L'ESSENTIEL SUR…

Commission DES LOIS

SÉNAT

…le rapport d'information

SURVEILLER POUR PUNIR ?

POUR UNE RÉFORME DE L'ACCÈS AUX DONNÉES DE CONNEXION DANS L'ENQUÊTE PÉNALE

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.

1. 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-relai 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.

2. 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.

3. 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 :

- 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.

[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.

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.

4. 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.**

LES PRINCIPAUX CONSTATS

- **Un rôle central des données de connexion dans les enquêtes pénales, celles-ci étant devenues une nouvelle « reine des preuves » et représentant chaque année un nombre massif d'accès**
- **Une jurisprudence européenne qui, depuis près de dix, vient remettre en cause le régime français en ce qui concerne à la fois la conservation des données de connexion par les opérateurs et l'accès à ces données**
- **En Europe, des tentatives insatisfaisantes de mise en conformité des droits internes avec le droit de l'Union et des perturbations dans le processus décisionnel de l'Union en matière de protection des données et de numérique**
- **En France, des évolutions législatives qui n'ont pas suffi à mettre le droit national en pleine conformité avec les arrêts de la Cour de justice de l'Union européenne, notamment du fait du maintien d'une conservation générale et indifférenciée des données de connexion et d'un accès qui n'est pas toujours soumis à un contrôle préalable et indépendant**

LES PRINCIPALES PROPOSITIONS

- **Assumer une position forte dans le dialogue européen pour faire aboutir les négociations sur *e-privacy 2***
- **Mieux tirer profit des « soupapes » offertes par la jurisprudence européenne, qui offre des souplesses pour la conservation et l'accès aux données d'identification**
- **Mettre en place un contrôle préalable et indépendant confié au juge des libertés et de la détention**
- **Concevoir pragmatiquement ce futur contrôle pour limiter la surcharge de travail induite sur les enquêteurs et les magistrats et éviter le « choc procédural »**

François-Noël Buffet

Président de la commission

Sénateur (Les Républicains) du Rhône

Agnès Canayer

Rapporteur

Sénateur (Rattachée au groupe Les Républicains) de la Seine-Maritime

Philippe Bonnecarrère

Rapporteur

Sénateur (Union Centriste) du Tarn

Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale

http://www.senat.fr/commission/loi/index.html

Téléphone : 01 42 34 23 37

Pour en savoir plus : consulter le contrôle en clair.