parquet pour classement. Avec la PPN, ces procédures seront établies dès l'origine sous forme numérique et transmises de façon dématérialisée au parquet des tribunaux judiciaires.

PPN, qui n'est pas une application informatique mais un programme regroupant 14 projets informatiques, permet donc l'abandon du dossier papier de la procédure et de la signature manuscrite, celle-ci étant remplacée par la signature électronique.

La stratégie du programme s'appuie sur trois principes :

– la numérisation de la procédure pénale est réalisée à partir des systèmes d'information déjà existants, qui devront évoluer et être mis en relation ;

– les travaux de développement informatique sont menés par paliers ;

– les utilisateurs sont associés à toutes les phases de la conception du nouveau système.

Les utilisateurs regroupent les forces de sécurité intérieure responsables de la police judiciaire, les magistrats et les personnels de greffe en charge du pénal, mais aussi les autres acteurs de la chaîne pénale tels que les avocats, les huissiers et les partenaires institutionnels : la douane et la DGFiP à terme.

Sont concernées annuellement près de 4,5 millions de procédures, dont près de 2 millions sont des « petits X ». […]

Après avoir été expérimenté durant un an, le déploiement a débuté, par étapes (concernant les « petits X », puis certaines procédures correctionnelles, puis tous les délits) et par vagues.

Les vagues, au nombre de six, s'étendent sur une durée de six mois et ne concernent, pour sécuriser le déploiement, qu'un département par cour d'appel. En juin 2021, la troisième vague avait débuté et PPN devait être déployée dans 44 tribunaux judiciaires en mars 2022. L'objectif est de parvenir en fin d'année 2023 à ce que la totalité des délits soit traitée numériquement par les tribunaux et que tous les services d'enquête qui concourent à une procédure délictuelle échangent en numérique dès l'origine avec les juridictions et entre eux sur tout le territoire.

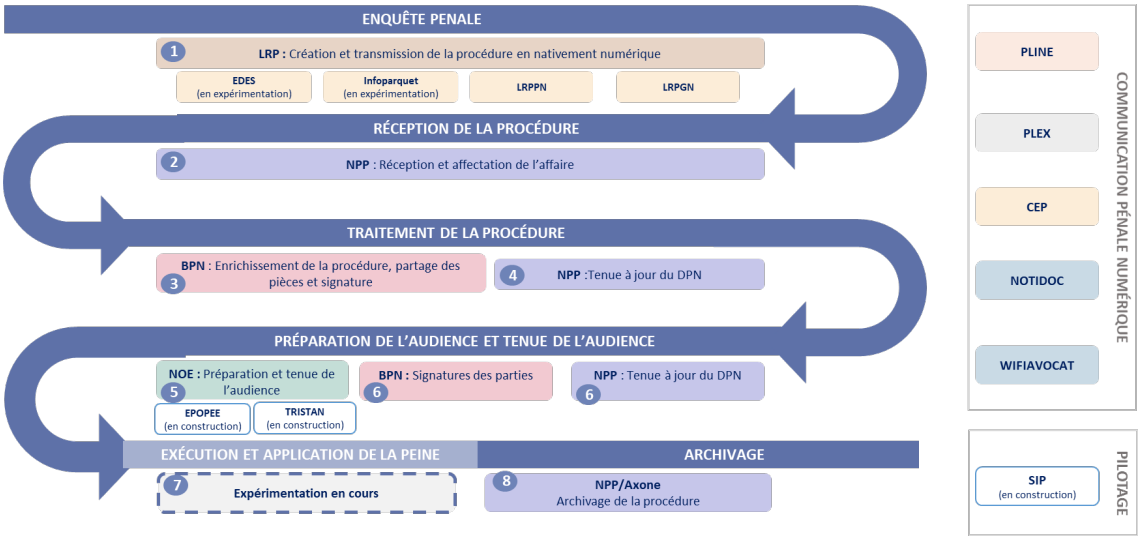
*Source : communication de la Cour des comptes à la commission des finances du Sénat – janvier 2022*[1]

[1] *Ce document est accessible sur le site de la Cour des comptes.*

Le projet PPN, dont la direction est depuis peu assurée par un programme unique regroupant les ministères de l'Intérieur et de la Justice, vise à couvrir toute la « vie » d'une procédure. Si **le projet, dans son périmètre actuel, comporte quelques interactions avec la PNIJ** (utilisation du multimédia par le biais d'un nouvel applicatif appelé EPOPEE et portant notamment sur des éléments issus de la PNIJ, comme des extraits d'écoutes et des éléments liés à la géolocalisation, avec une cartographie associée), il n'était pas initialement prévu d'y intégrer d'autres pans de la plateforme**. L'impératif d'un travail sur la signature des réquisitions a récemment été mis au jour et devrait se voir inclus dans le champ du projet.**

**ANTENJ prévoit, en parallèle, de faciliter l'interaction entre la PNIJ et les logiciels de rédaction de procédure (LRP) des forces de sécurité intérieure** (par exemple, en facilitant l'import automatique des données produites sur la PNIJ dans les LRP), ce point étant loin d'être anecdotique au vu du rôle central de ces LRP dans le fonctionnement de la procédure pénale numérique.

Le fonctionnement projeté de PPN est synthétisé dans le schéma ci-après.




*Source : direction du programme PPN*

**Le déploiement de PPN, qui a vocation à terme à s'étendre à tout le périmètre délictuel, connaît depuis le début de l'année 2023 une accélération qu'il convient de saluer.** Au 30 septembre 2023, selon la direction du programme PPN, 68,3 % des procédures étaient nativement prises en numérique ; 826 unités de police et de gendarmerie, soit 97,5 %, étaient déployées sur PPN, et 94 % des tribunaux judiciaires (soient 158 tribunaux) avaient déployé la filière automatisée des classements sans suite tandis que 39 % d'entre eux (65 tribunaux) avaient déployé une ou plusieurs filières de PPN en matière correctionnelle avec poursuite. Selon les indications recueillies par les rapporteurs, la part la plus fastidieuse du projet porte sur la mise à niveau des outils informatiques du ministère de la justice, les applicatifs existants n'étant réputés ni pour leur ergonomie ni pour leur efficacité.

**Des questions demeurent quant au bon fonctionnement des LRP, dont le rôle clé a été souligné ci-avant.** La Cour des comptes relevait ainsi, dans un point d'étape sur la transformation numérique du ministère de la justice rendu public en janvier 2022[1], que « *le développement de PPN […] impose que les logiciels de rédaction des procédures (LRP) de la police et de la gendarmerie nationale soient modifiés pour permettre la transmission des pièces des procédures sous forme numérique* », ce que devait permettre un nouveau logiciel de rédaction appelé Scribe ; cependant, **en 2023[2], la Cour a n'a pu que constater « *l'échec de Scribe* »** et déplorer que cette situation « *éloigne d'autant l'horizon de déploiement d'une solution technique et performante améliorant le travail de tous les jours des enquêteurs* » - à quoi on peut ajouter que ces difficultés ne rapprochent pas les services d'enquête d'un aboutissement de la procédure pénale numérique.

**Les rapporteurs rappellent que la procédure pénale numérique constitue une attente forte des acteurs de l'enquête pénale**, qui espèrent légitiment pouvoir en tirer des gains de temps sur des tâches « administratives » dont certaines, comme les « re-saisies », sont inutilement lourdes et chronophages. **Il est indispensable que ce projet, dont l'aboutissement est aujourd'hui prévu à la fin de l'année 2025, puisse toucher à une fin satisfaisante et rapide** afin de compenser les missions supplémentaires qui seront confiées aux officiers de police judiciaire et aux parquets en matière de motivation des accès aux données de connexion. Il est tout aussi essentiel que **des réflexions soient engagées sans tarder sur la prise en compte, par le projet PPN, du futur processus** de formalisation par les enquêteurs, puis de validation par le parquet et de contrôle par l'entité indépendante qui en sera chargée, de ces mêmes demandes d'accès.

> **Proposition n° 15 : S'imposer, avant l'entrée en vigueur du nouveau contrôle des autorisations d'accès aux données de connexion, de mener à bien le projet procédure pénale numérique (PPN).**

À titre subsidiaire, les rapporteurs soulignent que cette évolution se cumulera avec l'entrée en vigueur, dans trois ans, du règlement *e-evidence* et du nouveau portail associé par lequel les services d'enquête pourront émettre des réquisitions pour obtenir des preuves numériques[3]. L'enjeu est d'éviter la mise en place d'une « usine à gaz » qui ferait percevoir négativement, par les services d'enquête, une réglementation qui doit au

---

[1] *Ce document est accessible sur le site de la Cour des comptes.*

[2] *Enquête sur les moyens affectés aux missions de police judiciaire, rendue publique en mai 2023 et accessible sur le site de la Cour des comptes.*

[3] *Selon les informations obtenues par les rapporteurs lors de leur déplacement à Bruxelles, ce portail ne prendra pas la forme d'un outil unique à l'échelle de l'Union, mais d'un système décentralisé (mais standardisé) dans chaque État ayant vocation à se connecter avec les plateformes nationales préexistantes.*

contraire marquer un réel progrès et leur permettre d'obtenir de nouvelles preuves. La Commission européenne se donne deux ans pour définir, sous forme d'actes délégués, les spécifications techniques d'*e-evidence*, qui porteront en particulier sur les interactions entre ce futur portail et les systèmes existants dans les États membres (ce qui correspond, en pratique, à la PNIJ pour la France). **Ce travail doit faire l'objet d'un suivi aussi attentif qu'étroit par le Gouvernement, sous peine de condamner les nouvelles opportunités créées par *e-evidence* à rester lettre morte.**

Enfin, les rapporteurs insistent sur la nécessité de **préserver l'avenir de la numérisation de la procédure pénale – et, plus généralement, d'assurer la capacité de nos services d'enquête à s'adapter aux évolutions technologiques** qui viennent chaque jour modifier les usages quotidiens des honnêtes gens comme des délinquants – en garantissant la modularité de tous les outils informatiques actuellement en chantier. Il est en effet crucial d'éviter que ces outils soient trop dépendants des procédures existantes et qu'ils soient appelés, en conséquence, à connaître des modifications techniques substantielles à chaque adoption d'une nouvelle loi de procédure pénale. Ils doivent, tout à l'inverse, être aussi souples que possible et ne pas rigidifier les liens fonctionnels qui existent entre les différents acteurs.

Cet impératif est d'autant plus fort à l'heure où le code de procédure pénale, outre sa recodification à droit constant par ordonnance, est voué à faire l'objet d'une réforme pouvant améliorer les équilibres des enquêtes pour offrir enfin aux policiers, aux gendarmes, aux parquets et au siège, mais aussi et surtout aux justiciables, un cadre pénal lisible et équilibré.

**<u>Proposition n° 16 :</u> Assurer la modularité des outils créés par les chantiers informatiques sur la procédure pénale numérique (PPN).**

# EXAMEN EN COMMISSION

_____

MERCREDI 15 NOVEMBRE 2023

**M. François-Noël Buffet, président**. - Nous allons aborder le dernier point de notre ordre du jour, qui est l'examen du rapport d'information sur les modalités d'investigations recourant aux données de connexion dans le cadre des enquêtes pénales.

**M. Philippe Bonnecarrère, rapporteur**. **–** Je rends tout d'abord hommage au travail conduit par notre ancien collègue Jean-Yves Leconte, qui a contribué aux travaux de la mission d'information jusqu'en octobre dernier.

Ce rapport concerne la conjonction entre deux sujets. Le premier est le fait que nos enquêteurs utilisent de plus en plus les données issues de nos appareils connectés pour identifier l'auteur d'une infraction et sa localisation. Le second concerne la jurisprudence de la Cour de justice de l'Union européenne (CJUE), qui est extrêmement restrictive quant aux conditions de conservation et d'accès aux données de connexion. Notre sujet est donc de savoir comment s'organiser et comment résoudre ce conflit. Je m'attacherai à établir un constat de la situation, tandis qu'Agnès Canayer présentera les propositions et la manière dont nous abordons l'avenir.

Les données de connexion sont de plusieurs types. Il y a bien sûr le numéro d'abonné ou le numéro de carte qui permet d'identifier une tablette ou un mobile. À côté de ces éléments d'identification, il y a aussi les données trafic, par exemple qui vous appelez, ou à qui vous adressez des mails. Le troisième type de données sont les données de localisation, qui permettent par exemple de savoir qui se trouve à proximité, à tel moment, de tel lieu de cambriolage, et qui ne s'y trouve pas.

Ces multiples données floutent, aujourd'hui, la différence entre le contenu et le contenant. En croisant les auteurs des appels et les horaires, il est possible de définir un mode de vie.

Il s'agit d'un sujet massif, puisqu'un peu plus de deux millions de réquisitions ont pu être émises sur le dernier exercice. À l'heure actuelle, ceci fonctionne de manière assez simple. Il a fallu dix laborieuses années, de 2007 à 2017, pour mettre en œuvre le système de la plateforme nationale des interceptions judiciaires (PNIJ), ouverte à plus de 60 000 personnes dans la gendarmerie ou la police.

Concrètement, un enquêteur à qui on a signalé un cambriolage va vérifier, en premier lieu, s'il n'y a pas de témoignages ou d'éléments qui le mettent sur une piste. Il va essayer de voir qui pouvait se trouver dans le secteur à l'heure concernée. Pour cela, il remplit un formulaire, se munit de sa carte professionnelle qui l'authentifie et permet l'accès à la PNIJ, et fait une demande d'identification auprès de son parquetier au téléphone.

Une fois cette autorisation donnée, l'enquêteur précise sa demande dans le système informatique de la PNIJ, puis reçoit dans un délai de deux heures les données dont il a besoin. Il s'agit donc d'un système qui automatise l'envoi et la réception entre cette agence et les quatre grands opérateurs de téléphonie. Nous signalons accessoirement qu'il existe encore des accès hors PNIJ, qui peuvent poser question.

Les enquêteurs estiment que ce système fonctionne bien et les parquetiers n'y voient pas de difficultés puisqu'ils assurent la maîtrise de l'enquête, en autorisant ou non l'accès aux données. Cependant, tout a changé depuis maintenant quelques années. La Cour de Luxembourg est partie de l'idée que le stockage des données de connexion rappelle de mauvais souvenirs, en particulier dans les pays de l'Est. Elle a fait le choix de ne pas faire confiance aux États et de passer par une interdiction pure et simple, plutôt que de demander à chaque État de justifier son organisation pour garantir une proportionnalité entre la conservation et les autorisations accordées aux enquêteurs.

Premièrement, la CJUE n'accepte plus la conservation générale et indifférenciée des données de trafic et de localisation ; elle ne l'accepte qu'en cas de menace grave et pour la sécurité nationale.

Deuxièmement, une différence est faite, entre, d'une part, les données de trafic et de localisation et, d'autre part, les données d'identification, pour lesquelles la procédure de réquisition est, selon la jurisprudence de la CJUE, plus aisée. Concernant l'accès aux données de trafic et de localisation, l'accès n'est possible qu'en cas de criminalité grave et sous la forme d'un « *quick freeze* », c'est-à-dire une injonction de conservation rapide. En d'autres termes, l'autorité judiciaire peut demander à garder les éléments pendant quelques temps. Or, l'intérêt des données de connexion est de pouvoir chercher rétrospectivement. Notre système juridique permet parfaitement d'intercepter les communications d'un suspect, de savoir qui appelle ou est appelé. C'est donc l'utilisation des données conservées et non pas des données de flux qui pose question.

Troisièmement, la CJUE impose, dans l'hypothèse d'une criminalité grave et d'un *quick freeze*, des conservations ciblées. Dans ce cadre, les États sont censés ne pas conserver la globalité des données, mais celles concernant certains secteurs géographiques ou certains secteurs considérés comme sensibles, à l'instar des ports, des aéroports, des quartiers à proximité des lieux de gouvernement.

Ce sont donc des choix jurisprudentiels qui conduisent à ne plus avoir de conservation générale mais à avoir une conservation ciblée dont tout le monde dit qu'elle est quasiment impossible.

Enfin, l'accès à ces données n'est possible qu'à la condition qu'il soit autorisé par une autorité administrative indépendante ou par un juge qui n'est pas chargé de l'accusation. Ce dernier élément est une critique directe du système judiciaire français où le Procureur de la République, qui a certes

toutes les caractéristiques fondant, pour la Cour européenne des droits de l'homme (CEDH), l'indépendance d'un magistrat, mais qui est chargé de l'accusation.

Alors qu'environ 85 % des enquêtes aujourd'hui en France utilisent ces moyens techniques, les enquêteurs ne peuvent travailler sans, d'autant que l'obtention d'aveux et de témoignages est aujourd'hui difficile. Tous ces éléments expliquent comment les données de connexion sont devenues la reine des preuves.

Le résultat est donc une déstabilisation complète des systèmes dans l'ensemble de l'Union européenne. Certains États, notamment à l'Est, poursuivent leur route sans se préoccuper de la jurisprudence de la CJUE. D'autres ont abrogé leur réglementation et n'arrivent pas à faire face aux problèmes que cela engendre - nous pouvons citer les difficultés néerlandaises et suédoises en matière de lutte contre la criminalité organisée -, ou font mystère de la manière dont ils arrivent à s'en passer. Je pense à nos voisins allemands dont la coalition au pouvoir n'arrive pas à définir de nouveau régime de conservation des données de connexion et que nous soupçonnons, dans l'intervalle, de s'appuyer sur les données recueillies dans le cadre de l'activité de leurs services de renseignement. D'autres pays ont fait semblant d'appliquer la jurisprudence de la CJUE. C'est le cas de la Belgique qui a adopté un système de conservation ciblée dont les critères sont si larges que l'ensemble du territoire est couvert par ce « ciblage », à l'exception, peut-être, d'un bout de forêt au fin fond des Ardennes belges. Vous comprenez aisément l'ampleur de la difficulté matérielle que pose un tel système.

Pour terminer, où en est-on sur le territoire français ? Le Conseil constitutionnel, le Conseil d'État et la Cour de cassation ont fourni un exceptionnel travail de créativité juridique dans le but de préserver le modèle français. Le Conseil d'État a formulé une solution ambitieuse dans l'arrêt *French Data Network* qui consiste à considérer que les conséquences de la mise en œuvre de la jurisprudence de la CJUE seraient telles qu'elles mettraient en danger la sécurité nationale. Il admet donc que le système français de conservation des données peut perdurer au nom du principe de la sauvegarde de l'ordre public. La Cour de cassation a déployé un raisonnement comparable et, tout en admettant que le cadre juridique n'était pas idéal, a fixé des conditions si strictes qu'aucune nullité ne pourra être prononcée. Mais aucune autorité indépendante n'intervient dans le contrôle des réquisitions qui relève encore du parquet en charge de l'accusation, ce qui implique que, tôt ou tard, notre système juridique devra évoluer. Nous avons quelques années devant nous – peut-être 3 à 5 ans – pour agir ; nous ne pouvons pas nous permettre de procrastiner. Pour trouver une solution, il apparaît nécessaire de traiter du volet purement français mais aussi du volet européen de ce problème.

**Mme Agnès Canayer, rapporteur**. **–** Au terme de 3 déplacements et après avoir auditionné plus de 50 personnes, nous avons tenté de trouver un équilibre entre respect de la jurisprudence européenne et pragmatisme pour permettre aux enquêteurs de mener les enquêtes de façon satisfaisante afin de préserver la sécurité publique.

Le premier niveau sur lequel nous proposons d'agir est le niveau européen, en profitant de la prise de conscience des États membres sur le sujet, même si nous avançons à petits pas. Nous préconisons que la France soit plus présente et s'engage dans une renégociation non pas des traités, qui serait bien trop ambitieuse et inefficace, mais du règlement « *E-privacy 2* » pour exclure de son cadre les enquêtes pénales. Nous souhaitons également que la France pèse dans le groupe d'experts de haut niveau « *Going Dark* » rebaptisé « *ADELE* » lancé par la Suède lorsqu'elle assurait la présidence du Conseil de l'Union européenne. Cette initiative témoigne de la prise de conscience de la nécessité de trouver une solution pour les forces de l'ordre des États membres. Mais les travaux de ce groupe de travail sont extrêmement opaques ; nous préconisons donc que le Gouvernement informe le Parlement de son état d'avancement pour garantir un suivi effectif.

En France, il convient de mieux cadrer et délimiter le sujet. En premier lieu, nous devons répondre à la question suivante : quelles sont les données qui doivent être conservées par les quatre opérateurs majeurs (Free, SFR, Bouygues et Orange) ? Il s'agit d'un point essentiel car, à l'heure actuelle, il n'existe aucune harmonisation des pratiques. De même, la refonte de la procédure de contrôle de la réquisition des données nous paraît essentielle. L'existence d'une procédure harmonisée pour tous les types de données et de réquisitions n'est pas satisfaisante car la jurisprudence de la CJUE admet que le parquet puisse assurer le contrôle de la réquisition des seules données d'identification. À la lecture des conclusions de l'avocat général Szpunar dans l'affaire *Hadopi* qui viennent d'être rendues publiques, nous comprenons que la CJUE est prête à faire preuve d'ouverture sur ce sujet, notamment dans le cadre de la cybercriminalité. Il faudra en tirer les conséquences. Enfin, nous plaidons pour une harmonisation des procédures en ce qui concerne la criminalité grave, car c'est bien la finalité répressive de la réquisition qui détermine la nature de son contrôle. La Cour de cassation considère que ce n'est pas seulement le quantum des peines mais aussi un faisceau d'indices qui permet de définir la criminalité grave. Celle-ci est donc appréciée au cas par cas : certains parquets demandent une réquisition par dossier, d'autres par groupe de localisation ou de temporalité… Nous pensons qu'il est nécessaire d'inscrire cette notion dans le code de procédure pénale pour harmoniser et clarifier les pratiques.

Notre troisième axe de travail porte sur le contrôle de l'accès aux données de connexion. Aujourd'hui, la mission conférée au parquet ne remplit pas les conditions du contrôle préalable et impartial imposé par la CJUE. Nous avons tenté de réfléchir à la meilleure manière de s'y conformer.

Confier ce contrôle à une autorité indépendante, qu'elle soit administrative ou judiciaire, ne nous semblait pas répondre de façon pragmatique aux exigences de la CJUE car il s'agit de contrôler plusieurs millions de réquisitions par an. Nous avons donc plutôt opté pour un contrôle par le juge des libertés et de la détention (JLD) en prévoyant des aménagements pour que cette nouvelle mission n'absorbe pas toutes les créations d'emplois obtenues dans le cadre de la loi d'orientation et de programmation du ministère de la justice pour 2023-2027. Une telle réforme imposerait donc une redéfinition globale du rôle et des fonctions du JLD. Sur cette base, deux options nous paraissent possibles : la création d'un pôle de JLD à l'échelle de chaque cour d'appel ou l'affectation de JLD détachés à raison d'une journée par semaine dans les juridictions. Il apparaît aussi nécessaire de travailler sur la procédure et les outils numériques pour fluidifier le contrôle des réquisitions et permettre aux enquêteurs de travailler sur un logiciel efficace et connecté à la procédure pénale numérique. Nous savons que le développement des outils numériques est toujours un sujet complexe pour le ministère de la justice. Mais il nous faut y travailler car, aujourd'hui, les enquêteurs sont contraints d'appeler le parquet pour formuler leurs demandes, ce qui constitue une perte de temps considérable.

L'enjeu est également de lutter contre deux dérives. Il s'agit, d'une part, de la pratique du « hors-PNIJ » : 20 à 25 % des enquêteurs n'ont pas recours à la procédure de réquisition par le biais de la PNIJ, dont l'avantage est d'assurer une traçabilité. D'autre part, s'impose un contrôle des logiciels de retraitement des informations et des données, qui permettent, si je schématise, à l'enquêteur de faire ressortir un coupable idéal à partir de ces données. Ces moyens permettent donc de se mettre en conformité. Il n'y a cependant pas urgence, dès lors que les jurisprudences de la Cour de cassation, du Conseil d'État et du Conseil constitutionnel ont permis de trouver des ouvertures. Néanmoins, cette robustesse a ses limites. Il faut donc prendre le temps et anticiper, c'est l'intérêt de ce rapport, qui sera prochainement complété par d'autres dont celui du conseiller d'État Alexandre Lallet, chargé d'une mission sur le sujet par le gouvernement. Sont ainsi posées les premières bases de réflexion, en prévision du jour où notre système sera sanctionné par la jurisprudence européenne.

**M. Jérôme Durain**. **–**Jean-Yves Leconte, qui a collaboré avec Agnès Canayer et Philippe Bonnecarrère sur cette mission, a eu l'amabilité de faire quelques retours, que nous énonçons ici au nom de notre groupe. S'alignant sur les travaux rendus par les rapporteurs, il s'interroge toutefois sur la mise en œuvre de la solution relative au recours aux JLD, qu'il craint compliquée, au regard de l'articulation de cette activité complémentaire avec les missions principales du JLD. Il rejoint les propos de Philippe Bonnecarrère sur la jurisprudence de l'Union européenne.

En premier lieu, cette vision très restrictive portée par la CJUE empêche la juridictionnalisation de certaines infractions, ayant, de fait, des conséquences paradoxales en matière de protection des droits.

En second lieu, les obligations qui pèsent sur les opérateurs traditionnels et les nouveaux entrants ne sont pas de même nature, il est très difficile de contrôler Telegram, WhatsApp ou Starlink, il s'agirait donc de se pencher sur cette question.

**Mme Agnès Canayer, rapporteur**. **–** Le recours aux JLD n'est certes pas la solution qui s'impose naturellement, mais il permet de répondre autant aux exigences de la CJUE et aux critères d'efficacité de la procédure. Dans la loi d'orientation et de programmation du ministère de la justice pour 2023-2027, nous avions retiré une partie des compétences nombreuses du JLD, déjà fortement mobilisé, notamment dans les contentieux civils. Je pense qu'il faudrait aller encore plus loin pour le recentrer sur son rôle premier de juge de l'enquête.

**M. Philippe Bonnecarrère, rapporteur**. **–** Je soulignerai, pour conclure, deux sujets passionnants en arrière-plan.

En premier lieu, la CJUE surprend en intervenant sur des terrains nationaux, s'appuyant, pour ce faire, sur la Charte des droits fondamentaux de l'Union européenne. Nous sommes, par ailleurs, habitués au contrôle d'équilibrage mené par le Conseil constitutionnel, conciliant les enjeux de défense des libertés privées et les principes de préservation de l'ordre public. À l'inverse, la CJUE ne recourt pas à cette méthode de la proportionnalité et concentre son attention sur le seul principe de défense des libertés fondées sur la Charte.

En second lieu, nous imposons de strictes conditions pour contrôler l'accès de nos services d'enquête aux données de connexion. Cependant, ces données sont à la disposition d'opérateurs qui, comme Google ou Facebook, en font commerce sans que nous ayons le moindre contrôle sur eux. Il y a ainsi un déséquilibre entre la sphère privée et la sphère publique. Enfin, notre système fonctionne vis-à-vis des opérateurs traditionnels, mais il y en a d'autres, dont Starlink, ce qui donne ainsi aux malfaiteurs un large avantage sur les enquêteurs.

Nous avons là un débat classique entre la défense des libertés et les nécessités concrètes et pragmatiques.

**Mme Agnès Canayer, rapporteur**. **-** Nous proposons, pour le rapport, le titre suivant : « Surveiller pour punir ? Pour une nouvelle régulation des accès aux données de connexion dans l'enquête pénale ».

*Les recommandations sont adoptées.*

*La commission adopte à l'unanimité le rapport d'information et en autorise la publication.*

# LISTE DES PERSONNES ENTENDUES ET DES CONTRIBUTIONS ÉCRITES

**Ministère de l'intérieur**

*Direction générale de la gendarmerie nationale (DGGN)*

**M. le colonel Alexandre Malo**, sous-directeur de la police judiciaire

**M. le lieutenant-colonel Dominique Bousquet**, chef du pôle prospective pénale et pratique judiciaire

*Direction générale de la police nationale (DGPN)*

**M. Philippe Chadrys**, directeur central adjoint de la police judiciaire

**M. Alex Gadré**, conseiller juridique

*Direction générale de la sécurité intérieure*

**M. Nicolas Lerner**, directeur général

**Mme Caroline Boussion**, conseillère juridique

**Ministère de la justice**

*Direction des affaires criminelles et des grâces (DACG)*

**M. Olivier Christen**, directeur

**M. Nicolas Renucci**, chef du bureau de la police judiciaire

**Mme Elise Barbe**, sous-directrice de la négociation et de la législation pénales

**Ministère des armées**

*Direction générale de la sécurité extérieure*

**Ministère de l'économie, de finances et de la relance**

*Commissariat aux communications électroniques de défense (CCED)*

**M. Didier Vidal**, administrateur interministériel des communications électroniques de défense

**M. Frédéric Burtin,** expert

**Conseil d'État**

**M. Patrick Pailloux**, conseiller d'État

**M. Alexandre Lallet,** conseiller d'Etat

**Secrétariat général des affaires européennes (SGAE)**

**Mme Caroline Vinot**, secrétaire générale adjointe – Protection, frontières et justice

**Mme Vanessa El Khoury Moal**, cheffe du bureau justice pénale et civile

**Mme Constance Deler**, cheffe du bureau Parlements

**Mme Anne Thimpont**, adjointe à la cheffe du bureau sécurité intérieure de l'Union européenne

**Mme Louise Bréhier**, conseillère juridique

**Représentation permanente de la France auprès de l'Union européenne**

**Mme Pauline Dubarry**, adjointe au chef du service justice et affaires intérieures

**Cour de cassation**

**M. Nicolas Bonnal**, président de la chambre criminelle

**Conférence nationale des procureurs de la République**

**M. Raphaël Balland**, président, procureur de la République de Béziers

**Mme Anne Gaches**, vice-présidente, procureure de la République d'Albertville

**Mme Marie-Céline Lawrysz**, procureure de la République de Compiègne

**Conseil national des barreaux**

**Mme Laurence Roques**, présidente de la commission « Libertés et droits de l'homme »

**M. Gérard Tcholakian**, membre de la commission « Libertés et droits de l'homme »

**M. Emmanuel Raskin** - membre des commissions « Accès au droit » et « Textes »

**Conférence des bâtonniers**

**Mme Justine Devred**, membre du bureau

**Autorité de régulation de la communication audiovisuelle et numérique**

**M. Denis Rapone**, membre du collège

**Mme Ségolène Mariotte-Sirdey**, adjointe au directeur de la création

**Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)**

**Mme Laure de La Raudière**, présidente

**M. David Epelbaum**, chef de l'unité « Opérateurs télécom et obligations légales »

**M. Olivier Delcos,** directeur « Internet, Presse, Postes, Utilisateurs »

**Agence nationale des techniques d'enquêtes judiciaires**

**M. Jean-Julien Xavier-Rolain**, directeur

**M. Yves Bronoel,** directeur adjoint

**Personnalités qualifiées**

**M. François Molins,** procureur général près la Cour de cassation

**Table ronde - universitaires**

**M. Benoît Auroy**, maître de conférences en droit privé et sciences criminelles, université de Rennes

**M. Winston Maxwell**, directeur d'études droit et numérique, institut polytechnique de Paris

**Mme Clara Saillant**, assistante de recherche à l'université de Vienne, département d'innovation et de digitalisation en droit

**M. Etienne Vergès**, professeur de droit privé et sciences criminelles, université Grenoble Alpes

**Table ronde des associations**

*La Quadrature du Net (LQN)*

**M. Bastien Le Querrec**, juriste, membre de La Quadrature du Net

*French Data Network (FDN)*

**M. Benjamin Bayart**, membre d'honneur, ancien président

*European Digital Rights (EDRi)*

**Mme Chloé Berthélémy**, conseillère politique

**Commission nationale de contrôle des techniques de renseignement (CNCTR)**

**M. Serge Lasvignes**, président

**M. Samuel Manivel**, conseiller

**Commission nationale de l'informatique et des libertés (CNIL)**

**M. Paul Hébert**, directeur adjoint de l'accompagnement juridique

**Mme Nina Le Bonniec**, juriste au service des affaires régaliennes et des collectivités territoriales

**Mme Chirine Berrichi**, conseillère pour les questions institutionnelles et parlementaires

**Fédération française des télécoms (FFT)**

**Mme Muriel Levêque**, directrice des obligations légales de Bouygues Telecom

**M. Franck Laurent,** juriste, Orange

**M. Stéphane Tiberi,** Strategic intelligence Senior Analyst, Orange

**Mme Myriam Madore**, responsable de projets - Maîtrise d'ouvrage au sein de la Direction des Obligations Légales, SFR

**M. Alexandre Galdin**, directeur délégué aux études économiques, à l'environnement et à la sécurité, Fédération Française des Télécoms

## CONTRIBUTIONS ÉCRITES

**Ministère de la justice**

*Direction de programme - Procédure pénale Numérique*

**Ministère de l'intérieur**

*Direction des libertés publiques et des affaires juridiques*

# PROGRAMME DES DÉPLACEMENTS

*Déplacement au tribunal judiciaire de Paris et au commissariat (jeudi 20 juin 2023)*

Commissariat du 17ème arrondissement

**M. Fabrice Corsaut**, commissaire divisionnaire, commissaire central du 17ème arrondissement

**M. Georges Tymen**, commandant divisionnaire, chef du service d'accueil et de l'investigation de proximité

**M. Samuel Cerna**, chef de la brigade des enquêtes d'initiative (démonstration de la PNIJ et du logiciel Mercure)

Parquet de Paris

**Mme Laure Beccuau**, procureur de la République près le Tribunal judiciaire de Paris

**M. Laurent Guy**, procureur de la République adjoint (1ère division)

**M. Antoine Pesme,** secrétaire général

**Mme Emilie Rigaber**, secrétaire générale adjointe

**Mme Sophie Lacote**, 1ère vice procureure (section P12)

**Mme Valérie Cadignan**, 1ère vice procureure (section P20)

**M. Nicolas Barret**, 1er vice procureur (section J2)

**Mme Céline Mietka**, vice procureure (section F3)

**M. François Antona**, vice procureur (section P20)

**Mme Laure Brasseur**, vice procureure (section P20)

**Mme Hélène Collet**, vice procureure (section F3)

**Mme Sophie Gschwind**, substitut (section J3)

*Déplacement à l'agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) (lundi 4 septembre 2023)*

**M. Jean-Julien Xavier-Rolai**, magistrat, directeur de l'Agence

**M. Yves Bronoël,** directeur adjoint

**M. le capitaine Julien Lemercier,** officier de liaison Gendarmerie

**M. Fabrice Valembois,** magistrat, chargé de mission Formation

**Mme Isabelle Guibert,** directrice de projet et relations métiers

**M. Gabriel Ramanatsoavina,** chargé de mission gouvernance du SITENJ

*Déplacement à Bruxelles (lundi 16 octobre 2023)*

Déjeuner avec les autorités belges

**M. Patrick Vandenbruwaene**, procureur général d'Anvers

**M. Frédéric Van Leeuw**, procureur du Parquet fédéral

**M. Robrecht De Keersmaecker**, avocat général près la cour d'appel d'Anvers

**M. Daniel Flore**, directeur général de la législation et des droits fondamentaux au ministère belge de la Justice

**M. Laurent Blondiau**, directeur de la police judiciaire

**M. Steven Limbourg**, directeur du droit pénal au ministère belge de la Justice

Entretien avec la Commission européenne

***Représentation Permanente de la France auprès de l'Union européenne***

**M. Nicolas de Maistre**, préfet, chef du service Justice, Affaires intérieures (JAI) à la Représentation permanente de la France auprès de l'UE

**M. Sylvain Humbert,** conseiller juridique

**Mme Marie Dugre**, conseillère Justice à la Représentation Permanente de la France auprès de l'UE

**Colonel Olivier Pezza**, conseiller affaires intérieures

***Direction générale de la justice (DG Just)***

**Mme Irena Moozova**, directrice générale adjointe

**M. Olivier Micol**, chef de l'unité chargée de la protection des données

**Mme Tania Schroeter**, cheffe adjointe de l'unité chargée de la procédure pénale

***Direction générale des affaires intérieures (DG Home)***

**M. Gilles Robine**, chef d'unité

**M. Ignacio Gomez Navarro**, référent sur l'accès à la donnée

# TABLEAU DE MISE EN ŒUVRE ET DE SUIVI

| N° de la proposition | Proposition | Acteurs concernés | Calendrier prévisionnel | Support |
|---|---|---|---|---|
| 1 | Lever toute ambiguïté quant à la nature des données devant être conservées par les opérateurs. | CCED | 2023 | Mesure administrative |
| 2 | Intégrer dans le code de procédure pénale le faisceau d'indices retenu par la Cour de cassation pour définir la notion de « criminalité grave » | Ministère de la justice | 2024-2027 | Loi |
| 3 | Maintenir au niveau de chaque État membre la définition de ce que recouvre la « criminalité grave », sans en faire une notion autonome du droit de l'Union européenne. | Union européenne | 2024 | Règlement |
| **AGIR EN EUROPE DANS LE SENS D'UN PLUS GRAND PRAGMATISME** | | | | |
| 4 | Obtenir du Gouvernement qu'il rende compte au Parlement des échanges menés dans le cadre du groupe d'experts de haut niveau *Going dark*. | Ministères de la justice et de l'intérieur | 2023-2024 | Mesure administrative |
| 5 | Tirer profit des éventuelles évolutions de la position de la CJUE pour, d'une part, renforcer les souplesses d'accès aux données de connexion en matière de lutte contre les infractions commises en ligne et, d'autre part, envisager un assouplissement du régime d'accès aux adresses IP. | Ministère de la justice | 2024-2027 | Loi |

| N° de la proposition | Proposition | Acteurs concernés | Calendrier prévisionnel | Support |
|---|---|---|---|---|
| **ADAPTER LES NORMES FRANÇAISES À L'IMPÉRATIF D'UN CONTRÔLE PRÉALABLE DES ACCÈS AUX DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES** | | | | |
| 6 | Permettre au parquet d'exercer le contrôle des demandes d'accès aux données de connexion aux seules fins d'identification. | Ministère de la justice | 2024-2027 | Loi |
| 7 | Attribuer la mission de contrôle des accès aux données de connexion au juge des libertés et de la détention. | Ministère de la justice | 2024-2027 | Loi |
| 8 | Prévoir, en cas d'urgence, la possibilité d'un accès aux données de connexion avec une autorisation *a posteriori*. | Ministère de la justice | 2024-2027 | Loi |
| 9 | En cas de choix du juge des libertés et de la détention pour contrôler l'accès aux données de connexion, engager une réflexion sur le statut et les missions de ce magistrat. | Ministère de la justice | 2024-2027 | Loi |
| 10 | Engager une réflexion sur la proportionnalité des actes d'enquête en fonction de leur degré d'intrusion dans la vie privée. | Ministère de la justice | 2024-2027 | Loi |
| **GARANTIR LA FLUIDITÉ DE LA CHAÎNE PÉNALE POUR PROTÉGER LES ACTEURS DE L'ENQUÊTE DU « CHOC PROCÉDURAL »** | | | | |
| 11 | Renforcer la formation des services enquêteurs au maniement de la PNIJ. | ANTENJ | 2024-2027 | Mesure administrative |

| N° de la proposition | Proposition | Acteurs concernés | Calendrier prévisionnel | Support |
|---|---|---|---|---|
| 12 | Soumettre à un contrôle renforcé l'emploi par les services enquêteurs d'outils de retraitement des données de connexion. | Ministères de la justice et de l'intérieur | 2024-2027 | Loi et règlement |
| 13 | Sécuriser l'action des services d'enquête en précisant par circulaire le périmètre des autorisations d'accès aux données de connexion. | DACG | 2024 | Circulaire |
| 14 | Engager un travail sur la forme de la motivation de la demande d'accès aux métadonnées visant à limiter la charge de travail supplémentaire induite par la nouvelle procédure. | Ministère de la justice | 2024-2027 | Mesure administrative |
| 15 | S'imposer, avant l'entrée en vigueur du nouveau contrôle des autorisations d'accès aux données de connexion, de mener à bien le projet procédure pénale numérique (PPN). | Ministère de la justice | 2024-2027 | Mesure administrative |
| 16 | Assurer la modularité des outils créés par les chantiers informatiques sur la procédure pénale numérique (PPN). | Ministère de la justice | 2024-2027 | Mesure administrative |

# ANNEXE 1
# DROIT COMPARÉ - CONSERVATION ET ACCÈS AUX DONNÉES DE CONNEXION DANS L'UNION EUROPÉENNE

## *A. L'ALLEMAGNE*

**A. Un système de conservation des données non-applicable depuis l'arrêt *SpaceNet* du 20 septembre 2022.**

Le précédent régime allemand de conservation des données s'articulait autour de l'article 176 du *Telekommunikationsgesetz* (loi de 2021 relative aux télécommunications, ci-après dénommé « TKG »), qui prévoyait une **obligation de conservation généralisée des données de localisation pour une durée de quatre semaines** et des **données de trafic pour une durée de dix semaines**.

Dans l'esprit du législateur, le régime de conservation posé en 2021 respectait le droit de l'Union européenne dans la mesure où **des limitations strictes étaient apportées**. En sus des courts délais de conservation des données, l'accès à ces dernières était restreint aux fins de répression des infractions pénales graves ou de prévention d'un risque concret pour la sécurité nationale. De plus, l'article 178 du TKG prévoyait la mise en place par les opérateurs de mesures visant à protéger les données conservées, conformément à un catalogue d'obligations techniques élaborées par la *Bundesnetzagentur*. Cette agence fédérale s'assurait du respect par les opérateurs de ces obligations de sécurité et pouvait prendre des mesures pour les y contraindre, pouvant aller jusqu'à interdire l'utilisation des opérateurs concernés (article 183, al. 4, TKG).

Toutefois, dans sa **décision du 20 septembre 2022 *SpaceNet* et *Telekom Deutschland*,** la CJUE a jugé la loi allemande de 2021 relative aux télécommunications non conforme au droit de l'Union européenne[1], confirmant en cela les précédentes décisions des juridictions nationales[2].

La Cour de Justice a, en effet, considéré que la conservation des données de trafic et de localisation « ***présente en tout état de cause un caractère grave indépendamment de la durée de la période de conservation***, *de la quantité ou de la nature des données conservées, lorsque ledit ensemble de données est susceptible de permettre de tirer des conclusions très précises concernant*

[1] *CJUE, 20 septembre 2022, SpaceNet Ag et Telekom Deutschland GmbH (aff. jointes C-793/19, C-794/19).*

[2] *OVG Nordrhein-Westfalen, 22.06.2017 - 13 B 238/17 : le juge des référés de la Cour administrative d'appel de la Rhénanie du Nord – Westphalie décharge ainsi le fournisseur d'accès à Internet, SpaceNet, de l'obligation de stocker les données relatives au trafic et à la localisation de ses clients. Cette décision a été confirmée au fond par le tribunal administratif de Cologne, qui a jugé en avril 2018 que les entreprises SpaceNet et Deutsche Telekom n'étaient pas obligées de respecter la loi de 2015 sur la conservation des données (Verwaltungsgericht Köln, 20 avril 2018 - 9 K 7417/17 et 9 K 3859/16).*

*la vie privée de la ou des personnes concernées* » (point 88). La Cour **écarte également l'argument tendant à compenser un système élargi de conservation des données par un système d'accès plus restreint**, en précisant que « *la conservation de ces données et l'accès à celles-ci constituent (…) des ingérences distinctes dans les droits fondamentaux garantis aux articles 7 et 11 de la Charte, nécessitant une justification distincte* » (point 91).

Dans la droite ligne de la jurisprudence européenne, la loi allemande relative à la conservation des données n'est ainsi définitivement plus appliquée par les juridictions nationales[1] et la *Bundesnetzagentur*[2].

**Les opérateurs allemands ne sont dès lors soumis, à ce stade, à aucune obligation de conservation des données de connexion**. Seules les données permettant de répondre aux besoins commerciaux et techniques des opérateurs sont conservées pour une durée pouvant aller jusqu'à six mois.

**B. Une volonté de réforme à la faveur d'un système d'injonction de conservation rapide des données.**

Annoncé par le ministre de la Justice et encore en discussion au sein de la coalition gouvernementale, **un avant-projet de loi prévoit la possibilité pour les instances répressives d'enjoindre aux opérateurs d'effectuer une conservation rapide de métadonnées**[3].

La mesure ne pourra être prononcée que **pour une durée de conservation d'un mois, renouvelable deux fois**. Seront exigés des indices factuels laissant supposer qu'une infraction grave a été commise et que les données à conserver pourront jouer un rôle pour l'établissement des faits ou la localisation du suspect.

L'initiative appartiendra au ministère public, qui devra en principe adresser sa demande au « juge de l'enquête » (*Ermittlungsrichter*) du tribunal cantonal (*Amtsgericht*). Ce dernier émettra, le cas échéant, une injonction écrite aux opérateurs justifiant de la nécessité et de la proportionnalité de la mesure. En cas de péril imminent, l'injonction peut émaner directement du ministère public, sous réserve de la confirmation de la demande par le juge dans un délai de trois jours ouvrés.

**C. Soumise au contrôle du juge, la procédure allemande d'accès aux données demeure inchangée.**

Selon l'article 100e du *Strafprozeßordnung* (StPO), les mesures de collecte des données sont **ordonnées par le tribunal, sur demande du**

---

[1] *BVerwG, 14.08.2023 - 6 C 6.22 et 6 C 7.22*

[2] *Communiqué de la Bundesnetzagentur d'août 2023, consultable à l'adresse suivante : https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/Ueberwachung_Auskunftsert/VDS_113aTKG/node.html*

[3] *Avant-projet du Ministère fédéral de la justice du 25 octobre 2022 pour l'introduction d'une ordonnance de conservation des données de trafic dans l'ordonnance de procédure pénale, avec motifs, consultable à l'adresse suivante : https://kripoz.de/wp-content/uploads/2022/10/refE-quick-freeze.pdf*

**ministère public**. En cas d'urgence, l'ordonnance peut toutefois être prise par le ministère public, mais doit être confirmée par le tribunal dans un délai de trois jours ouvrables.

L'accès aux données conservées est soumis au respect de plusieurs conditions. D'une part, il nécessite l'existence d'une infraction particulièrement grave, c'est-à-dire susceptible de troubler le sentiment de sécurité publique de la population. La gravité de l'infraction est donc ici indépendante de la peine encourue. D'autre part, il exige l'existence d'un soupçon simple qu'une personne ait été auteur ou complice d'infractions listées à l'article 100a du StPO. Il en résulte que l'accès aux données de tout autre tiers (témoin, victime) est exclu. Enfin, la collecte doit être nécessaire et proportionnée à l'infraction poursuivie.

Pour des infractions ne présentant pas une « *particulière gravité* », un accès aux données peut encore être accordé, en vertu de l'article 100g, alinéa 1er du StPO, lorsqu'elles sont commises avec des moyens de télécommunication. Dans ce cas, en vertu d'une clause de subsidiarité, il est exigé que l'établissement des faits soit difficile ou voué à l'échec par d'autres moyens.

L'avant-projet entend conserver, sous réserve d'un toilettage, les conditions d'accès aux données de connexion telles qu'elles ont été décrites ci-avant, puisque celles-ci apparaissent vraisemblablement conformes aux exigences du droit de l'Union. Par extension, l'accès aux données ayant fait l'objet d'un « quick freeze » obéirait à la même procédure.

## *B. LA BELGIQUE*

### **A. La mise en place en 2022 d'un système mixte conciliant une conservation ciblée et généralisée des données de connexion.**

La Cour constitutionnelle belge a annulé, en 2021, la loi de 2016 sur la collecte et la conservation de métadonnées. Cette dernière imposait une conservation généralisée des données de connexion pour une durée de douze mois et un accès limité dans le temps en fonction de la gravité de l'infraction[1].

Adoptée le 20 juillet 2022, la nouvelle loi en vigueur institue **un système de conservation mixte, à la fois généralisée et ciblée selon le type de données ou la nature de l'infraction**[2].

Les **données d'identification** font, d'une part, l'objet d'une conservation généralisée sur une durée de douze mois pour la lutte contre la criminalité en général[3]. S'agissant des données relatives au trafic et à la localisation, la conservation généralisée est limitée aux fins de détection d'une fraude ou d'une utilisation malveillante des réseaux.

D'autre part, est instauré un **système de conservation ciblée** pour une durée de quatre à douze mois, **fondée sur des critères géographiques**, aux fins de la prévention des menaces graves pour la sécurité publique et de la prévention ou de la poursuite de faits relevant de la criminalité grave. Dans ce cadre, les données sont automatiquement conservées dans les zones particulièrement exposées à des menaces de crimes graves ou d'atteinte à la sécurité nationale (aéroports, gares etc.), ainsi que dans les zones sujettes à un taux important de criminalité grave. Ce taux est constaté par arrondissement judiciaire sur une moyenne de trois ans et rapporté à mille habitants. Il est calculé par le biais de la Banque nationale générale des données (BNG), renseignée par les officiers de police judiciaire.

Le procureur du Roi peut, en outre, ordonner, par une décision motivée, aux opérateurs **le gel rapide des données de trafic et de localisation** pour autant qu'il existe des indices sérieux pouvant donner lieu à une peine d'emprisonnement d'un an ou plus. La durée totale de conservation des données ne peut excéder six mois.

---

[1] *Cour constitutionnelle belge, 22 avril 2021, n°57/2021, point B.17, consultable à l'adresse suivante : https://www.const-court.be/public/f/2021/2021-057f.pdf*

[2] *Loi n° 2022/015454 du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, consultable à l'adresse suivante : http://www.ejustice.just.fgov.be/eli/loi/2022/07/20/2022015454/moniteur*

[3] *Les données d'identification comprennent aussi bien l'identité civile que numérique (adresse IP). Par exception, l'accès aux adresses IP attribuées à la source n'est autorisé qu'aux fins de la lutte contre la criminalité grave, lorsque l'autorité serait en mesure de tracer le parcours de navigation d'un utilisateur final sur Internet (article 127/1, §3, al.4 de la loi du 13 juin 2005, modifiée par la loi du 20 juillet 2022).*

**B. La conformité réelle du système belge aux exigences de la CJUE est cependant sujette à interrogation.**

En somme, la législation belge sur la conservation des données de connexion reprend, en apparence, le modèle exposé dans l'arrêt du 5 avril 2022, *Commissioner of An Garda Síochána* (alinéa 79 à 82)[1]. Pour autant, **les associations de protection des données personnelles dénoncent un simple respect des formes.**

Le législateur belge considère, ainsi, que la conservation généralisée des données de trafic et de localisation peut être justifiée par l'objectif de détection d'une fraude ou d'une utilisation malveillante des réseaux, alors que la CJUE ne réserve cette possibilité qu'aux fins de la sauvegarde de la sécurité nationale[2].

Les critères géographiques retenus pour définir la conservation ciblée permettent, par ailleurs, une couverture vaste du territoire belge. Ainsi, la notion d'infractions graves telle qu'utilisée pour calculer le taux de criminalité est extrêmement large, incluant, à l'article 90ter du code d'instruction criminelle, des infractions de droit commun (fraude, détention de stupéfiants, *etc.*).

Les taux de criminalité assignés aux unités territoriales dépendent, en plus, de la fiabilité des données criminelles enregistrées par les services de police. Or, selon l'Organe de contrôle de l'information policière dans son rapport annuel de 2020, « *la BNG contient de nombreuses inexactitudes et/ou erreurs* » et souligne les trop fréquentes « *qualification(s) erronée(s) conférée(s) aux faits* »[3].

**C. Un contrôle seulement partiel de l'accès aux données de connexion.**

En fonction du type de données, **le système belge ne soumet pas systématiquement les demandes d'accès aux données de connexion au contrôle d'un juge ou d'une autorité administrative indépendante**.

S'agissant des **données d'identification**, la réquisition est ordonnée par le procureur du Roi qui assume le rôle de la partie poursuivante et « *ne peut donc être considéré comme impartial* » selon la Cour constitutionnelle belge[4]. Une décision écrite doit expliciter le caractère proportionné de la demande. Pour les infractions passibles d'une peine d'emprisonnement inférieure à un an, seules les données émises dans les six mois précédant la décision peuvent être demandées.

---

[1] *CJUE, 5 avril 2022, Commissioner of An Garda Siochana (C-140/20).*
[2] *CJUE, 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 168.*
[3] *Organe de contrôle de l'information policière (COC), Rapport d'activité 2020, p. 18.*
[4] *Cour constitutionnelle, 25 janvier 2017, arrêt n°6/2017, C 6325 et 6326, B. 5.2.)*

S'agissant des **données de trafic et de localisation**, la décision est prise par le juge d'instruction (article 88 *bis* du Code d'instruction criminelle). L'accès à ces données est autorisé en présence d'indices sérieux que les infractions sont de nature à entraîner une peine d'emprisonnement d'un an ou plus. Toutefois, un seuil si bas peut difficilement être associé à une infraction grave au sens de la jurisprudence de la CJUE.

Par ailleurs, des exceptions existent. En cas de flagrant délit, la décision peut émaner du procureur du Roi, sous réserve d'une confirmation par le juge d'instruction dans les vingt-quatre heures. Cette dernière n'est pas nécessaire en matière d'infraction terroriste, de prise d'otage, de détention illégale ou d'extorsion.

**Cette approche différenciée de la procédure de collecte des données** en fonction du type de données de connexion et des infractions considérées est susceptible de ne pas être compatible avec **la jurisprudence de la CJUE**, qui exige que toute demande d'accès, sans distinction, fasse l'objet d'un contrôle préalable par une juridiction ou une autorité indépendante[1].

[1] *CJUE, 2 mars 2021, Prokuratuur, aff. (C-746/18).*

### *C. LE DANEMARK*

**A. Un régime modulable qui, dans la pratique, s'est limité à une obligation de conservation généralisée des données.**

En mars 2017, le gouvernement danois a reconnu que la loi de 2007 sur la conservation des données, qui imposait une conservation générale et indifférenciée d'un an, n'était pas conforme au droit de l'UE tel qu'interprété par la CJUE dans l'arrêt *Télé2*[1]. La révision de la loi danoise a été reportée cinq fois, dans l'attente de la décision *La Quadrature du Net*. La nouvelle loi est entrée en vigueur le 8 mars 2022[2].

Cette dernière pose **un système double et alternatif, combinant à la fois une conservation généralisée et une conservation ciblée des données en cas d'infractions graves**. Néanmoins, l'interprétation étendue qui a été faite, lors de l'élaboration de la loi, de l'accès aux données conservées de manière généralisée a rendu le dispositif d'une conservation ciblée inopérant en pratique.

En premier lieu, l'article 786f de la loi sur l'administration de la justice (*Retsplejeloven*) prévoit la **conservation générale et indifférenciée des données d'identification relatives à un utilisateur d'internet**, dont les adresses IP sources, pour la lutte contre la criminalité en général.

En second lieu, en vertu de l'article 786e de cette même loi, le ministre de la Justice peut ordonner la **conservation générale des données s'il y a des raisons de croire que la sécurité nationale du Danemark est gravement menacée**. Les arrêtés sont délivrés pour une période de douze mois[3].

Dans une première interprétation, le gouvernement danois a estimé que les autorités répressives pouvaient accéder à ces données conservées de manière généralisée pour les affaires impliquant des infractions graves et ayant, ainsi, des fins autres que la protection de la sécurité nationale. **.**

**B. Une nouvelle interprétation de la règle de droit tendant à limiter le recours à la conservation généralisée et à mettre en place une conservation ciblée.**

À la suite de la décision *Commissioner of An Garda Síochána*[4] rendue six jours après l'entrée en vigueur de la nouvelle loi danoise, la police

---

[1] *CJUE, 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. (C-203/15 et C-698/15)*

[2] *Loi n°291 du 8 mars 2022 modifiant la loi sur l'administration de la justice et la loi sur les réseaux et services de communication électronique (Lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og –tjenester).*

[3] *Un deuxième arrêté a été émis pour la période du 30 mars 2023 au 29 mars 2024, cf. arrêté n° 337 du 28 mars 2023 (Bekendtgørelse om generel og udifferentieret registrering af trafikdata fra og med den 30. marts 2023 til og med den 29. marts 2024 og opbevaring til og med den 29. marts 2025).*

[4] *CJUE, 5 avril 2022, Commissioner of An Garda Siochana (C-140/20)*

nationale danoise et le Procureur général sont revenus sur leur première interprétation et ont restreint, par voie de circulaire, l'accès de leurs services aux données conservées à des fins de protection de la sécurité nationale[1].

En conséquence, **à compter de juin 2022, le gouvernement a eu recours à une conservation géographique ciblée**. Celle-ci était rendue possible par deux articles de la loi de mars 2022, jusqu'alors non appliqués et autorisant une conservation ciblée des données, en cas d'infraction grave et pour une durée d'un an. Une telle mesure de conservation est établie en fonction de catégories de personnes (article 786b de la loi sur l'administration de la justice) ou de critères géographiques (article 786c).

En vertu de l'article 786b, la conservation ciblée des données est automatique **pour les personnes condamnées pour des infractions pénales graves** et cela pendant une période comprise entre trois et dix ans, ainsi que pour les numéros de téléphone qui ont fait l'objet d'une ordonnance d'interception des communications.

Conformément à l'article 786c, une zone sur le territoire danois de 3 km² sera automatiquement couverte par une conservation ciblée des données **si le nombre d'infractions pénales graves signalées à la police ou le nombre de résidents locaux condamnés pour des infractions pénales graves est supérieur à 1,5 fois la moyenne nationale au cours des trois dernières années**. La conservation des données visées à l'article 786c comprend également des « *zones critiques pour la sécurité* ». Y sont listés différents types de bâtiments institutionnels et d'infrastructures tels que les palais royaux, les ponts et les gares[2].

La loi de mars 2022 met également en place des **procédures de conservation rapide des données existantes (*quick freeze*)**, d'une part, **et des données produites en temps réel ou dans le futur (*future freeze*)**, d'autre part. En premier lieu, pour la poursuite des infractions graves[3], l'article 786a autorise la police à enjoindre aux opérateurs de sauvegarder, pour une période de 90 jours renouvelable, les métadonnées conservées au moment de la demande. En second lieu, l'article 786d permet au juge d'ordonner la conservation ciblée, pour une durée maximum de six mois renouvelable, des données concernant des personnes ou des zones spécifiques s'il y a des raisons de penser qu'elles sont liées à des infractions graves.

---

[1] *Réponse du Ministre de la Justice à la question n° 776 posée le 7 avril 2022 par la commission des affaires juridiques du Parlement danois, consultable à l'adresse suivante : https://www.ft.dk/samling/20211/almdel/reu/spm/776/svar/1874527/2560122.pdf*

[2] *De manière exhaustive, sont compris les palais royaux, le Parlement, la résidence du Premier Ministre, les ambassades, les commissariats, les prisons, les zones militaires, les industries dangereuses (par exemple les explosifs), les ponts, les tunnels, les intersections de trafic et les routes principales, les points de passages frontaliers, les gares ferroviaires et le métro.*

[3] *Les infractions graves comprennent notamment celles passibles d'une peine d'emprisonnement de trois ou plus (art. 786a, §1).*

**Le caractère « ciblé » du nouveau régime de conservation apparait néanmoins relatif.** En effet, la mesure se fonde sur le nombre brut, et non rapporté à la population, d'infractions ou de condamnations sur un territoire : par conséquent, les villes les plus peuplées sont inévitablement intégrées au « ciblage ».

La police nationale danoise a estimé que la conservation des données ciblées couvre 11 % de la zone géographique du Danemark et 67 % de la population[1].

À l'heure actuelle, le ministère de la Justice continue de travailler avec les opérateurs pour clarifier les possibilités de mise en œuvre des autres modalités de la conservation ciblée. **La pratique d'un accès restreint aux données conservées de manière généralisée pour les besoins de sécurité nationale n'est**, d'ailleurs, **pas encore entérinée par la loi**. En réponse à une question parlementaire sur le sujet, le gouvernement a annoncé qu'un projet de loi, annoncé depuis avril 2022, sera éventuellement soumis au Parlement lors de la session parlementaire 2023-2024[2].

**C. Une procédure d'accès aux données de connexion contrôlée par un juge, conformément aux exigences de la CJUE.**

L'accès aux données de connexion ne peut être accordé aux autorités répressives que **sous trois conditions** (article 781 de la loi sur l'administration de la justice) :

- s'il existe certaines raisons de supposer que des communications sont effectuées à destination ou en provenance d'un suspect ;
- si ces données sont présumées être d'une importance décisive pour l'enquête ;
- si l'enquête concerne une infraction punissable par la loi d'une peine d'emprisonnement de trois ans et plus ou une infraction liée à des conflits entre bandes violentes.

**Il revient au tribunal de statuer par ordonnance sur le respect de ces trois conditions** (article 783 de la loi sur l'administration de la justice). L'ordonnance précise le délai dans lequel l'intervention peut être effectuée. Il ne peut excéder 4 semaines, mais peut être renouvelé.

En cas d'urgence, la police peut décider de procéder à la collecte, mais doit saisir le tribunal au plus tard dans les vingt-quatre heures. Le tribunal autorise *a posteriori* l'intervention et statue sur la durée de son

---

[1] *Réponse du ministre de la Justice à la question n° 62 relative au projet de loi L. 93 posée le 25 janvier 2022 par la commission des affaires juridiques du Parlement danois, consultable à l'adresse suivante : https://www.ft.dk/samling/20211/lovforslag/L93/spm/62/svar/1852881/2524089.pdf*

[2] *Réponse du ministre de la Justice à la question n°133 relative à la proposition de loi de finances pour l'exercice 2023 (L 207) posée le 19 septembre 2022 par la commission des finances du Parlement danois, consultable à l'adresse suivante : https://www.ft.dk/samling/20211/lovforslag/l207/spm/133/index.htm*

maintien. Si l'intervention est jugée illicite, le tribunal en avise le procureur général, qui le signale au ministère de la Justice.

### *D. L'ESTONIE*

A. Un régime d'accès et de conservation des données de connexion modifié pour prendre en compte les dernières évolutions de la jurisprudence de la CJUE.

**1. Des garanties supplémentaires en matière d'accès aux données de connexion**

À la suite de l'arrêt *Prokuratuur* de la Cour de justice de l'Union européenne du 2 mars 2021[1] prononcé dans le cadre d'un renvoi préjudiciel formulé par la juridiction suprême estonienne, **le législateur estonien a modifié le code de procédure pénale en 2022 afin de mieux encadrer l'accès aux données de connexion**. Les données de trafic et de localisation ne sont désormais accessibles que sur décision de la juridiction - et non plus du procureur -, la requête ne pouvant cibler que des données conservées par les opérateurs pour leurs besoins propres. Par ailleurs, d'après les réponses apportées par le ministère de la justice estonien au questionnaire adressé par les rapporteurs, l'accès aux métadonnées est limité à la lutte contre la délinquance organisée[2].

L'Estonie a par ailleurs **renforcé l'information des citoyens** sur l'usage des données de connexion dans le cadre des enquêtes pénales puisque les opérateurs sont tenus de fournir annuellement à l'Autorité de la protection des consommateurs et de la régulation technique le nombre de requêtes et les délais de conservation. L'Autorité a l'obligation de publier ces informations sur son site internet et de les transmettre à la Commission européenne[3].

**2. Un régime de conservation généralisée révisé à la marge**

Si le régime de conservation a été adapté à la marge pour prendre en compte les évolutions du droit européen, **le législateur estonien n'a pas souhaité mettre en œuvre un système de conservation ciblée, système jugé « *irréaliste et inopérant* »[4] pour des raisons à la fois techniques et juridiques** tenant notamment à **l'impossibilité de définir des critères de ciblage non discriminatoires.**

---

[1] *CJUE, 2 mars 2021, Prokuratuur, aff. (C-746/18).*

[2] *« Access to data is limited and only possible in case of serious offences », réponse du ministère de la justice au questionnaire adressé par les rapporteurs.*

[3] *Article 112 de la loi sur les communications électroniques du 8 décembre 2004.*

[4] *Source : réponse du ministère de la justice estonien au questionnaire adressé par la mission d'information.*

**L'Estonie a donc conservé un régime de conservation généralisée des données tout en limitant la durée de conservation à douze mois pour les données d'identification, de trafic et de localisation.** Cette période peut être prorogée, pour une durée limitée, pour la sauvegarde de l'ordre public et de la sécurité nationale, en informant la Commission européenne et les États membres de cette décision.

**B. Malgré la réforme de l'accès aux données de connexion, un régime de conservation généralisée des données qui pose encore question au regard du droit de l'Union.**

Même si elle s'est efforcée de se conformer aux exigences du droit de l'Union en matière d'accès, **l'Estonie a choisi de maintenir un système de conservation généralisée et indifférenciée des données, indépendamment de la nature des données et des finalités poursuivies.**

*L'IRLANDE*

**A. Un nouveau régime légal de conservation des données adopté en urgence pour prendre en compte l'évolution de la jurisprudence européenne.**

La **loi du 21 juillet 2022 dite « *Communications (Retention of Data) (Amendement) Act 2022* »** a été adoptée en procédure accélérée en moins de trois semaines[1] à la suite de l'arrêt de la Grande chambre de la CJUE du 5 avril 2022, *Graham Dwyer c/ Commissioner of An Garda Síochánax*[2] qui, dans le cadre d'une question préjudicielle adressée par la Cour suprême d'Irlande, a confirmé que **la loi irlandaise de 2011 sur les données de connexion n'était pas conforme au droit de l'Union.**

Auparavant, le législateur irlandais n'avait pas souhaité modifier la législation en vigueur depuis 2011 malgré son invalidation par la CJUE par la décision du 8 avril 2014, *Digital Rights Ireland*[3]. L'ancien régime prévoyait la conservation générale et indifférenciée des métadonnées pour une période de 2 ans et autorisait l'accès à ces données sans contrôle préalable et indépendant.

**Le nouveau régime de conservation réduit le champ des données concernées et prévoit que la durée légale de conservation varie en fonction de la nature des données et de la finalité poursuivie.** Cette durée peut être adaptée par décision ministérielle ou judiciaire, dans le strict respect des principes de nécessité et de proportionnalité.

Pour les données d'identité civile et numérique, la durée de conservation, fixée à un an, peut être rallongée sur décision ministérielle ; cette prolongation peut aller jusqu'à une année supplémentaire dans le cadre de la lutte contre la criminalité en général, et peut aller au-delà d'un an en matière de lutte contre la criminalité grave ou la sauvegarde de la sécurité nationale. La conservation des données de trafic et de localisation est restreinte à la lutte contre une menace sérieuse et réelle, actuelle et prévisible pour la sécurité nationale, sur décision du juge compétent et pour une durée d'un an, conformément aux exigences fixées par la Cour de justice de l'Union européenne.

**B. Un contrôle de l'accès dont la rigueur varie en fonction de la nature des données concernées.**

La procédure d'accès aux données de connexion et les modalités de son contrôle varient en fonction de la nature des données. Les données

---

[1] *Le projet de loi a été déposé devant le Parlement le 4 juillet 2022 et promulgué le 21 juillet 2022. La loi est entrée en vigueur le 26 juin 2023 à l'issue de la procédure d'information prévue par la directive (UE) 2015/1535 qui permet à la Commission européenne de formuler des observations.*

[2] *CJUE, 5 avril 2022, Commissioner of An Garda Siochana (C-140/20).*

[3] *CJUE, 8 avril 2014, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a. (C-293/12).*

d'identification des utilisateurs sont directement accessibles aux agents habilités à y accéder, sans contrôle judiciaire. En revanche, le juge du tribunal de district compétent doit autoriser l'accès aux données des sources internet et aux données de trafic, tandis que l'accès aux données de localisation de l'équipement terminal doit être autorisé par le supérieur hiérarchique de l'agent puis validé *a posteriori* par le juge qui effectue un contrôle de proportionnalité.

La liste des autorités habilitées à accéder aux données de connexion demeure large, la loi irlandaise permettant à certains agents (ceux de l'administration fiscale et de la Commission de la concurrence et de la protection des consommateurs) une possibilité d'accès aux métadonnées pour d'autres motifs que la lutte contre la criminalité grave.

**C. Des doutes subsistent quant à l'effectivité et à la conformité de la législation irlandaise au droit de l'Union.**

**La conformité totale au droit de l'Union reste à confirmer** car ni les juges nationaux, ni le juge européen ne se sont prononcés sur cette question.

La procédure d'adoption de la loi du 21 juillet 2022 précitée a été vivement critiquée par l'opposition, la société civile et les institutions européennes, le texte ayant été promulgué 17 jours seulement après son dépôt devant le Parlement[1]. **Des doutes subsistent donc quant à l'efficacité et l'applicabilité du nouveau régime légal de conservation des données qui, au regard des délais d'examen du texte, n'ont pas pu être correctement anticipés par les pouvoirs publics irlandais.** Le projet de loi n'ayant pas été notifié à la Commission européenne dans les délais prévus par la procédure d'information dite « *TRIS* » prévue par la directive (UE) 2015/1535 qui permet à la Commission de formuler des observations, l'entrée en vigueur de la loi a été repoussée au 26 juin 2023.

[1] *Le projet de loi a été déposé devant le Parlement le 4 juillet 2022 et promulgué le 21 juillet 2022. La loi est entrée en vigueur le 26 juin 2023 à l'issue de la procédure d'information prévue par la directive (UE) 2015/1535 qui permet à la Commission européenne de formuler des observations.*

*L'ITALIE*

**A. Un régime d'accès aux données de connexion adapté pour tenir compte de l'évolution de la jurisprudence européenne.**

Le régime italien d'accès aux données de connexion a été modifié par le **décret-loi n° 132 du 30 septembre 2021** adopté après l'arrêt *Prokuratuur* de la Cour de justice de l'Union européenne[1].

Désormais, les données qui font l'objet de la requête sont acquises auprès de l'opérateur à la demande du procureur de la République ou de l'avocat de la personne mise en cause, de la personne mise en examen, de la victime et des parties civiles et sur **ordre motivé du juge**. En cas d'urgence, le procureur de la République peut ordonner lui-même l'accès aux données, par une décision motivée communiquée au juge. Si le juge n'a pas validé la requête dans un délai de 48 heures, les données acquises ne peuvent être utilisées.

Par ailleurs, **la réforme de 2021 a limité l'accès aux métadonnées aux seuls cas de commission d'infractions graves.**

**B. Un régime de conservation qui demeure en contradiction avec la jurisprudence de la CJUE.**

**L'Italie a en revanche maintenu un régime de conservation généralisée dont la conformité au droit de l'Union pose question**. L'article 132 du code de la vie privée prévoit un régime de conservation qui couvre tous les moyens de communication électronique et tous les utilisateurs de ces moyens, sans distinction. La législation italienne prévoit également **une procédure de conservation rapide dite « *quick freeze* »** pour une durée de 90 jours prorogeable, sous certaines conditions, jusqu'à six mois. La conservation rapide peut être ordonnée pour les besoins d'une enquête visant la prévention d'infractions graves ou dans le but de la constatation et de la poursuite d'infractions spécifiques. L'ordre de conservation rapide doit être communiqué dans un délai de 48 heures au procureur de la République pour contrôle et validation. Il peut définir, le cas échéant, des modalités particulières de conservation des données et prévoir l'indisponibilité des données visées pour les opérateurs, les fournisseurs ou les tiers[2].

**La Cour de cassation italienne a jugé à plusieurs reprises que les règles internes étaient conformes aux principes consacrés par la CJUE** dans la mesure où, notamment, celles-ci limitent la durée de conservation dans le temps et confient à l'autorité judiciaire le contrôle effectif de l'accès aux

[1] *CJUE, 2 mars 2021, Prokuratuur, aff. (C-746/18).*

[2] *Source : étude sur la conservation des données de connexion et les modalités d'accès à ces données dans le cadre d'une enquête judiciaire (Allemagne, Belgique, Irlande, Italie, Suède) commandée par la direction des affaires européennes et internationales du ministère de la justice (1er mars 2023).*

données[1]. Les délais de conservation généralisée des données varient en effet entre 30 jours et six ans en fonction de la nature de la donnée et de la finalité poursuivie[2]. Cependant, les opérateurs ignorant, en amont, le type d'infractions justifiant l'accès aux données de connexion, ils se voient dans l'obligation de conserver l'ensemble des données pour une durée de six ans.

De même, **la législation italienne prévoit la conservation des données aux fins de lutte contre la criminalité en général et non pas uniquement en matière de criminalité grave, en opposition aux principes dégagés par la Cour de justice de l'Union européenne** dans l'arrêt *La Quadrature du Net et autres* du 6 octobre 2020[3]. Cependant, « *ces dispositions ne s'appliquent pas, faute de droit d'accès*[4] » car l'étendue du régime de conservation des métadonnées entre en contradiction directe avec le régime d'accès très restrictif qui ne permet par l'accès à ces données dans le cadre de la lutte contre la criminalité en général.

[1] *Cass., sez. V, 24 avril 2018, n. 33851 ; sez. III, 23 août 2019, n. 36380 ; sez. II, 10 décembre 2019, n. 5741. À l'inverse, la doctrine italienne et le Garant de la vie privée ont à plusieurs reprises dénoncé l'incompatibilité du régime légal italien et du droit de l'Union, même si la CJUE ne s'est pas prononcée, à ce jour, sur cette question.*

[2] *Dans le cadre de la lutte contre la criminalité grave, les données sont conservées pendant 72 mois. Dans le cadre de la lutte contre la criminalité en général, les données téléphoniques sont conservées durant 30 jours (pour les appels sans réponse), 12 mois (pour les données télématiques) ou 24 mois (pour les données téléphoniques).*

[3] *CJUE, 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a. (C-511/18).*

[4] *Source : étude sur la conservation des données de connexion et les modalités d'accès à ces données dans le cadre d'une enquête judiciaire (Allemagne, Belgique, Irlande, Italie, Suède) commandée par la direction des affaires européennes et internationales du ministère de la justice (1er mars 2023).*

### *E. LA LETTONIE*

La législation lettone relative à la conservation et à l'accès aux données de connexion est établie par la **loi sur les procédures pénales du 21 avril 2005** et la **loi sur les communications électroniques du 14 juillet 2022**.

À ce jour, La Lettonie **n'a pas fait évoluer sa législation** pour tenir compte de la jurisprudence européenne en matière de conservation et d'accès aux données de connexion. Un **groupe de travail *ad hoc*** a toutefois été constitué à l'initiative du ministre des transports, compétent en matière de communications électroniques, dans le but de **formuler des amendements** permettant une **mise en conformité** au regard des **exigences de la CJUE** en la matière.

#### **A. L'absence de restriction selon la nature des données ou à la finalité poursuivie en matière de conservation des données de connexion**

La loi sur les communications électroniques du 14 juillet 2022 n'a pas modifié les dispositions applicables jusqu'alors en matière de conservation de données de connexion. Ainsi, les **fournisseurs de services de communication électronique** ont l'**obligation de conserver** les **données d'identification**, **de trafic** et **de localisation pendant dix-huit mois**.

#### **B. Un contrôle préalable de l'accès aux données de connexion exercé sans garantie d'indépendance**

Les **finalités de nature à justifier l'accès** aux données de connexion recouvrent un **large champ** : la législation relative à l'utilisation des données stockées par les fournisseurs de services de communication électroniques à des fins d'enquête prévoit la possibilité de recourir au « *traitement des données pertinentes pour **détecter, prouver, prévenir les infractions pénales**, les **infractions administratives pertinentes**, ainsi que pour **prévenir les menaces à la sécurité nationale*** »[1].

En ce qui concerne la **procédure d'accès aux données de connexion**, la loi sur les procédures pénales lettone dispose que :

- **en amont d'un procès**, un enquêteur, sur **autorisation du procureur**, d'un **procureur de rang supérieur** ou de la **personne concernée** par les données, peut **demander à un opérateur de télécommunication** de lui **transmettre des données** qu'il conserve, conformément aux procédures prévues par la loi sur les communications électroniques ;
- **à l'occasion d'un procès pénal**, le **juge** ou la formation de jugement peut **demander à un opérateur de télécommunication** la **transmission de données** conservées, selon les procédures susmentionnées.

[1] *Source : réponse au questionnaire adressé à l'ambassade de France en Lettonie.*

Par **dérogation** au principe de l'**autorisation préalable** du juge ou du procureur, l'*Operational activity law* admet « *la* ***possibilité de traiter des données*** *qui* ***n'affectent pas de manière significative la vie privée*** *d'une personne* »[1] pendant une **période maximale de trente jours sans contrôle préalable** de l'autorité judiciaire.

La **procédure d'accès** prévue par la législation lettone, en ce qu'elle confie au **procureur** la **responsabilité d'autoriser** les enquêteurs à accéder aux données de connexion dans le cadre des enquêtes pénales, **contrevient à l'exigence d'indépendance** de l'autorité chargée du contrôle, dégagée dans l'arrêt de la CJUE du 2 mars 2021[2].

**C. Une volonté de mise en conformité au regard de la jurisprudence européenne**

À l'initiative du ministère des transports letton, un **groupe de travail *ad hoc*** a été créé afin de préparer des **modifications à la loi du 14 juillet 2022**.

L'objectif est de **faire évoluer le dispositif actuel** pour prendre en compte les conclusions de la CJUE, notamment en ce qui concerne :

- l'**introduction d'une conservation des données ciblée** en fonction de critères tenant à la **gravité de l'infraction** et à la **zone géographique** d'une part ;
- le **choix de l'autorité chargée d'exercer un contrôle préalable** à l'accès à ces données d'autre part.

Dans ses réponses apportées au questionnaire adressé dans le cadre de la présente mission, l'ambassade de France en Lettonie souligne toutefois la **crainte des autorités judiciaires lettones et des services de renseignement** quant aux **effets de la limitation des informations** qu'elles pourront obtenir à l'avenir, mais aussi quant **au « *travail considérable* *à entreprendre pour* ***mettre en conformité le droit letton*** *et les* ***procédures internes*** »[3] vis-à-vis de la jurisprudence européenne.

[1] *Source : réponse au questionnaire adressé à l'ambassade de France en Lettonie*
[2] *Affaire C-746/18, « Prokuratuur ».*
[3] *Source : réponse au questionnaire adressé à l'ambassade de France en Lettonie*

### *F. LA LITUANIE*

La législation lituanienne relative aux données de connexion est établie par la **loi sur les communications électroniques du 15 avril 2004** en ce qui concerne leur **conservation**, et par des **lois sectorielles** – loi sur le renseignement, loi sur le renseignement criminel ou code de procédure pénale – en ce qui concerne l'**accès**.

**Aucune évolution législative** n'est intervenue en Lituanie **à la suite de l'arrêt *Quadrature du Net et autres*** rendu par la CJUE le 6 octobre 2020. Si un **groupe d'experts** a été **constitué** à l'initiative du ministre de la justice afin de définir, le cas échéant, les **mesures à adopter** pour mettre en conformité la loi lituanienne au droit de l'Union européenne, **aucune modification législative n'est prévue à ce jour**.

#### A. Une conservation généralisée des données de connexion pour une durée comprise entre six et douze mois

Conformément à l'article 77 de la loi sur les communications électroniques du 15 avril 2004, les fournisseurs de services de télécommunications sont tenus de **conserver** et de **mettre à disposition** les **données d'identification, de trafic et de localisation** qu'ils détiennent pour une **durée de six mois**.

Afin de **garantir l'accès aux données** dans le but de « ***prévenir, rechercher, détecter et poursuivre les crimes**, ou des **menaces** qui affecteraient la **souveraineté**, l'**intégrité du territoire**, l'**ordre constitutionnel**, les **intérêts de l'État**, la **défense** ou le **pouvoir économique*** »[1], la **durée de conservation** des données de connexion peut être **prorogée** pour une durée additionnelle de six mois maximum, soit **douze mois au total**.

Nonobstant l'existence d'une **durée de conservation différenciée** des données de connexion **selon la finalité poursuivie**, la législation lituanienne prévoit ainsi **une conservation généralisée de ces données** pendant au moins **six mois**.

#### B. Un contrôle judiciaire préalable de la demande d'accès aux données de trafic et de localisation

L'**autorité judiciaire** est chargée de **contrôler les demandes d'accès** aux données de trafic et de localisation conservées. Elle se prononce, par **décision de justice**, sur les demandes formulées. L'**accès aux données d'identification** des abonnés n'est en revanche **soumis à aucune procédure de contrôle** préalable.

#### C. Un *statut quo* de la législation lituanienne à court terme

Dans ses réponses au questionnaire adressé dans le cadre de la présente mission, le **ministère de la justice lituanien** indique avoir **constitué**

[1] *Source : réponse du ministère de la justice lituanien au questionnaire.*

**un groupe de travail** composé d'experts et chargé d'**analyser** les **arrêts de la CJUE** et les **documents** examinés par les groupes de travail du **Conseil de l'Union européenne** relatifs à la conservation des données, d'**évaluer** leur **impact sur le droit national**, et de **contribuer à façonner** la **position de la Lituanie** sur les questions de conservation des données.

Toutefois, il **n'existe pas**, à ce jour, de **projet visant à amender la législation nationale** en vue d'une éventuelle mise en conformité au regard de la jurisprudence européenne.

## *G. LES PAYS-BAS*

### A. L'absence de toute obligation légale de conservation des données comme conséquence de la suspension de l'ancien régime juridique.

La loi du 18 juillet 2009 modifiant la loi sur les télécommunications (*Wet bewaarplicht telecommunicatiegegevens*) avait introduit, à des fins d'enquête et de poursuites d'infractions pénales graves, une obligation de conservation généralisée des données de connexion pendant six mois pour les données internet et jusqu'à douze mois pour les données téléphoniques.

**Ce dispositif a toutefois été suspendu par le juge des référés du tribunal de La Haye le 11 mars 2015**[1] au motif d'une violation des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Aucun appel n'a depuis été interjeté ni aucune procédure engagée sur le fond.

Depuis mars 2015, **les opérateurs ne sont donc plus tenus de conserver les données de connexion de leurs utilisateurs**. Seules les données conservées pour répondre aux besoins commerciaux des opérateurs eux-mêmes peuvent, dès lors, faire l'objet de réquisitions par les autorités répressives, qui ont émis à ce titre 35 130 demandes en 2017 et 34 221 en 2018[2].

### B. Une procédure peu encadrée d'accès aux données qui a été également suspendue par le tribunal.

Sur le fondement de la loi de 2009 précitée, l'accès aux données est limité aux infractions terroristes ou aux infractions pour lesquelles la détention provisoire est autorisée, c'est-à-dire celles qui sont punies d'une peine d'emprisonnement d'au moins quatre ans. Or, comme souligné par la décision du 11 mars 2015 du tribunal de la Haye, la détention provisoire est possible pour des délits comme le vol d'une bicyclette, ce qui a conduit le juge des référés à conclure à **l'absence de garanties limitant l'accès aux données à ce qui est strictement nécessaire pour lutter contre la seule criminalité grave.**

Le juge des référés de La Haye a, en outre, jugé que le procureur, qui émet la réquisition d'accès aux données, ne pouvait être considéré comme une autorité indépendante au sens de la jurisprudence de la Cour de Luxembourg. Il en a déduit que l'accès aux données conservées **n'était pas soumis au contrôle préalable d'une autorité judiciaire ou administrative indépendante, en contradiction avec les exigences définies par la CJUE**[3].

---

[1] *Tribunal de La Haye, 11 mars 2015, C/09/480009 / KG A 14/1575.*

[2] *Réponse n° 178 (2019-2020) aux questions du député Van der Graaf sur l'article "Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark".*

[3] *CJUE, 2 mars 2021, Prokuratuur, aff. (C-746/18)*

**C. La mise en place contrariée d'un nouveau régime juridique en matière de conservation des données et d'accès à celles-ci.**

En réponse à ces développements, en septembre 2016, un projet de loi (*Aanpassing bewaarplicht telecommunicatiegegevens*) a été soumis à la Chambre des représentants néerlandaise[1]. Il prévoit **un nouveau régime d'accès aux données de connexion**, en amendant les articles 126n et 126u du Code de procédure pénale (*Wetboek van Strafvordering*), afin que la réquisition ne puisse être faite qu'après accord du juge d'instruction. Dans ce cadre, il appartient au procureur de la République, qui émet la demande, puis au juge d'instruction, qui la valide, d'apprécier si la gravité du délit justifie la réquisition des données de connexion conservées. En cas d'urgence, la demande et sa validation peuvent être faites oralement, à condition d'être actées par écrit dans un délai de trois jours.

Le gouvernement néerlandais reconnaît toutefois, dans son exposé des motifs, que **la nouvelle procédure de réquisition des données de connexion** « ***aura de graves conséquences financières et organisationnelles pour la police, le ministère public et la magistrature en exercice*** »[2]**.** Selon leurs estimations, le nombre de demandes portées devant le juge d'instruction augmentera structurellement, avec environ 42 000 demandes supplémentaires par an, pour des coûts supplémentaires d'environ deux millions d'euros par an.

En outre, si le projet de loi initial tendait à modifier les seules modalités d'accès aux données de connexion, il maintenait un régime de conservation générale et indifférenciée, selon des délais de conservation inchangés. Dès lors, à la suite de l'arrêt *Tele2 Sverige* du 21 décembre 2016[3] qui exclut formellement le recours à une conservation généralisée et indifférenciée des données pour les affaires de criminalité grave, le ministre de la Justice néerlandais a annoncé au Parlement **son intention de modifier le projet de loi afin de limiter l'obligation de conservation aux seules données d'identification**[4].

L'examen du texte a été repoussé pour des besoins d'expertise supplémentaire concernant la prise en compte du dispositif *carrier grade network address translation (CGNAT)*, utilisé par les fournisseurs d'internet afin de regrouper une centaine de connexions internet sous une seule adresse IPv4[5].

---

[1] *Projet de loi n°34 537, déposé le 13 septembre 2016, modifiant la loi sur les télécommunications et du code de procédure pénale concernant la conservation des données traitées dans le cadre de la fourniture de services publics de télécommunications et de réseaux publics de télécommunications.*
[2] *Exposé des motifs du projet de loi n° 34 537, p. 30.*
[3] *CJUE, 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. (C-203/15 et C-698/15)*
[4] *Lettre du ministre de la Justice à la chambre des représentants du 26 mars 2018.*
[5] *Lettre du ministre de la Justice à la chambre des représentants du 25 septembre 2018.*

Le rapport d'expertise a été publié en 2019[1] et propose notamment d'imposer de nouvelles obligations aux opérateurs. Pour autant, depuis mars 2018, le processus législatif est au point mort. Aucun projet de loi modifié n'a encore été déposé.

[1] *Zie T. van der Vorst, e.a., Mogelijkheden voor identificatie op internet op basis van IP-adres, Dialogic in opdracht van het WODC (Ministerie van Justitie en Veiligheid), Den Haag: nov. 2019*

### *H. LA POLOGNE*

La **législation polonaise** sur la conservation et l'accès aux données de connexion n'a quasiment **pas évolué** depuis la **loi du 15 janvier 2016** modifiant la loi sur la police et organisant la rétention de données et l'accès à celles-ci. Le **droit en vigueur** en Pologne est donc resté **hermétique** aux jurisprudences récentes de la CJUE.

Dans un courrier du Médiateur de la République polonais adressé au Premier ministre en date du 6 janvier 2023, celui-ci fait état de la **non-conformité** des dispositions prévoyant des **mesures préventives et généralisées de collecte** et de **rétention indifférenciée des données** avec les normes internationales et européennes, définies dans la jurisprudence de la CJUE.

#### A. Un régime de conservation des données généralisée et indifférenciée

Les articles 180a et 180c de la loi du 16 juillet 2004 sur les télécommunications disposent que les opérateurs de télécommunications sont tenus de **conserver et de stocker les données d'identification**, de **trafic** et de **localisation**, générées dans le réseau de télécommunication ou traitées par eux, pour une **durée de douze mois**[1].

Les **données de connexion** font donc l'objet d'une **conservation généralisée et indifférenciée**. Les dispositions législatives polonaises ne prévoient **pas de régime différencié** de conservation selon le double critère de la nature des données collectées et de la finalité de leur conservation.

Comme le souligne l'**ambassade de France en Pologne** dans ses réponses au questionnaire qui lui a été adressé dans le cadre de la présente mission d'information, « ***le droit polonais n'a pas été mis en conformité avec le droit européen*** *depuis l'arrêt Quadrature du Net,* ***ni s'agissant de la conservation des données de connexion*** *(durée, motifs),* ***ni concernant l'accès à ces données*** *(motifs invoqués, contrôle des données recueillies par un organisme indépendant)* ».

#### B. Un encadrement *a minima* de l'accès aux données de connexion au regard de la finalité poursuivie

S'agissant des infractions à caractère pénal, les **services relevant du ministre chargé des affaires intérieures** – à savoir la police, les gardes-frontières et le service du renseignement intérieur – sont **autorisés à obtenir communication** des données conservées par les entreprises de télécommunication dans le cadre de la **« *reconnaissance opérationnelle*** *menée au nom de la* ***prévention*** *et de la* ***détection*** *des* ***crimes*** *et des* ***infractions fiscales*** »[2].

---

[1] *Avant 2012, la durée de conservation des données de connexion était de 24 mois.*

[2] *Source : réponses au questionnaire adressé à l'ambassade de France en Pologne.*

La notion « *d'opération de reconnaissance opérationnelle* » a été **précisée** dans la loi du 15 janvier 2016 modifiant la loi sur la police afin de **limiter l'accès aux données** par les autorités de police **au strict nécessaire**. Depuis lors, la demande d'accès doit être **ciblée**, c'est-à-dire qu'elle doit être liée à une **personne, un lieu ou un appareil clairement identifié.** Toutefois, cette évolution législative **ne répond pas aux enjeux identifiés par la jurisprudence de la CJUE** en matière de conservation des données de connexion.

**C. L'absence d'un contrôle effectif et indépendant préalable à l'accès aux données de connexion en pratique**

Plusieurs dispositions législatives prévoient **l'encadrement, par l'autorité judiciaire, de l'accès aux données de connexion**. L'article 218 du code de procédure pénale dispose que les opérateurs de télécommunications « *sont tenus de* ***fournir aux juridictions ou au procureur*** […] *les* ***données visées à l'article 180c*** *et à l'article 180d de la loi du 16 juillet 2004 sur les télécommunications* […]. ***Seul une juridiction ou le procureur*** *a le* ***droit de les ouvrir*** *ou* ***d'en ordonner l'ouverture*** »[1].

À cette procédure de contrôle *a priori* s'ajoute une **procédure de contrôle *a posteriori*** par les **tribunaux de districts** compétents, sur le fondement de **rapports semestriels** recensant les données auxquelles la police et les autres entités autorisées ont pu accéder.

En pratique toutefois, l'ambassade de France en Pologne relève « ***l'absence d'un contrôle effectif et indépendant*** » de l'action des services d'enquête nationaux en matière de données de connexion[2]. En effet, le **procureur polonais**, chargé d'effectuer un contrôle *a priori* sur les demandes d'accès aux données de connexion, **ne semble pas disposer** des **caractéristiques d'une « *juridiction* »** au sens de la CJUE du fait de son **insuffisante indépendance vis-à-vis de l'enquête**[3].

[1] *Réponse de la Pologne à la requête de la Lettonie sur la conservation des données en date du 19 juin 2023 dans le cadre du réseau de coopération législative des ministères de la Justice de l'Union européenne (RECL - LEGICOOP)*

[2] *Source : réponses au questionnaire adressé à l'ambassade de France en Pologne.*

[3] *Paragraphe 32 - REPORT of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware | A9-0189/2023 | European Parliament (europa.eu)*

## *I. LA SLOVAQUIE*

### **A. Un système qui depuis 2015 fonctionne sans obligation de conservation généralisée des données, mais qui tend à affaiblir l'efficacité des services d'enquête.**

Dans sa version originale de 2011, la loi slovaque sur les communications électroniques imposait, à ses articles 58 et 63, une conservation généralisée des données de connexion pendant six mois pour les communications par internet et jusqu'à douze mois pour les autres types de communication.

Saisie par un groupe de députés, la **Cour constitutionnelle slovaque a abrogé en avril 2015 ces dispositions**[1], déclarées à la fois contraires à trois articles de la Constitution slovaque, à la Convention européenne des droits de l'Homme, ainsi qu'à la Charte des droits fondamentaux de l'UE à la lumière de l'arrêt *Digital Rights Ireland* du 8 avril 2014.

Tirant les conséquences de cette décision, le législateur a amendé, en novembre 2015, la loi sur les communications électroniques et le code de procédure pénale[2]. **Les opérateurs ne sont ainsi plus soumis à une obligation légale de conservation des données de connexion**, y compris en matière de renseignement. Les autorités ne peuvent, dès lors, accéder qu'aux données de connexion conservées par les opérateurs pour répondre à leurs propres besoins.

Le juge peut également ordonner aux opérateurs un gel rapide des données de connexion (*quick freeze*)[3], à la demande d'une autorité habilitée[4]. La conservation rapide est limitée à une période ne pouvant excéder six mois, renouvelable pour deux mois sur décision du juge.

Si le régime actuel apparaît conforme aux exigences posées par la CJUE, les services du ministère de la Justice slovaque considèrent que **l'absence de conservation obligatoire des données de connexion pénalise l'efficacité de la lutte contre la criminalité grave, notamment en matière de pédocriminalité**[5].

---

[1] *Cour constitutionnelle slovaque, 29 avril 2015, PL. ÚS 10/2014, consultable sur leur site.*

[2] *Titre III de la loi n° 397/2015 du 13 novembre 2015*

[3] *Art. 112 de la Loi sur les communications électroniques (zákon n° 452/2021 z 24. novembra 2021 o elektronických komunikáciá).*

[4] *En plus des services d'enquêtes, certaines institutions peuvent également accéder à ces données de connexion comme les douanes, l'agence nationale de cybersécurité, sous le contrôle du Parlement, dans le but de résoudre un incident de cybersécurité ou encore, jusqu'à la fin de l'urgence sanitaire, l'agence nationale de santé publique dans le but de lutter contre une pandémie.*

[5] *Source : réponse au questionnaire adressé à l'Ambassade de France en Slovaquie.*

**B. Une procédure d'accès aux données de connexion renforcée en 2015, conformément à la jurisprudence de la CJUE.**

Avant la réforme de 2015, les autorités répressives pouvaient accéder aux données de connexion dans le cadre d'une enquête pénale ordinaire, après autorisation par un juge. Le contrôle du juge n'était, pour autant, pas nécessaire lorsque la réquisition concernait une infraction pénale particulièrement grave, en l'occurrence les actes de terrorisme, les trafics d'armes et de stupéfiants ou la criminalité organisée.

La réforme de 2015, en sus de supprimer l'obligation de conservation généralisée des données, a conforté le contrôle du juge en matière d'accès aux données de connexion. Ainsi, les autorités répressives accèdent à ces **données sous réserve de l'accord systématique du juge** et **dans le seul cadre d'une procédure pénale relative à une infraction pénale grave**. La notion d'infraction pénale « grave » comprend les crimes ou délits passibles de trois ans de prison ou plus, les actes ayant causé des blessures physiques graves ou la mort, les menaces graves contre une personne, les atteintes à la vie privée au sein du domicile, les actes d'escroquerie et les infractions définies par un traité international[1].

En pratique, le procureur chargé de l'affaire adresse une demande au juge en justifiant par écrit son caractère indispensable à l'avancée de l'enquête. Le juge autorise l'accès aux données par une ordonnance motivée. En cas d'urgence, le ministère public peut adresser la réquisition directement à l'opérateur, à condition de la notifier au juge. Si ce dernier ne valide pas l'ordre de réquisition dans les 24 heures, les données ainsi obtenues ne seront pas utilisables et devront être détruites.

[1] *Article 116 du code procédure pénale (zákon z 24. mája 2005 trestný poriadok).*

## *J. LA SUÈDE*

### A. Un régime de conservation des données de connexion strict adapté à la jurisprudence récente de la CJUE.

La Suède a modifié à plusieurs reprises son régime légal d'accès et de conservation des données de connexion dans le cadre des enquêtes pénales pour **prendre en compte l'évolution de la jurisprudence de la Cour de justice de l'Union européenne (CJUE)**. La première modification législative dans ce domaine est intervenue après l'arrêt *Tele2* du 21 décembre 2016[1] répondant à la demande de décision préjudicielle formulée par la Cour administrative d'appel de Stockholm. Par cet arrêt, **la Cour a considéré que la loi suédoise, qui prévoyait une conservation générale et indifférenciée des données de trafic et de localisation, n'était pas conforme au droit de l'Union.**

Une commission d'enquête a été créée dans le but de modifier la loi sur les communications électroniques (LEK)[2] et la loi sur la collecte de données relatives aux communications électroniques en matière de renseignement (IHL)[3]. Les modifications issues de ces travaux, entrées en vigueur en octobre 2019, ont porté, d'une part, sur **la limitation dans le temps et en fonction du type de données de la durée de conservation et de la portée de l'obligation de conservation** et, d'autre part, sur **la désignation du procureur comme instance compétente pour autoriser l'accès aux données en matière de renseignement.**

Une nouvelle loi dite « **LEK 2022**[4] », qui prévoit des modifications à la marge du système déjà en vigueur, a été adoptée pour se conformer aux exigences de la directive (UE) 2018/1972 établissant le code des communications électroniques européen.

**Le législateur suédois a volontairement exclu la possibilité d'une conservation ciblée**, considérant que ce système n'offrirait pas de garanties supplémentaires en termes d'efficacité et présenterait une atteinte disproportionnée au respect de la vie privée. Il a suivi la position du gouvernement qui considère qu'« *introduire un cadre réglementaire qui aboutit à ce qu'il serait beaucoup plus difficile, et dans certains cas peut-être même impossible, d'éclaircir des crimes graves selon l'endroit où le crime a été commis ou planifié est inacceptable* »[5].

---

[1] *CJUE, 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. (C-203/15 et C-698/15).*
[2] *Loi 2003:389 sur les communications électroniques.*
[3] *Loi 2012-278 sur la collective des données relatives aux communications électroniques en matière de renseignement.*
[4] *Electronic Communications Act (2022:482) du 3 juin 2022.*
[5] *Prop. 2018/19:86 Datalagring vid brottsbekämpning – anpassningar till EU-rätten, p. 32.*

Le régime suédois est donc fondé sur **la conservation généralisée et indifférenciée des données. La durée et les modalités de la conservation varient en fonction de la nature de la donnée.** Depuis 2022, les données relatives aux conversations transférées, aux communications fixes et à la mise à disposition d'une capacité d'accès à internet ont été exclues du champ des données à conserver. Désormais, les données de localisation – qui sont considérées par la Cour de justice de l'Union européenne comme les plus sensibles - ne sont conservées que deux mois s'il s'agit de données de téléphonie ou six mois lorsqu'elles proviennent d'Internet. Les autres données de connexion sont conservées pendant six mois dans le cadre de la téléphonie et dix mois pour les données issues d'Internet. **Ces délais de conservation sont plus courts que ceux observés dans la plupart des États membres de l'Union européenne.**

Ce régime prévoit par ailleurs **une procédure de *quick freeze* dans le cadre de la lutte contre la criminalité grave.** La demande doit préciser la durée de conservation qui ne peut excéder 90 jours[1]. L'injonction de conservation est prononcée par le procureur ou l'enquêteur, l'opérateur pouvant en contester la légalité devant le juge.

Comme dans la plupart des États membres de l'Union européenne**, la loi suédoise oblige les opérateurs[2] à garantir la qualité, le stockage et la protection des données**. Ces obligations sont édictées et contrôlées par l'autorité suédoise des postes et télécommunications (PTS) qui dispose de larges pouvoirs de sanction (amende, révocation de l'autorisation d'exercer, *etc.*). Les décisions de cette autorité sont susceptibles de recours devant le juge administratif.

**B. Une procédure d'accès différenciée en fonction de la nature des données de connexion et de la finalité répressive.**

**Les règles d'accès aux données de connexion conservées varient en fonction du type de données et de la finalité répressive.** Les données relatives aux abonnements sont directement accessibles aux autorités judiciaires, de renseignement, de la sécurité nationale et à certaines autorités administratives pour l'identification et la poursuite d'une activité criminelle ou d'une infraction présumée, sans critère de gravité et sans contrôle par une autorité indépendante.

L'accès aux données relatives au trafic et à la localisation n'est possible qu'en matière de lutte contre la criminalité grave et dans deux cas de figure :

- pour les besoins de l'enquête préliminaire, sur ordonnance du tribunal ;

[1] *Avec possibilité de prorogation de 90 jours en cas de circonstances particulières.*

[2] *Notons que le législateur suédois a lancé en 2021 une initiative pour dresser le bilan de l'évolution du droit depuis l'arrêt* Tele2 *et réfléchir à l'intégration des fournisseurs de services par contournement au champ des opérateurs soumis à ces obligations.*

- pour les besoins des activités de renseignement, sur décision du ministère public, après présentation d'une requête par les autorités concernées.

Le respect de la proportionnalité de la mesure est contrôlé *a posteriori* par la Commission de la sécurité et de la protection de l'intégrité, l'autorité requérante étant tenue de notifier l'autorisation de l'accès aux données dans un délai d'un mois après la clôture du dossier.

**C. Malgré les évolutions récentes du droit suédois, des points de vigilance demeurent.**

Malgré la réforme récente du régime d'accès et de conservation des données de connexion dans le cadre des enquêtes pénales, **la conformité totale du droit suédois au droit de l'Union reste à confirmer**, la Cour de justice de l'Union européenne ne s'étant pas prononcée sur certains aspects de la législation suédoise.

En matière de conservation, d'une part, il n'est pas certain que la modulation de la durée et la réduction du champ des données conservées suffisent à considérer que la Suède n'est plus dotée d'un système de conservation générale et indifférenciée des données, indépendamment des finalités poursuivies.

En matière d'accès, d'autre part, l'autorisation délivrée par le ministère public pour permettre l'accès aux données de trafic et de localisation pour les activités de renseignement ne semble pas répondre aux exigences de contrôle indépendant fixées par la Cour de justice de l'Union européenne[1] qui a imposé la mise en œuvre d'un *« contrôle préalable, effectué soit par une juridiction, soit par une entité administrative indépendante »*[2].

[1] *CJUE, 6 octobre 2020, Privacy International (C-623/17), La Quadrature du Net e.a., French Data Network e.a., (C-511/18 et C-512/18), Ordre des barreaux francophones et germanophone (C-520/18).*

[2] *Consultable sur le site.*

# ANNEXE 2

## ÉTUDE DE DROIT COMPARÉ - TABLEAU DE SYNTHÈSE DES RÉGIMES LÉGAUX D'ACCÈS ET DE CONSERVATION DES DONNÉES DE CONNEXION DANS LE CADRE DES ENQUÊTES PÉNALES

| | | Allemagne | Pays-Bas | Slovaquie | Pologne | Lettonie | Lituanie |
|---|---|---|---|---|---|---|---|
| **Réception de la jurisprudence de la CJUE** | **Jurisprudentielle** | Loi de 2021 relative à la conservation des données rendue non-applicable par l'arrêt *SpaceNet* de la CJUE du 20 septembre 2022. | Suspension de la loi de 2009 relative à la conservation des données et à leur accès par une décision de 2015 du juge des référés du tribunal de la Haye. | Loi de 2011 relative à la conservation des données abrogée en avril 2015 par la Cour constitutionnelle slovaque. | / | / | / |
| | **Législative** | / | / | Adoption d'une nouvelle loi relative à la conservation et à la collecte des métadonnées en novembre 2015. | Pas d'évolution législative à la suite de la jurisprudence européenne | Pas d'évolution législative, mais institution d'un groupe de travail *ad hoc* chargé de proposer des amendements visant une mise en conformité de la législation nationale au regard du droit de l'UE. | Pas d'évolution législative, mais création d'un groupe d'experts chargé de formuler des propositions visant, le cas échéant, à modifier la législation nationale. |

| | | Allemagne | Pays-Bas | Slovaquie | Pologne | Lettonie | Lituanie |
|---|---|---|---|---|---|---|---|
| **Conservation des données de connexion** | **Type de conservation** | Aucune obligation légale de conservation | Aucune obligation légale de conservation | Aucune obligation légale de conservation | Généralisée | Généralisée | Généralisée |
| | **Si conservation ciblée, critères retenus** | / | / | / | / | / | / |
| | **Type de données et finalités de conservation finalités de conservation** | Données conservées par les opérateurs à des fins commerciales | Données conservées par les opérateurs à des fins commerciales | Données conservées par les opérateurs à des fins commerciales | Conservation indifférenciée des données d'identification, de trafic et de localisation. | Conservation indifférenciée des données d'identification, de trafic et de localisation. | Conservation indifférenciée des données d'identification, de trafic et de localisation. |

| | | Allemagne | Pays-Bas | Slovaquie | Pologne | Lettonie | Lituanie |
|---|---|---|---|---|---|---|---|
| **Conservation des données de connexion** | **Durée de conservation** | 6 mois pour les données conservées à des fins commerciales | N/C | N/C | 12 mois | 18 mois | De 6 à 12 mois |
| | **Existence d'une procédure de *quick freeze*** | Non. | Non. | Oui. Injonction du juge à la demande d'une autorité habilitée, qui ne peut excéder une période de 6 mois. | Oui, à la demande d'une juridiction ou du procureur général, obligation de conserver les données pour une durée de 3 mois maximum. | N/C | N/C |

| | | Allemagne | Pays-Bas | Slovaquie | Pologne | Lettonie | Lituanie |
|---|---|---|---|---|---|---|---|
| **Accès aux données de connexion** | **Procédure de droit commun d'autorisation et de contrôle des requêtes** | Réquisition émise par le tribunal, à la demande du ministère public.<br>Conditions : la collecte doit<br>1) concerner une infraction particulièrement grave ou commise grâce à des moyens de télécommunication ;<br>2) cibler l'auteur ou le complice d'une infraction précisée dans une liste exhaustive de la loi ;<br>3) être nécessaire et proportionnée à l'infraction poursuivie. | Réquisition émise par le procureur.<br>Conditions : la collecte doit concerner des infractions terroristes ou infractions pour lesquelles la détention provisoire est autorisée (i.e. punies d'une peine d'emprisonnement d'au moins quatre ans). | Réquisition par l'autorité répressive, après autorisation du juge.<br>Conditions : la collecte doit<br>1) concerner une infraction grave (notamment, passibles de trois ans d'emprisonnement ou plus) ;<br>2) être nécessaire à l'avancée de l'enquête. | Réquisition émise par les juridictions ou par le procureur, contrôlée *a posteriori* par les tribunaux de districts compétents, sur la base d'un rapport semestriel recensant les données auxquelles les autorités de police ont eu accès.<br>Conditions : la collecte doit<br>1) concerner un crime ou une infraction fiscale ;<br>2) concerner une personne, un lieu ou un appareil clairement identifié. | Réquisition émise par un enquêteur, sur autorisation du procureur, d'un procureur de rang supérieur ou de la personne concernée par les données.<br>Procédure dérogatoire : accès sans autorisation à des données qui n'affectent pas de manière significative la vie privée d'une personne pendant une durée maximale de 30 jours. | Réquisition émise par l'enquêteur, après autorisation par un juge, pour les données de trafic et de localisation uniquement.<br>Conditions: prévenir et poursuivre les crimes ou les menaces susceptibles d'affecter la souveraineté, l'intégrité du territoire, l'ordre constitutionnel, les intérêts de l'État, la défense ou le pouvoir économique. |
| | **Procédure d'urgence** | Réquisition prise par le ministère public, confirmée par le tribunal dans un délai de trois jours ouvrables. | Non. | Réquisition prise par le ministère public, validée par le juste dans un délai de 24 heures. | N/C | N/C | N/C |

| | | Italie | Irlande | Suède | Estonie |
|---|---|---|---|---|---|
| **Réception de la jurisprudence de la CJUE** | **Jurisprudentielle** | La Cour de cassation italienne a jugé à plusieurs reprises que la législation italienne était conforme aux principes consacrés par la CJUE. | Par l'arrêt *Graham Dwyer c/ Commissioner of An Garda Síochána* du 5 avril 2022, la CJUE a jugé la loi irlandaise de 2011 sur les données de connexion non-conforme au droit de l'Union. | Par l'arrêt *Tele2* (2016), la CJUE juge la loi suédoise, qui prévoyait une conservation générale et indifférenciée des données de trafic et de localisation, non conforme au droit de l'Union. | Par l'arrêt *Prokuratuur* du 2 mars 2021, de la CJUE a déclaré le régime estonien d'accès aux métadonnées non-conforme au droit de l'UE. |
| | **Législative** | Modification du régime d'accès aux données de connexion par le décret-loi n° 132 du 30 septembre 2021 à la suite de l'arrêt *Prokuratuur* de la CJUE du 2 mars 2021. | Modification de la loi de 2011 sur les communications (conservation des données) par la loi du 21 juillet 2022. | Modification des régimes d'accès et de conservation des données prévus par la loi sur les communications électroniques (LEK) en 2019 puis en 2022. | Modification du code de procédure pénale en 2022 afin de mieux encadrer l'accès aux données de connexion. |
| **Conservation des données de connexion** | **Type de conservation** | Généralisée | Généralisée pour les données d'identité civile et numérique ; procédures spécifiques pour les données de trafic et de localisation. | Généralisée | Généralisée |
| | **Si conservation ciblée, critères retenus** | / | / | / | / |

| | | Italie | Irlande | Suède | Estonie |
|---|---|---|---|---|---|
| **Conservation des données de connexion** | **Type de données et finalités de conservation finalités de conservation** | Prévention et lutte contre la criminalité grave et contre la criminalité en générale, prévention de la cybercriminalité et défense de la sécurité intérieure. Cependant, l'accès aux données de connexion est limité aux fins de lutte contre la criminalité grave. | Lutte contre la criminalité en général, lutte contre la criminalité grave, sauvegarde de la sécurité nationale (conservation généralisée de certaines données et procédure de *quick freeze*), lutte contre une menace sérieuse et réelle, actuelle et prévisible pour la sécurité nationale (conservation généralisée de l'ensemble des données de connexion). | - *Conservation des données d'identité : aux fins de lutte contre la criminalité en général et de lutte contre la criminalité grave ;*<br>- *Conservation des données de trafic et de localisation : limitée à la lutte contre la criminalité grave.* | Lutte contre la criminalité grave et préservation de la sécurité nationale. |
| | **Durée de conservation** | Pour la lutte contre criminalité en général :<br>- *24 mois pour les données téléphoniques ;*<br>- *12 mois pour les données télématiques ;*<br>- *30 jours pour les appels sans réponse.*<br>En l'absence de droit d'accès, ces dispositions ne s'appliquent pas.<br>Pour la lutte contre criminalité grave : 72 mois. | - *Données des utilisateurs : 12 mois sauf décision ministérielle imposant une durée différente, dans la limite de 24 mois ;*<br>- *Données des sources internet : 12 mois sauf décision ministérielle imposant une durée différente aux fins de lutte contre la criminalité grave ;*<br>- *Données de trafic et de localisation : 12 mois, uniquement aux fins de lutter contre une menace sérieuse, réelle, actuelle et prévisible pour la sécurité nationale.* | *Données de localisation : 2 mois (téléphonie) ou 6 mois (internet) ;*<br>*Autres données de connexion : 6 mois (téléphonie) ou 10 mois (internet).* | 12 mois.<br>Si les données ont fait l'objet d'une demande d'accès, elles doivent être conservées pour 24 mois. Ces délais peuvent être prorogés pour la sauvegarde de l'ordre publique et de la sécurité nationale. |

| | | Italie | Irlande | Suède | Estonie |
|---|---|---|---|---|---|
| **Conservation des données de connexion** | **Existence d'une procédure de *quick freeze*** | Oui, l'injonction doit être communiquée, dans un délai de 48 heures, à l'opérateur et au procureur de la République pour validation.<br>Conditions : pour la prévention d'infractions graves ou pour la poursuite d'infractions spécifiques, pour une durée maximale de 90 jours prorogeable jusqu'à 6 mois. | Oui, pour les données de trafic et de localisation, sur autorisation du juge qui effectue un contrôle de proportionnalité de la mesure et pour une durée maximale de 90 jours. En cas d'urgence, contrôle judiciaire *a posteriori* dans un délai de 72 heures. | Oui. Injonction prononcée par le procureur ou l'enquêteur pour une période de 90 jours avec prorogation de 90 jours sous conditions<br>- *Condition : Uniquement dans le cadre de la lutte contre la criminalité grave.* | Non. |
| **Accès aux données de connexion** | **Procédure de droit commun d'autorisation et de contrôle des requêtes** | Les données sont acquises à la demande du procureur de la République ou de l'avocat de la personne mise en cause, de la personne mise en examen, de la victime et des parties civiles, sur ordre motivé du juge. | - *Les données des utilisateurs sont directement accessibles aux agents habilités à y accéder ;*<br>- *L'accès aux données des sources internet et aux données de trafic est autorisé par le juge ;*<br>- *l'accès aux données de localisation doit être autorisé par le supérieur hiérarchique et validé a posteriori par le juge.* | Pour les données d'identification : accès direct par l'autorité qui formule la requête.<br>Pour les données de trafic et de localisation : réquisition autorisée par le ministère public, sur ordonnance du tribunal et uniquement aux fins de lutte contre la criminalité grave. La demande d'accès est formulée par l'autorité de police, le service de la sécurité nationale ou le service des douanes. | Requête écrite adressée à l'opérateur par l'autorité chargée de l'enquête, l'autorité de renseignement ou le procureur, sur autorisation du juge compétent. |
| | **Procédure d'urgence** | Accès ordonné par le procureur de la République et contrôlé *a posteriori* du juge, dans un délai de 48 heures. | L'autorisation d'accès est délivrée par le supérieur hiérarchique de l'agent qui doit rédiger un rapport dans un délai de 8 heures et saisir le juge dans les 72 heures. | N/C | Délai de traitement des requêtes réduit à 10 heures (au lieu de 10 jours ouvrables). |

| | | Belgique | Danemark |
|---|---|---|---|
| **Réception de la jurisprudence de la CJUE** | **Jurisprudentielle** | Annulation en avril 2021 de la loi de 2016 relative à la conservation et la collecte des données par la Cour constitutionnelle belge. | / |
| | **Législative** | Adoption en juillet 2022 d'une nouvelle loi relative à la conservation et la collecte des données. | Révision, à l'initiative du gouvernement, du dispositif de conservation des données, lancée en 2017 et entrée en vigueur en mars 2022. |
| **Conservation des données de connexion** | **Type de conservation** | Mixte (généralisée et ciblée) | Mixte (généralisée et ciblée) |
| | **Si conservation ciblée, critères retenus** | <u>Critères géographiques</u> :<br>- *Zones particulièrement exposées à des menaces de crimes graves ou d'atteinte à la sécurité nationale (aéroports, gares etc.) ;*<br>- *Zones sujettes à un taux important de criminalité grave.* | *1) <u>Critères géographiques</u> :*<br>- *Zones particulièrement exposées à des menaces d'atteinte à la sécurité nationale (aéroports, gares etc.) ;*<br>- *Zones ayant un nombre important d'infractions pénales graves ou de résidents condamnés pour de telles infractions.*<br>*2) <u>Catégories de personnes</u> :*<br>- *Personnes condamnées pour des infractions pénales graves ;*<br>- *Numéros de téléphone faisant l'objet d'une ordonnance d'interception.* |

| | | Belgique | Danemark |
|---|---|---|---|
| **Conservation des données de connexion** | **Type de données et finalités de conservation** | - <u>*Conservation généralisée des données d'identification*</u> *: lutte contre la criminalité en général ;*<br>- <u>*Conservation généralisée des données de trafic et de localisation*</u> *: détection d'une fraude ou d'une utilisation malveillante des réseaux ;*<br>- <u>*Conservation ciblée*</u> *: prévention des menaces graves pour la sécurité publique et de la prévention ou de la poursuite de faits relevant de la criminalité grave.* | - <u>*Conservation généralisée des données d'identification numérique*</u>*: lutte contre la criminalité en général ;*<br>- <u>*Conservation généralisée des autres données*</u> *: la protection de la sécurité nationale ;*<br>- <u>*Conservation ciblée*</u> *: lutte contre les infractions graves.* |
| | **Durée de conservation** | 4 à 12 mois | 12 mois |
| | **Existence d'une procédure de *quick freeze*** | Oui.<br>- <u>*Future freeze*</u> *: Injonction émise par le procureur du Roi pour la conservation durant six mois des données émises en temps réel.* <u>*Condition*</u> *: nécessité d'indices sérieux pouvant donner lieu à une peine d'emprisonnement d'un an ou plus.*<br>- <u>*Quick freeze*</u> *: Injonction émise par la police pour la sauvegarde de données existantes pour une durée maximale de 90 jours.* <u>*Condition*</u> *: raisons de croire que ces données sont particulièrement susceptibles de perte ou de modification.* | Oui.<br>- <u>*Future freeze*</u> *: Injonction émise par le tribunal pour la conservation durant un an des données émises en temps réel.*<br>- <u>*Quick freeze*</u> *: Injonction émise par la police pour la sauvegarde de données existantes pour une durée de 90 jours, renouvelable.*<br><u>Condition</u> : ces données doivent être liées à des infractions graves (peine d'emprisonnement de trois ans ou plus). |

| | | Belgique | Danemark |
|---|---|---|---|
| **Accès aux données de connexion** | **Procédure de droit commun d'autorisation et de contrôle des requêtes** | <u>Pour les données d'identification</u> : réquisition émise par le procureur du Roi. Pour les infractions passibles d'une peine d'emprisonnement inférieure à un an, seules les données émises dans les six mois précédant la décision peuvent être demandées.<br><br><u>Pour les données de trafic et de localisation</u> : réquisition émise par le juge d'instruction.<br><u>Conditions</u> :<br>1) concerne une infraction de nature à entraîner une peine d'emprisonnement d'un an ou plus ;<br>2) nécessité de la mesure. | Réquisition émise par la police, après autorisation du tribunal.<br><u>Conditions</u> : les données doivent<br>1) être à destination ou en provenance d'un suspect ;<br>2) être d'une importance décisive pour l'enquête ;<br>3) concerner une infraction passible d'une peine d'emprisonnement de trois ans et plus ou une infraction liée à des conflits entre bandes violentes. |
| | **Procédure d'urgence** | <u>Données de trafic et de localisation</u> : en cas de flagrant délit, le procureur du Roi peut ordonner la mesure, sous réserve d'une confirmation par le juge d'instruction dans les 24 heures. Cette dernière n'est pas nécessaire en matière d'infraction terroriste, prise d'otage, détention illégale ou extorsion. | Réquisition émise par la police, sous réserve de la saisine du tribunal dans les vingt-quatre heures. Le tribunal autorise *a posteriori* la mesure et statue sur la durée de son maintien. |

# LE CONTRÔLE EN CLAIR

## POUR CONSULTER LA PAGE DE LA MISSION D'INFORMATION

https://www.senat.fr/travaux-parlementaires/commissions/commission-des-lois/les-modalites-dinvestigation-recourant-aux-donnees-de-connexion-dans-le-cadre-des-enquetes-penales.html