N° 7424[8]

CHAMBRE DES DEPUTES

PROJET DE LOI

portant création d'une plateforme commune de transmission électronique sécurisée et modification :

1° du Code de procédure pénale ;

2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

* * *

DEUXIEME AVIS COMPLEMENTAIRE DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(31.10.2024)

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

Par ailleurs, l'article 36.4 du RGPD dispose que « *[l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement* ».

2. Le 5 juin 2019, la CNPD a avisé le projet de loi n°7424 portant création d'une plateforme commune de transmission électronique sécurisée et modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat (ci-après le « projet de loi »)[1]. Suite à des amendements parlementaires adoptées le 11 juin 2024, la CNPD a adopté son avis complémentaire le 30 août 2024[2].

3. Le 15 octobre 2024, la Commission de la Justice a adopté un amendement unique (ci-après l' « amendement ») visant à répondre aux critiques soulevés par le Conseil d'Etat[3].

4. La Commission nationale regrette que l'amendement et son commentaire ne répondent pas aux interrogations soulevées dans son avis complémentaire. Néanmoins, l'amendement lui permet de mieux comprendre l'intention des auteurs du projet de loi, notamment en ce qui concernent les modifications apportées à l'article 43-1 du Code de procédure pénale.

---

1 V. Délibération n°40/2019 du 5 juin 2019 de la Commission nationale pour la protection des données, doc. parl. N°7424/01.

2 V. Délibération n°56/AV24/2024 du 30 août 2024 de la Commission nationale pour la protection des données, doc. parl. N°7424/06.

3 V. Avis complémentaire n°53.323 du Conseil d'Etat du 12 juillet 2024, doc. parl. N°7424/5.

5. En effet, la CNPD comprend désormais que la nouvelle rédaction de l'article 43-1 du Code de procédure pénal entend introduire une mesure d'accès aux données de trafic et de localisation, sans prévoir une mesure de conservation. Ainsi, le procureur d'Etat peut ordonner que les opérateurs et fournisseurs de services de communications électroniques fournissent pour une durée d'un mois les données de trafic et de localisation qu'ils détiennent à ce moment. Il convient de noter que cette mesure est renouvelable.

6. La CNPD souhaite cependant soulever quelques interrogations quant à la nouvelle mesure d'accès aux données de trafic et de localisation.

7. Tout d'abord, il y a lieu de relever que la disposition sous avis introduit une mesure d'accès et non pas une mesure de conservation. Elle se limite donc à permettre aux autorités compétentes d'accéder aux seules données que les opérateurs et fournisseurs de services de communications électroniques détiennent au moment de l'ordonnance, voire les données qui auraient été collectées par ces derniers durant la durée d'application de l'ordonnance du procureur d'Etat. Une obligation de conservation ultérieure de telles données par les opérateurs et fournisseurs de services de communications électroniques, pour des finalités ultérieures, c'est-à-dire les objectifs de la recherche de personnes disparues, ne peut pas avoir lieu. Ceci est notamment important à prendre en compte en vue du changement de paradigme que le projet de loi 81484 entend apporter. En effet, le projet de loi 8148 entend abroger le principe de conservation généralisée et indifférenciée des données de trafic et de localisation.

Ainsi, pour contraindre les opérateurs et fournisseurs de services de communications électroniques à conserver de telles données, au-delà du délai de conservation prévu pour les finalités de facturation ou de recours en relation avec ces factures[5], il faudrait prévoir une mesure de conservation propre. Il résulte effectivement de la jurisprudence de la Cour de Justice de l'Union européenne (ci-après la « CJUE » ou la « Cour ») que le principe de la hiérarchie des objectifs exige que des données de trafic et de localisation conservées pour, par exemple, des objectifs de sauvegarde de la sécurité nationale ne peuvent pas être accédées pour des objectifs de moindre importance.

Dès lors, l'article 43-1 du Code de procédure pénale ne pourra être utilisé que pour accéder à des données actuellement à disposition des opérateurs et fournisseurs de services de communications électroniques ou éventuellement à des données conservées pour des objectifs avec le même degré d'importance.

En revanche, elle ne pourra pas être utilisée pour accéder à des données conservées pour des finalités avec un degré d'importance plus élevé. Pour des développements plus amples sur le principe de la hiérarchie des objectifs, la CNPD renvoie à son avis relatif au projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat[6].

---

4 Projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

5 A noter qu'il existe quelques autres exceptions pour conserver les données de trafic et de localisation.

6 Délibération n°28/AV12/2024 de la Commission nationale de la protection des données du 16 mai 2024, doc. parl, n°8148/06, notamment point 109.

8. Il convient encore de rappeler que toute mesure d'accès aux données de trafic et de localisation doit répondre aux exigences de la CJUE en matière de rétention des données[7]. Ainsi, la mesure d'accès sous avis doit être lue à la lumière des arrêts pertinentes de la CJUE.

9. La Cour exige notamment que « *il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* »[8]. Ainsi, la Cour exige deux choses : une demande motivée par les autorités compétentes qui souhaitent accéder aux données et un contrôle préalable indépendant.

10. Si la CJUE ne donne pas davantage de précisions sur la demande d'accès motivée, que les autorités compétentes doivent soumettre à l'entité qui effectue le contrôle, elle s'est néanmoins prononcée sur le caractère indépendant et préalable de ce contrôle.

11. Premièrement, en ce qui concerne le caractère indépendant du contrôle, la Cour explique 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* »[9]. Elle ajoute encore que « *[t]el n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. En effet, le ministère public a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale. La circonstance que le ministère public soit, conformément aux règles régissant ses compétences et son statut, tenu de vérifier les éléments à charge et à décharge, de garantir la légalité de la procédure d'instruction et d'agir uniquement en vertu de la loi et de sa conviction ne saurait suffire à lui conférer le statut de tiers par rapport aux intérêts en cause […]* »[10]. La CJUE finit par conclure que « *le ministère public n'est pas en mesure d'effectuer le contrôle préalable* »[11].

12. Deuxièmement, la Cour souligne encore à plusieurs reprises le caractère préalable du contrôle. En effet, elle n'admet un contrôle postérieur qu'en cas d'urgence dûment justifiés[12]. Elle exige par ailleurs que le contrôle a posteriori intervient « *dans de brefs délais* »[13].

---

7 Arrêt du 8 avril 2014, Digital Rights Ireland e. a., C-293/12 et C-594/12, EU:C:2014:238 ;
arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15et C-698/15, EU:C:2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e. a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ;
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021 , Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Siochâna e. a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ;
arrêt du 17 novembre 2022, Spetsializiranaprokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura délia Repubblica pressa il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ; et
arrêt du 30 avril 2024, La Quadrature du Net e. a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.

8 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15et C-698/15, EU:C:2016:970, point 120.

9 Arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 54.

10 Ibid. points 55 et 56.

11 Ibid. point 57.

12 Voir par exemple arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 120.

13 Arrêt du 5 avril 2022, Commissioner of An Garda Siochána e.a., C-140/20, EU:C:2022:258, point 110.

13. Dans la mesure où la disposition sous avis entend laisser l'appréciation de la nécessité de la mesure au seul procureur d'Etat, la CNPD se demande si les exigences de la CJUE concernant le contrôle indépendant et préalable sont remplies.

14. Ensuite, la CJUE exige que la législation nationale prévoit des garanties effectives contre les risques d'abus. Ainsi, la CJUE demande à ce que les « *autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités* »[14]. En effet, cette information est nécessaire pour permettre aux personnes dont les données ont été accédées d'exercer leurs droits. Il est effectivement impossible pour une personne d'exercer ses droits s'il n'est pas au courant de la situation.

15. Etant donné que l'amendement sous avis n'entend pas introduire une telle information à fournir aux personnes concernées, la CNPD estime que l'exigence de la CJUE n'est pas respectée.

16. Enfin, la CJUE soulève que l'accès ne peut avoir lieu que dans la limite du strict nécessaire. Elle décide « *dès lors qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire […]* »[15]. La Cour explique que « *la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction (voir, par analogie, Cour EDH, 4 décembre 2015, Zakharov c. Russie, CE:ECHR:2015: 1204JUD004714306, § 260). Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités* »[16].

17. Au vu de ce qui précède, la CNPD se demande encore si la rédaction actuelle de la disposition répond aux critères de la CJUE en ce qui concerne la limitation au strict nécessaire. En effet, la disposition reste muette sur le choix des personnes dont les données pourraient être accédées, ou pour tout le moins elle ne contient pas de conditions ou critères permettant de délimiter ces personnes. Tel que soulevé par la CJUE, il devrait au moins exister un lien indirect entre l'objectif recherché (la recherche de la personne) et les personnes dont les données seront accédées.

Ainsi adopté à Belvaux en date du 31 octobre 2024.

La Commission nationale pour la protection des données

Thierry LALLEMANG	Alain HERRMANN	Marc LEMMER
Commissaire	*Commissaire*	*Commissaire*

14 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 121.

15 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

16 *Ibid*.

Impression: CTIE – Division Imprimés et Fournitures de bureau