



Avis n° 25/2020 du 13 mars 2020

Objet : Demande d'avis concernant

- **le Projet d'arrêté ministériel portant exécution de l'article 6, § 3, alinéa 2, et de l'article 10bis, alinéa 2, de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques (CO-A-2020-012)**
- **le Projet d'arrêté ministériel portant exécution de l'article 6, alinéa 2, et de l'article 8, § 3, alinéa 3, de l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité (CO-A-2020-016)**

L'Autorité de protection des données (ci-après l' "Autorité") ;

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu le 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") ;

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après "la LTD") ;

Vu la demande d'avis de Philippe De Backer, ministre de l'Agenda numérique, des Télécommunications et de la Poste, chargé de la Simplification administrative, de la Lutte contre la fraude sociale, de la Protection de la vie privée et de la Mer du Nord, reçue le 14 janvier 2020 ;

Vu le rapport de Madame Alexandra Jaspar, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Émet, le 13 mars 2020, l'avis suivant :

I. OBJET DE LA DEMANDE

1. Le ministre de l'Agenda numérique, des Télécommunications et de la Poste, chargé de la Simplification administrative, de la Lutte contre la fraude sociale, de la Protection de la vie privée et de la Mer du Nord (ci-après "le demandeur"), sollicite l'avis de l'Autorité sur deux projets d'arrêtés ministériels :

- le projet d'arrêté ministériel *portant exécution de l'article 6, § 3, alinéa 2, et de l'article 10bis, alinéa 2, de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques* (ci-après le projet 1) et
- le projet d'arrêté ministériel *portant exécution de l'article 6, alinéa 2, et de l'article 8, § 3, alinéa 3, de l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité* (ci-après le projet 2).

Contexte

2. En vertu des articles 88*bis* et 90*quater* du Code d'Instruction criminelle, les autorités judiciaires peuvent, dans le cadre de l'exercice de leurs missions, requérir la collaboration d'opérateurs de réseaux de communications électroniques et de fournisseurs de services de communications électroniques (ci-après opérateurs et fournisseurs télécoms). Conformément aux articles 18/8 et 18/17 de la loi *organique des services de renseignement et de sécurité* du 30 novembre 1998, les services de renseignement et de sécurité peuvent également le faire. Les modalités de cette obligation légale de collaboration sont élaborées par arrêté royal, plus précisément : l'arrêté royal susmentionné du

9 janvier 2003¹ relatif aux demandes judiciaires et l'arrêté susmentionné du 12 octobre 2010² relatif aux demandes par les services de renseignement et de sécurité.

3. L'article 6, § 3, alinéa 2 et l'article 10bis, alinéa 2 de l'arrêté royal susmentionné du 9 janvier 2003 ainsi que l'article 6, alinéa 2 et l'article 8, § 3, alinéa 3 de l'arrêté royal susmentionné du 12 octobre 2010 disposent ce qui suit en ce qui concerne l'obligation légale de collaboration des opérateurs et fournisseurs télécoms envers, respectivement, les autorités judiciaires et les services de renseignement et de sécurité :

- les ministres compétents en la matière *"déterminent le format spécifique de présentation des données par les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques, ainsi que le mode de transmission de ces données"* ;
- *"Les spécifications techniques doivent répondre aux standards et rapports mentionnés ci-dessous du "European Telecommunications Standards Institute" (ci-après ETSI), y compris les actualisations éventuelles (...).*

Les options qui doivent être prises dans ces standards seront déterminées par les ministres compétents.

4. Les projets qui sont soumis pour avis exécutent les dispositions susmentionnées et leur contenu est quasi identique. Les deux projets prévoient les modalités techniques suivantes pour les transferts de données dans le cadre de l'obligation légale de collaboration des opérateurs et fournisseurs télécoms (et ce à chaque fois en référence aux normes ETSI applicables) :

- mise en mémoire tampon (buffering) (article 1^{er} des deux projets) : pour éviter la perte de données et en cas d'interruption de la transmission des données demandées des opérateurs et fournisseurs télécoms vers le service NTSU-CTIF³ (pour les demandes judiciaires) d'une part et vers le point de terminaison du réseau désigné par le dirigeant du service concerné (pour les demandes de services de renseignement et de sécurité) d'autre part, l'opérateur/le fournisseur veille à ce que les données soient temporairement conservées dans une mémoire tampon disposant à cette fin d'une capacité suffisante ;
- filtrage (article 2 des deux projets) : afin d'éviter la transmission de données non pertinentes de manière à ce que seules les données effectivement demandées par l'autorité ou le service compétents soient transmises, chaque opérateur/fournisseur est techniquement à même de

¹ En ce qui concerne le projet d'arrêté royal abrogeant et remplaçant cet arrêté royal du 9 janvier 2003, le prédécesseur en droit de l'Autorité a déjà émis l'avis n° 29/2008 du 3 septembre 2008.

² Le prédécesseur en droit de l'Autorité a émis un avis concernant le projet d'arrêté royal, à savoir l'avis n° 23/2010 du 30 juin 2010.

³ "National Technical & Tactical Support Unit-Central Technical Interception Facility" : le système central d'interception technique du service de police intégrée (voir les articles 1.4, 3 et 10bis de l'arrêté royal du 9 janvier 2003 *déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques*).

filtrer ce flux de données au strict minimum, sans prendre connaissance du contenu des communications.

5. Déjà en 2014, un texte très similaire des deux projets avait été soumis pour avis au prédécesseur en droit de l'Autorité, qui s'était alors exprimé favorablement à leur sujet dans l'avis n° 27/2014 du 2 avril 2014.

Le Conseil d'État avait toutefois estimé dans ses avis 66.672/4 et 66.673/4 du 25 novembre 2019 concernant les deux projets que ceux-ci devaient à nouveau être soumis à l'Autorité de protection des données, vu que depuis 2014, le cadre juridique en matière de protection des données avait changé, tant sur le plan européen que national.

6. Les projets sont confrontés ci-après au RGPD et à la LTD.

II. EXAMEN DE LA DEMANDE

7. L'Autorité renvoie tout d'abord aux remarques déjà formulées par son prédécesseur en droit dans son avis n° 27/2014 du 2 avril 2014, lesquelles s'appliquent encore intégralement aux projets qui sont actuellement soumis.

8. L'article 1^{er} des projets prescrit la conservation temporaire par les opérateurs et fournisseurs télécoms des données de télécommunication qui leur sont demandées dans une mémoire tampon disposant d'une capacité suffisante, et ce pour éviter la perte de données en cas d'interruption éventuelle de la transmission des données.

9. L'Autorité attire l'attention sur le fait que les données à caractère personnel qui font l'objet d'une transmission déterminée doivent être immédiatement supprimées de la mémoire tampon précitée dès que leur transmission aux autorités judiciaires ou aux services de renseignement et de sécurité compétents a été menée à bien. Selon l'article 5.1.e) du RGPD, les données à caractère personnel sont en effet conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité visée.

10. L'article 2 des projets oblige les opérateurs et fournisseurs télécoms à filtrer préalablement les flux de données vers les autorités judiciaires ou les services de renseignement et de sécurité compétents de sorte que seules les données pertinentes dans le cadre de la demande formulée soient transmises. Les projets précisent également à cet égard que lors de ce filtrage, les opérateurs et fournisseurs télécoms ne peuvent en aucun cas prendre connaissance du contenu des communications. Cette méthode de travail est conforme au principe de minimisation des données (article 5.1.c) du RGPD).

11. L'article 2, § 2, in fine du projet prévoit certes à cet égard que lorsqu'il n'est techniquement pas possible de filtrer sans prendre connaissance du contenu du flux de communication, le flux de données complet (non filtré) peut être transmis au service de renseignement et de sécurité demandeur. L'Autorité en prend acte. Elle attire cependant l'attention sur le fait que, si les autorités judiciaires ou les services de renseignement et de sécurité compétents reçoivent ainsi des données à caractère personnel qui tombent en dehors du champ d'application de leur demande en la matière, ils doivent les détruire/supprimer sans délai. En application de l'article 5.1.c) du RGPD, les données personnelles traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées⁴.

**PAR CES MOTIFS,
l'Autorité**

estime que l'adaptation suivante s'impose dans les projets :

- limitation explicite de la conservation de données à caractère personnel dans la mémoire tampon jusqu'à leur transmission réussie à l'autorité/au service demandeur (voir le point 9) ;

attire l'attention du demandeur sur l'importance de l'élément suivant :

- destruction/suppression sans délai par les autorités judiciaires ou les services de renseignement et de sécurité compétents de données à caractère personnelle excessives (tombant en dehors du champ d'application de leur demande) reçues suite à d'éventuels flux de communication non filtrés (voir le point 11).

(sé) Alexandra Jaspar
Directrice du Centre de Connaissances

⁴ Voir aussi le point 7 de l'avis n° 27/2014 du 2 avril 2014 du prédécesseur en droit de l'Autorité.