Commission nationale de l'informatique et des libertés

Délibération n° 2014-009 du 16 janvier 2014 portant avis sur un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires » (demande d'avis n° AV 13023753)

NOR : CNIX1423917X

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre de la justice d'une demande d'avis concernant un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires » ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de procédure pénale, notamment ses articles 20, 28-1 et 28-2, 60-2, 77-1-2, 99-4, 100 à 100-7, 157, 706-95, et R. 15-33-67 à R. 15-33-75 ;

Vu le code des postes et des communications électroniques, notamment ses articles L. 34-1, R. 10-12 à R. 10-14 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 26-II ;

Vu la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, notamment son article 6 ;

Vu la loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2007-115 du 30 juillet 2007 portant création d'un traitement automatisé de données à caractère personnel dénommé « Système de transmission d'interceptions judiciaires » ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu 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, notamment son article 1^{er} ;

Vu la délibération n° 2007-028 du 13 février 2007 portant avis sur le projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel dénommé « Centre de gestion des interceptions judiciaires (CGIJ) » ;

Après avoir entendu Mme Claire DAVAL, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

La commission a été saisie par le ministre de la justice d'une demande d'avis concernant un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires » (PNIJ).

Certaines données sensibles, au sens de l'article 8 de la loi du 6 janvier 1978 modifiée, sont susceptibles d'être collectées dans le cadre des interceptions de communications électroniques. Ce traitement doit dès lors être créé par décret en Conseil d'Etat pris après avis motivé et publié de la commission, conformément à l'article 26-II de la loi du 6 janvier 1978 modifiée.

Si la commission est consciente des avantages que peut apporter ce nouveau dispositif, les risques que cette centralisation d'une masse importante de données personnelles soulève sont substantiels. C'est pourquoi, au-delà de la vigilance exercée dans le cadre de l'instruction de cette demande d'avis, la commission souligne qu'elle se montrera particulièrement attentive aux conditions réelles de déploiement de la plate-forme et ne manquera pas de faire usage, le cas échéant, de ses pouvoirs de contrôle prévus à l'article 44 de la loi du 6 janvier 1978 modifiée.

Le traitement projeté centralisera les données résultant, d'une part, des interceptions de communications électroniques et, d'autre part, des réquisitions de données de connexion conservées par les opérateurs de communications électroniques, les fournisseurs d'accès à internet (FAI) et les hébergeurs, ordonnées par l'autorité judiciaire, dans le cadre des enquêtes et informations judiciaires prévues par le code de procédure pénale (CPP).

Les dispositifs actuels d'interception des communications électroniques et de réquisitions de données de connexion reposent sur un système hétérogène et décentralisé qui fait appel à plusieurs prestataires privés et présente des inconvénients majeurs. En effet, les fonctions et les outils de réquisition et d'interception sont variables et coûteux, et les mesures de sécurité et de traçabilité mises en œuvre ne sont pas satisfaisantes.

En ce qui concerne les interceptions de communications, le système de transmission d'interceptions judiciaires (STIJ), autorisé par le décret n° 2007-1145 du 30 juillet 2007 pris après l'avis de la commission en date du 13 février 2007, permet aux magistrats et aux officiers de police judiciaire de disposer des données de trafic des correspondances interceptées (numéros de téléphone, date, heure et durée de l'appel, etc.) ainsi que des contenus des minimessages (SMS ou MMS) émis ou reçus par un numéro de téléphone dont la ligne est surveillée. Le présent projet de décret prévoit, en son article 12, l'abrogation du décret du 30 juillet 2007 six mois après la mise en œuvre de la nouvelle plate-forme, et au plus tard le 31 décembre 2015. La commission prend acte qu'aucune donnée du STIJ ne sera reprise dans la PNIJ.

Les réquisitions de données de connexion, quant à elles, sont réalisées directement par l'enquêteur auprès de l'opérateur de communications électroniques, du FAI ou de l'hébergeur.

La nouvelle plate-forme PNIJ permettra de gérer dans un seul et même espace les deux catégories de demandes applicables aux communications électroniques auprès des opérateurs de communications électroniques, des FAI et des hébergeurs.

En effet, elle a pour objectif général de centraliser, d'une part, les données de connexion définies aux articles L. 34-1 du code des postes et des communications électroniques (CPCE) et 6-II de la loi n° 2004-575 du 21 juin 2004 modifiée (LCEN), obtenues dans le cadre d'une réquisition judiciaire en application des articles 60-2, 77-1-2 et 99-4 du code de procédure pénale (CPP), et, d'autre part, les données issues des interceptions de correspondances émises par la voie des télécommunications, réalisées sur le fondement des articles 74-2, 80-4, 100 à 100-7 et 706-95 du CPP.

Les avantages attendus sont nombreux : il s'agit d'augmenter les capacités d'interception, de réduire les délais de réponse, de renforcer le niveau de sécurité, notamment l'intégrité et la confidentialité des données à caractère personnel, et de réduire les frais de justice. Ainsi, la mise en œuvre de cette plate-forme constitue, pour le ministère de la justice, l'une des mesures prioritaires de modernisation de l'action publique.

A titre liminaire, la commission observe que la plate-forme projetée constitue une extension du système actuel, le STIJ ne couvrant pas l'ensemble des données qui seront centralisées au sein de la PNIJ. La plate-forme permettra en effet le regroupement au sein d'un même dispositif de deux types d'actes judiciaires, réalisés sur des fondements juridiques distincts. Elle relève néanmoins que cette centralisation ne modifie en rien les cadres juridiques applicables aux réquisitions et interceptions judiciaires et relève à cet égard que la plate-forme est conçue pour cloisonner les deux types de réquisitions.

En outre, le champ de la PNIJ est circonscrit exclusivement aux réquisitions et interceptions judiciaires, prises sur le fondement du code de procédure pénale. Par conséquent, les mesures d'instruction civile relevant, par exemple, des dispositions de l'article 145 du code de procédure civile, ne seront pas traitées dans la PNIJ. De même, les interceptions de sécurité (relatives aux enquêtes administratives et prises sur le fondement des articles L. 241-1 et suivants du code de la sécurité intérieure) ainsi que les réquisitions administratives de données de connexion (sur le fondement des articles L. 34-1-1 du CPCE et 6-II *bis* de la LCEN, tous deux codifiés à l'article L. 246-1 du code de la sécurité intérieure à compter du 1^{er} janvier 2016) ne seront pas concernées par le dispositif projeté.

Par ailleurs, l'objet de la PNIJ se limite à la gestion des réquisitions, c'est-à-dire la gestion des procédures, des demandes, des réponses (retranscription, désinfection de codes malveillants, traduction, mise au clair), des procès-verbaux et des scellés, ainsi qu'à la gestion financière, aux statistiques et à l'administration technique et fonctionnelle de la plate-forme. Ainsi, la PNIJ ne comprendra ni les autorisations des magistrats, ni les traitements réalisés par les opérateurs, ni le reste de la procédure d'enquête. A cet égard, si la commission prend acte que les magistrats sont informés régulièrement des réquisitions faites en leur nom, afin de limiter les risques induits par le fait que leurs décisions ne sont pour l'instant pas intégrées dans la PNIJ, elle estime toutefois qu'il serait opportun, à l'avenir, d'intégrer au sein de la PNIJ ces autorisations, afin de faire bénéficier l'ensemble de la procédure de la sécurité juridique et technique offerte par la plate-forme.

Si la sauvegarde de l'ordre public et la poursuite des auteurs d'infraction constituent des objectifs nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, la commission rappelle néanmoins que les conséquences pour les personnes des fichiers utilisés en la matière sont telles que la mise en place de garanties fortes constitue une exigence fondamentale et que le contrôle de la CNIL est à cet égard indispensable.

Ainsi, au regard de l'ampleur des données traitées, due notamment à la centralisation du dispositif et à l'augmentation sensible du nombre de réquisitions et d'interceptions judiciaires réalisées, et de la nature des actes d'enquêtes concernés, lesquels sont particulièrement intrusifs pour la vie privée des personnes concernées, la commission estime que des mesures juridiques et techniques adaptées doivent être prévues afin d'assurer un haut niveau de protection des données.

Sur les finalités du traitement :

L'article 1^{er} du projet de décret prévoit qu' « afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, ce traitement enregistre et met à la disposition des magistrats, des officiers et agents de police judiciaire de la gendarmerie et la police nationale ainsi que des agents des douanes et services fiscaux habilités à effectuer des enquêtes judiciaires, le contenu des communications électroniques interceptées ainsi que les informations utiles à la manifestation de la vérité

communiquées en application des articles 60-2, 77-1-2 et 99-4 du code de procédure pénale et des articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011 ». La plate-forme transmet donc les réquisitions établies par ces personnels aux opérateurs de communications électroniques, reçoit leurs réponses et les met à la disposition des magistrats, officiers et agents précités.

S'agissant du champ des interceptions concernées, il s'agit tout d'abord des interceptions judiciaires des correspondances émises par la voie des télécommunications, dont le régime de droit commun est prévu aux articles 100 à 100-7 du CPP, dispositions qui trouvent leur origine dans l'article 2 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances.

Chaque opération d'interception fait l'objet d'un enregistrement puis est transcrite, dès lors que le contenu est utile à la manifestation de la vérité, conformément à l'article 100-5 du CPP. A cet égard, la commission relève que la PNIJ ne prévoit pas de mesure permettant de garantir que la transcription ne contient que des éléments relatifs à l'enquête, ces transcriptions relevant de la responsabilité des magistrats et des officiers de police judiciaire.

Par ailleurs, le code de procédure pénale prévoit des dispositions spécifiques s'agissant de certaines professions. Ainsi, l'article 100-5 du CPP prévoit que les correspondances avec un avocat relevant de l'exercice des droits de la défense ainsi que celles avec un journaliste permettant d'identifier sa source ne peuvent être retranscrites. A cet égard, la commission prend acte que le ministère s'engage à ajouter aux visas du décret projeté la loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes.

S'agissant du type de contenu intercepté, la PNIJ ne traitera que des communications transitant par des opérateurs basés sur le territoire français. Les autres communications devant être traitées *via* une commission rogatoire internationale, elles ne seront pas concernées par la PNIJ. Le contenu des communications interceptées recouvre la voix, la vidéoconférence, la *data mobile* (Short Message Service [SMS], et Multimédia Messaging Service [MMS]) ainsi que la *data fixe* pour l'internet filaire.

La deuxième catégorie de données concerne les données issues des réquisitions judiciaires de données de connexion, prévues, d'une part, aux articles L. 34-1 et R.10-12 à R. 10-14 du CPCE pour les opérateurs de communications électroniques et, d'autre part, à l'article 6-11 de la LCEN et au décret n° 2011-219 du 25 février 2011 susvisé pour les FAI et les hébergeurs.

Ces réquisitions judiciaires sont prises sur le fondement des articles 60-2, 77-1-2 et 99-4 du CPP, qui permettent aux enquêteurs de demander la mise à disposition de données par voie électronique. Les articles R. 15-33-67 et suivants de ce même code fixent les conditions de ces demandes de mise à disposition de données par voie électronique. Ainsi, les informations sollicitées par les enquêteurs sont mises à disposition par les opérateurs par envoi d'un fichier dématérialisé, conservé dans la PNIJ jusqu'à la clôture des investigations. Le code de procédure pénale prévoit à cet égard que les modalités techniques d'interrogation et de transmission des informations soient précisées par un protocole passé par le ministre de la justice et, selon les cas, le ministre de l'intérieur ou le ministre chargé du budget, avec chaque organisme ou personne morale relevant des dispositions de l'article R. 15-33-68 du CPP. La commission prend acte qu'une copie de chaque protocole signé lui sera adressée par chaque organisme concerné à l'occasion du dépôt des formalités préalables prévues par la loi du 6 janvier 1978 modifiée, conformément aux dispositions de l'article R. 15-33-73 du même code.

Elle prend également acte que sont seuls concernés par la mise à disposition, par voie électronique, de données dans la PNIJ les organismes mentionnés au 1° de l'article R. 15-33-68 du CPP, c'est-à-dire les opérateurs de communications électroniques ainsi que les FAI et les hébergeurs et que le projet de décret sera complété sur ce point.

Enfin, la plate-forme doit permettre la réalisation de statistiques fonctionnelles et décisionnelles. En aucun cas, elles ne devront faire apparaître des données permettant d'identifier directement ou indirectement des personnes ou catégories de personnes.

La commission estime que ces finalités sont déterminées, explicites et légitimes. Elle relève que la centralisation projetée dans le cadre de la PNIJ permettra par ailleurs au ministère de la justice de mieux maîtriser ces actes d'enquêtes et, par conséquent, de mieux garantir la régularité des procédures concernées et de mieux gérer la facturation des actes requis.

Sur la nature des données traitées :

L'article 2 du projet de décret distingue les données collectées lors d'interceptions judiciaires de celles obtenues lors de réquisitions judiciaires visant les données de connexion.

Le 1° de l'article 2 du projet de décret mentionne les données collectées lors de la réalisation d'une interception de contenu, comprenant le contenu à proprement parler et les données de connexion nécessaires à l'interception de la communication. Les données seront relatives à la personne physique ou morale visée par l'enquête, à l'adresse ou à toute information permettant d'identifier le domicile, le lieu ou l'établissement visé par l'enquête judiciaire, aux éléments d'identification de la liaison et aux données relatives aux équipements terminaux de communication utilisés visés par l'enquête judiciaire. Elles concerneront également les numéros de téléphone, l'adresse de courrier électronique ou les données relatives aux services demandés ou utilisés visés par l'enquête judiciaire, les données à caractère technique relatives à la localisation de la communication et de l'équipement terminal. Enfin, les données permettant d'établir la facturation et le paiement, le contenu des communications électroniques interceptées ainsi que les informations utiles à la manifestation de la vérité pourront être collectées.

La plupart de ces données n'appellent pas d'observation particulière, mais la commission tient néanmoins à apporter les précisions suivantes.

La commission relève tout d'abord que, conformément à l'article 100-1 du CPP qui évoque la « *liaison à intercepter* », cette catégorie d'interception porte sur une liaison spécifique et non sur une personne « cible ». Par

conséquent, chaque moyen de communication à intercepter doit faire l'objet d'une décision spécifique, qui ne saurait donc porter sur l'ensemble des moyens de communication utilisés par une personne. Cette décision est prise par l'autorité judiciaire compétente en application des dispositions du CPP et l'officier de police judiciaire (OPJ), à la connaissance duquel cette décision est portée par tout moyen, est tenu, pour l'exécution de cette décision, d'adresser une réquisition écrite d'interception judiciaire à l'opérateur de communications électroniques.

S'agissant des « données à caractère technique relatives à la localisation de la communication et de l'équipement terminal », le ministère a fait savoir que la localisation géographique de l'équipement terminal est inhérente à toute interception d'une communication électronique. Or, la commission rappelle que le II de l'article R. 10-13 du CPCE précise que la donnée de localisation est conservée par les opérateurs uniquement pour les activités de téléphonie. Dès lors, la commission prend acte de l'engagement du ministère de limiter l'usage de ce dispositif à la téléphonie.

Elle prend également acte que la PNIJ permet techniquement, dès à présent, de traiter les réquisitions judiciaires de géolocalisation en temps réel, c'est-à-dire le suivi dynamique et immédiat d'un terminal de télécommunication. Elle considère dès lors que le projet de décret devrait mentionner explicitement la collecte de ces données, même si ces réquisitions ne seront pas mises en œuvre immédiatement, dans l'attente d'un fondement légal adéquat pour les mesures de géolocalisation réalisées dans le cadre des enquêtes de police judiciaire. A défaut, la commission devra être à nouveau saisie pour avis d'un projet de décret modificatif. En tout état de cause, s'agissant des réquisitions de géolocalisation réalisées sous le contrôle du procureur de la République, elles ne pourront être mises en œuvre qu'une fois ces moyens d'enquête autorisés par la loi.

Par ailleurs, le contenu de la communication s'accompagne de données de trafic relatives à cette correspondance, qui sont, dans le cadre de la PNIJ, placées sous scellés avec le contenu de la communication interceptée. La commission relève que le ministère a fait évoluer le projet de décret en ce sens, afin de mentionner expressément ces métadonnées propres à l'interception ainsi que celles propres aux données de connexion (au 2° de l'article 2 du projet de décret).

Le 2° de l'article 2 du projet de décret détaille les données qui pourront être collectées au titre des réquisitions judiciaires de données de connexion. Ces données sont relatives à la personne physique ou morale visée par l'enquête judiciaire, à l'adresse ou à toute autre information permettant d'identifier le domicile, le lieu ou l'établissement visé par l'enquête. Elles concerneront également les éléments d'identification de la liaison et les données relatives aux équipements terminaux de communications utilisés visés par l'enquête judiciaire, ainsi que les numéros de téléphone. Enfin, l'adresse de courrier électronique ou les données relatives aux services demandés ou utilisés, et les données permettant d'établir la facturation et le paiement, pourront être collectées. Elles reprennent les données mentionnées aux articles R.10-12 à R.10-14 du CPCE et dans le décret du 25 février 2011. La commission rappelle à cet égard que les mots de passe et informations associées ne sont pas des données de connexion. Elle prend d'ailleurs acte que celles-ci ne sont pas mentionnées dans le projet de décret et ne pourront donc pas être collectées.

L'article 2 du projet de décret prévoit en outre que peuvent être enregistrées les informations relatives aux faits, lieux, dates et qualification pénale des infractions objets de l'enquête.

Enfin, pourront être enregistrées les informations relatives à la reconnaissance vocale du locuteur. Cette reconnaissance permettra aux enquêteurs de reconnaître un individu parmi les interceptions vocales reçues ultérieurement au sein de la même affaire. A cet égard, la commission prend acte que le dispositif ne pourra permettre d'identifier des personnes qu'au sein d'une même affaire et qu'aucun rapprochement avec d'autres affaires ne peut être effectué. En outre, la mise en œuvre de cette fonctionnalité n'est pas automatique, puisqu'elle est décidée, au cas par cas, par l'enquêteur. Enfin, chaque création d'empreinte vocale est tracée, de même que chaque reconnaissance.

Si l'article 2 du projet de décret ne le prévoit pas expressément, il convient de noter que les données relatives aux utilisateurs de la plate-forme seront également collectées.

Sous ces réserves, la commission considère que les données collectées sont adéquates, pertinentes et non excessives au regard des finalités assignées au traitement PNIJ.

Sur la durée de conservation des données :

Le premier alinéa de l'article 5 du projet de décret prévoit que les informations relatives aux communications électroniques faisant l'objet d'une interception judiciaire sont placées sous scellés au format numérique et conservées jusqu'à expiration du délai de prescription de l'action publique. L'article 100-6 du CPP prévoit en effet que la destruction des enregistrements est réalisée à la diligence du procureur de la République ou du procureur général, à l'expiration de ce délai.

Cette durée de conservation est beaucoup plus longue que celle prévue à l'article 5 du décret n° 2007-1145 du 30 juillet 2007 relatif au STIJ. En outre, dans la mesure où une transcription obligatoire de la correspondance doit être réalisée en application de l'article 100-5 du CPP, laquelle contient tous les éléments nécessaires « à la manifestation de la vérité », la conservation de ces enregistrements après leur transcription pourrait apparaître discutable.

Cependant, la durée de conservation limitée à trente jours dans le STIJ s'explique par le fait que ces données sont transférées sur le poste de travail de l'enquêteur qui en conserve ensuite la totale disponibilité. Or, la commission estime que cette pratique ne permet pas d'assurer de manière satisfaisante la sécurité, notamment la confidentialité des enregistrements. Dès lors, la conservation dans l'application PNIJ des enregistrements permettra de faire bénéficier ces documents des mesures de sécurité et de traçabilité mises en œuvre au sein de cette application, ce dont la CNIL ne peut que se féliciter. Elle relève néanmoins qu'à titre exceptionnel, sur autorisation

écrite du magistrat, l'officier de police judiciaire ou l'agent des douanes ou des services fiscaux habilité à effectuer des enquêtes judiciaires peut procéder au transfert de tout ou partie des communications sur son poste de travail, par l'intermédiaire du réseau sécurisé du ministère de l'intérieur ; cette possibilité pourra notamment être mise en œuvre lorsque l'accès à la PNIJ est impossible (dans le cas d'audition d'un prévenu en établissement pénitentiaire, par exemple). Si ces exports seront tracés, la commission rappelle qu'ils ne devront être autorisés qu'exceptionnellement, sous peine de vider le principe général de sa substance et de perdre le contrôle sur ces enregistrements et leur devenir.

En outre, la conservation des enregistrements des communications interceptées jusqu'à la clôture de l'enquête, c'est-à-dire même postérieurement à la transcription, est justifiée par le fait que les enregistrements peuvent se révéler ultérieurement utiles. En effet, postérieurement à la transcription d'une communication enregistrée, le déroulement progressif de l'enquête peut amener l'enquêteur à devoir accéder à l'enregistrement, à la lumière de nouveaux éléments dont il dispose, par exemple pour identifier un nouveau correspondant ou opérer de nouveaux rapprochements.

La commission prend donc acte des justifications apportées par le ministère de la justice.

À la clôture de l'enquête, il est procédé à la mise sous scellés au format numérique des enregistrements, de telle sorte qu'ils ne sont alors plus accessibles aux enquêteurs. Les transcriptions réalisées dans la PNIJ sont quant à elles conservées pendant la durée des investigations.

Le deuxième alinéa de l'article 5 prévoit que les données et informations communiquées en application des articles L. 34-1 du CPCE et 6-II de la LCEN ainsi que les informations relatives à la reconnaissance vocale du locuteur soient conservées jusqu'à la date de clôture de l'enquête et de la transmission de la procédure à l'autorité judiciaire. Le dossier de saisine indique que les empreintes vocales sont quant à elles conservées pendant la durée de l'affaire puis sont effacées. Par conséquent, la commission demande que la durée de conservation de cette information et sa transmission ou non à l'autorité judiciaire soient clairement établies.

S'agissant des procès-verbaux, seuls ceux prévus aux articles 100-4, 100-5 et R.15-33-71 du CPP sont conservés dans la PNIJ, jusqu'à la date de clôture des investigations, puis ils sont automatiquement effacés. Les procès-verbaux prévus aux articles R. 15-33-74 et 100-6 du CPP ne sont pas enregistrés dans le traitement.

Sur les destinataires des données :

L'article 3 du projet de décret prévoit les personnels habilités à accéder directement aux données enregistrées dans le traitement.

Il s'agit, en application des I et II de cet article, chacun pour les besoins des procédures dont ils sont saisis, des magistrats, des officiers de police judiciaire mentionnés aux 2° et 4° de l'article 16 du CPP, des agents de police judiciaire au sens de l'article 20 du même code, ainsi que des agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires en application, respectivement, des articles 28-1 et 28-2 dudit code. Seuls les magistrats peuvent avoir accès aux scellés par l'intermédiaire du portail « scellés » de la PNIJ, tel n'est pas le cas des personnels visés au II de cet article 3.

L'article 100-5 du CPP prévoit que les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin. À cet égard, le III de l'article 3 prévoit que, pour les missions qui leur sont confiées, les interprètes-traducteurs peuvent accéder aux communications électroniques désignées par l'officier de police judiciaire, l'agent des douanes ou des services fiscaux, et ce pour une durée limitée. Ces personnels sont choisis dans les conditions prévues par l'article 157-1 du CPP. Toutefois, dans certaines hypothèses, il est possible de recourir à des tiers non répertoriés, notamment lorsque des langues rares sont concernées. La commission prend acte de l'engagement du ministère de modifier le projet de décret afin de mentionner expressément que les données relatives aux interprètes-traducteurs seront collectées.

Le IV de cet article prévoit que pour la mise au clair des données chiffrées, l'organisme technique soumis au secret de la défense nationale visé à l'article 230-2 du CPP peut accéder aux données et informations relatives au contenu des interceptions chiffrées et, le cas échéant, aux données et informations utiles au déchiffrement.

Les V et VI de l'article 3 du projet de décret prévoient que des personnels « supports » aidant à la résolution des difficultés techniques, à la maintenance et à l'entretien de la plate-forme pourront également avoir accès aux données et informations enregistrées dans le traitement. Ils sont soit désignés et spécialement habilités par le secrétaire général du ministère de la justice, soit liés par un contrat pour les prestations détachables des finalités judiciaires. Le VII du même article prévoit que ces deux catégories de personnes (les personnels en charge du fonctionnement, de la maintenance et de l'entretien de la plate-forme, et ceux auxquels peuvent être confiées par contrat les prestations détachables des finalités judiciaires du traitement) prêtent serment devant le tribunal d'instance de leur résidence administrative, la formule du serment étant mentionnée dans le projet de décret.

La commission s'interroge sur les différences qui marquent l'intervention de ces deux catégories de personnels. En effet, toutes les deux aident à la résolution des difficultés techniques, mais seuls les personnels de l'une des deux catégories sont habilités au niveau confidentiel défense et les modalités d'autorisation d'intervention de ces personnels diffèrent.

L'ensemble des accès s'effectue par authentification forte, excepté pour les traducteurs-interprètes. Afin de compenser l'absence d'authentification forte dans ce dernier cas, des mesures compensatoires ont été mises en place. En particulier, l'accès est, conformément au projet de décret, temporaire et limité aux seuls documents identifiés comme nécessitant une traduction. De plus, l'authentification au service par identifiant/mot de passe ne peut s'effectuer qu'en utilisant un ordinateur spécifiquement sécurisé mis à disposition par le ministère.

Sur le contrôle de la PNIJ :

L'article 7 du projet de décret prévoit que la PNIJ est placée, sous le contrôle d'un magistrat, assisté par un comité dont la composition est fixée à l'article 8 du projet. Ce magistrat peut demander à l'autorité gestionnaire toute information relative au traitement. Il peut en outre ordonner toute mesure nécessaire à l'exercice de son contrôle et il dispose, avec les membres du comité de contrôle, d'un accès permanent aux lieux où se trouve la PNIJ. Un rapport annuel établi par ce magistrat est enfin adressé au garde des sceaux.

Dès lors que les principaux fichiers de police judiciaire sont placés sous le contrôle d'un « magistrat référent », la commission ne peut que se satisfaire que tel soit également le cas pour la PNIJ.

Toutefois, dans la mesure où la PNIJ constitue un traitement de données à caractère personnel, qui plus est d'une grande sensibilité, la commission déplore que le ministère n'ait pas souhaité modifier le projet de décret afin de la rendre destinataire de ce rapport annuel.

Le ministère a indiqué, lors de l'instruction du dossier, que le comité qui assiste ce magistrat a pour mission de contrôler le respect des finalités de la PNIJ, notamment en opérant un contrôle sur le personnel chargé du support technique et fonctionnel. Il a ajouté que sa mission portera également sur le contrôle de la mise en œuvre des évolutions technologiques de la PNIJ. La commission regrette par conséquent, au regard de ces missions, de ne pas être représentée au sein de ce comité.

Enfin, si les pouvoirs confiés à ce magistrat s'exercent sans préjudice des pouvoirs de contrôle exercés par la commission en application de l'article 44 de la loi du 6 janvier 1978 modifiée, la commission aurait souhaité des clarifications sur l'articulation concrète de ces différents pouvoirs de contrôle.

Sur les droits des personnes :

L'article 10 du projet de décret prévoit que les droits d'information et d'opposition ne s'appliquent pas au traitement projeté, en application des articles 32-VI et 38 de la loi du 6 janvier 1978 modifiée. La commission relève toutefois que cette exception au droit d'information ne s'applique qu'aux personnes visées par l'interception ou la réquisition ainsi qu'à leurs interlocuteurs. Les utilisateurs de la PNIJ seront informés *a priori* des conditions de conservation des données les concernant.

En application des articles 41 et 42, les droits d'accès et de rectification s'exerceront de manière indirecte pour les personnes « cibles » et leurs interlocuteurs. Les utilisateurs de la PNIJ pourront quant à eux exercer leurs droits d'accès et de rectification de manière directe, conformément à l'article 39 de la loi du 6 janvier 1978 modifiée.

Ces dispositions n'appellent pas d'observation particulière de la part de la commission.

Sur la sécurité des données et la traçabilité des actions :

Tout d'abord, la PNIJ étant un système d'information faisant notamment l'objet d'échanges par voie électronique entre autorités administratives, la commission considère qu'elle est soumise à l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qui introduit le référentiel général de sécurité (RGS).

Les mesures prévues dans le système permettent, par rapport aux dispositifs actuellement utilisés, une amélioration très significative de la maîtrise par les magistrats de l'efficacité et de la sécurité des interceptions judiciaires et des données qu'elles contiennent, tout en apportant des garanties plus importantes vis-à-vis des citoyens et des enquêteurs.

En appliquant un principe de défense en profondeur, des mesures respectant les bonnes pratiques sont en effet prévues pour agir sur le caractère identifiant des données (minimisation des données et anonymisation des données de tests), sur le caractère préjudiciable des impacts potentiels (redondance et sauvegardes, contrôle d'intégrité et gestion des incidents), sur les capacités des sources de risques (cloisonnement, chiffrement, traçabilité des actions, marquage des documents, gestion des personnels, contrôle d'accès logique, encadrement des relations avec l'hébergeur, lutte contre les codes malveillants, contrôle d'accès physique, protection contre les sources de risques non humaines) et sur les vulnérabilités des supports des données (logiciels, matériels, canaux informatiques et personnes).

La commission note également l'existence d'une politique de sécurité, l'utilisation de produits certifiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le respect du référentiel général de sécurité (RGS) pour les fonctions d'authentification (d'une personne par l'utilisation d'identifiants et de mots de passe statiques, d'une personne par certificat électronique, d'un serveur par certificat électronique), de signature électronique (d'une personne par certificat électronique, cachet d'un serveur par certificat électronique), de confidentialité et d'horodatage.

En ce qui concerne la traçabilité, l'article 6 du projet de décret prévoit que toute action fait l'objet de mesures de traçabilité, les traces étant conservées cinq ans. Au regard de la nouveauté du dispositif et de l'ampleur des réquisitions qui seront traitées *via* le dispositif, la commission estime que cette durée permettra d'exploiter au mieux les traces afin de détecter tout détournement de finalité.

Il serait utile également qu'un mécanisme automatique soit mis en place pour détecter les traces dont la durée de conservation est arrivée à échéance pour les supprimer. A cet égard, la commission prend acte que cette préconisation fait partie des évolutions techniques que le ministère entend solliciter de son prestataire. Par ailleurs, il serait souhaitable que l'ensemble des traces, y compris celles relatives aux actions réalisées sur le cadre juridique associé à une réquisition, fasse l'objet d'une synthèse régulière à l'attention du comité mentionné aux articles 7 et 8 du projet de décret.

Il conviendrait enfin de clarifier la procédure de gestion des incidents et d'informer les parties prenantes de la personne qu'ils doivent contacter en cas d'incident.

Sous réserve de ces remarques, les mesures décrites par le ministère réduisent les risques identifiés sur la vie privée à un niveau acceptable au regard des enjeux du traitement considéré. Les mesures sont par conséquent conformes à l'exigence de sécurité prévue par l'article 34 de la loi du 6 janvier 1978 modifiée.

La commission rappelle toutefois que cette obligation nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

La présidente,
I. FALQUE-PIERROTIN