ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Notre référence	Annexe(s)	Date
DD180009		13.12.2018

Objet : Avis d'initiative relatif au cadre juridique (de protection des données) lors de consultations illicites de banques de données par les membres de la police intégrée, de l'AIG et de l'Unité d'information des passagers.

L'Organe de contrôle de l'information policière (ci-après "le COC" ou "l'Organe de contrôle").

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (*M.B.* du 5 septembre 2018, ci-après la "LPD"), en particulier l'article 59, § 1er, 2e alinéa, l'article 71 et le titre 7, en particulier l'article 236, § 2.

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 4, § 2, quatrième alinéa.

Vu la loi du 5 août 1992 *sur la fonction de police* (ci-après la "LFP"), en particulier l'article 44/6.

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 13 décembre 2018, l'avis d'initiative suivant :

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a profondément modifié les tâches et les missions de l'Organe

[1] 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 ou "RGPD").

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la*

de contrôle. L'article 4, § 2, quatrième alinéa de la loi organique du 3 décembre 2017 *portant création de l'Autorité de protection des données* (ci-après la "Loi organique APD") dispose que pour les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux*, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

2. Cela signifie notamment que l'Organe de contrôle est également compétent lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socio-économiques ou de traitements de ressources humaines. L'Organe de contrôle doit être consulté dans le cadre de la préparation d'une législation ou d'une mesure réglementaire liée au traitement de données à caractère personnel par les services de police de la police intégrée (voir l'article 236, § 2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la Directive Police-Justice). Dans ce cadre, l'Organe de contrôle a pour mission d'examiner si l'activité de traitement envisagée par les services de police est conforme aux dispositions des Titres 1er (pour les traitements non opérationnels)[3] et 2 (pour les traitements opérationnels) de la LPD[4]. En outre, le COC a également une mission d'avis d'initiative, prévue à l'article 236, § 2 de la LPD, et une mission d'information générale du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

3. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou de police judiciaire, l'Organe de contrôle émet un avis, soit d'initiative, soit à la demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police concernant toute question relative à la gestion de l'information policière, telle que régie dans la section 12 du chapitre 4 de la loi *sur la fonction de police*[5].

4. Enfin, l'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel telles que visées aux articles 44/1 à 44/11/13 de la loi *sur la fonction de police* et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois vis-à-vis des services de police, de l'Inspection générale de la police fédérale et de la police locale (ci-après l' "AIG"), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après "BelPIU"), telle que visée dans le Chapitre 7 de la loi du 25 décembre 2016[6].

---

libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la "Directive Police et Justice").

[3] Article 4, § 2, quatrième alinéa de la Loi organique APD.

[4] Article 71, § 1er, troisième alinéa de la LPD.

[5] Article 236, § 2 de la LPD.

[6] Article 71, § 1er, troisième alinéa *juncto* article 236, § 3 de la LPD.

II. Quant au fond

5. L'Organe de contrôle est régulièrement interrogé sur l'application des dispositions pénales prévues à l'article 222, 1° et 2° de 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 "LPD"). Plus précisément, il s'agit de la question visant à connaître l'incrimination concrète et le cadre juridique applicable lors de consultations, par des membres de services de police, de banques de données, telles que la BNG, le Registre national, etc. en dehors de leurs missions de police administrative et judiciaire, en d'autres termes lors de consultations illicites/illégales. Dans le prolongement de cela, se pose également la question de l'application de l'article 229 de la LPD, c'est-à-dire le concours de sanctions pénales et administratives. Le présent avis d'initiative se concentre sur la situation du membre des services de police mais s'applique également, *mutatis mutandis*, aux membres de l'AIG et de BelPIU.

6. Les points 1° et 2° de l'article 222 de la LPD sanctionnent le responsable du traitement ou le sous-traitant, son préposé ou son mandataire, l'autorité compétente, visés aux titres 1er et 2, lorsque :
1° les données à caractère personnel sont traitées sans base juridique conformément à l'article 6 du Règlement[7] et aux articles 29, § 1er, et 33, § 1er, de la LPD*, y compris les conditions relatives au consentement et au traitement ultérieur ;*
2° les données à caractère personnel sont traitées en violation des conditions imposées par l'article 5 du Règlement et par l'article 28 de la LPD *par négligence grave ou avec intention malveillante.*

Concrètement, la disposition pénale de l'article 222, 1° de la LPD concerne l'infraction aux conditions d'admissibilité, le traitement ultérieur à d'autres fins et l'absence d'un fondement légal pour le traitement. La disposition pénale de l'article 222, 2° concerne l'infraction aux principes du traitement de données à caractère personnel.

7. Il faut d'abord répondre à la question de savoir qui doit être désigné en tant que responsable du traitement, mandataire, sous-traitant, préposé ou autorité compétente. La réponse à cette question est déterminée par la finalité pour laquelle les données à caractère personnel sont traitées. En outre, comme cela apparaîtra dans la suite du texte, la réponse est cruciale pour la désignation de

[7] 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 ou "RGPD").

l'autorité de contrôle compétente pour la prise de mesures correctrices éventuelles. Ensuite, il faut examiner si le traitement peut reposer sur un fondement d'admissibilité légitime[8].

8. Le fonctionnaire de police qui recherche des personnes dans les banques de données susmentionnées en dehors de la finalité de police administrative ou judiciaire exécute une activité de traitement qui relève du champ d'application du Règlement général sur la protection des données ("RGPD") et du Titre 1er de la LPD, étant donné qu'il ne poursuit pas une finalité opérationnelle en vertu du Titre 2 de la LPD. Le fonctionnaire de police ne peut pas non plus, en soi, être qualifié d' "autorité compétente", vu qu'il ne constitue pas à lui seul un service de police au sens de l'article 2, 2° de la loi sur la police intégrée[9], et que le traitement n'est pas non plus exécuté pour le compte de l'autorité compétente dont le fonctionnaire de police fait partie. Dans ce cas, le fonctionnaire de police doit donc être considéré lui-même en tant que responsable du traitement, l'obligeant ainsi à respecter personnellement toutes les obligations du RGPD et de la LPD. Il faut en l'occurrence partir du principe que le fonctionnaire de police fixe lui-même les finalités et les moyens, certes de manière illicite (voir plus loin). Il définit en effet lui-même la raison pour laquelle les données à caractère personnel sont traitées (finalités : par exemple : "ce que sait la police me concernant ou concernant mon ex-conjoint", je veux connaître les antécédents d'une personne avec laquelle je suis impliqué dans un différend privé, etc.) et quelle(s) banque(s) de données (moyen) il utilise à cet effet[10].

Ensuite, la question de la licéité du traitement se pose. Étant donné que l'activité de traitement ne s'inscrit pas dans le cadre du champ d'application du Titre 2, le traitement ne relève pas des articles 29, § 1er et 33, § 1er mentionnés à l'article 222, 1° de la LPD. Dès lors, le traitement doit être conforme à un des fondements d'admissibilité de l'article 6 du RGPD[11]. Si le traitement ne peut pas se fonder sur l'une des conditions d'admissibilité de l'article 6 du RGPD, comportement qui est punissable en vertu de l'article 222, 1° de la LPD, le traitement est en principe également illicite au sens de l'article 5 du RGPD, comportement punissable en vertu de l'article 222, 2° de la LPD[12]. En effet, celui qui ne peut désigner aucun fondement légal pour son traitement traite les données à caractère personnel *ipso facto* de manière illicite et commet donc une violation de la LPD sanctionnée pénalement.

---

[8] Par souci d'exhaustivité, nous faisons remarquer que l'exception à l'application du Règlement pour les traitements par une personne physique pour des finalités strictement personnelles ou domestiques ne peut pas être retenue (article 2.2.c) du RGPD). Même si, par exemple, le fonctionnaire de police effectuait uniquement de lui-même une recherche dans la BNG, cela ne pourrait pas être considéré comme un traitement pour des finalités strictement personnelles étant donné que le fonctionnaire de police ne peut exécuter dans la BNG que des traitements ayant un caractère professionnel/opérationnel et jamais pour des finalités personnelles.

[9] Loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux*.

[10] Article 4, 7) et 2) du RGPD. Le responsable du traitement peut également être une personne physique.

[11] En bref, il s'agit du consentement, d'un contrat, d'une obligation légale, de l'intérêt public, de l'intérêt vital de la personne concernée et d'un intérêt important du responsable du traitement.

[12] Tout traitement n'est en effet licite que s'il répond aux obligations du RGPD. Il peut arriver que le traitement soit certes fondé sur une condition d'admissibilité de l'article 6 du RGPD mais soit quand même illicite, par exemple, parce qu'il est disproportionné.

La violation de l'article 5 (principes de base) du RGPD, punissable en vertu de l'article 222, 2° de la LPD, ne peut toutefois être sanctionnée pénalement que s'il s'agit d'une "*négligence grave ou d'une intention malveillante*"[13]. Comme précisé dans l'Exposé des motifs de la LPD, il s'agit de comportements qui sont qualifiés de "particulièrement graves". Le COC part du principe que lorsqu'un fonctionnaire de police consulte sciemment à des fins personnelles (non opérationnelles) la BNG, en contradiction dès lors avec les prescriptions légales, réglementaires et statutaires (qu'il est évidemment censé connaître), il traite dans ce cas des données à caractère personnel avec une intention malveillante, ou du moins en faisant preuve d'une négligence grave. Il convient de remarquer que les deux exigences morales particulières ne sont pas formulées dans l'article 222, 1° de la LPD, à savoir pour la violation des conditions d'admissibilité de l'article 6 du Règlement en l'occurrence, et que dans ce cas, une intention générale suffit pour pouvoir être punissable.

En d'autres termes, un tel comportement, à savoir une consultation illicite d'une banque de données policières, constitue toujours, selon le COC, une infraction tant à l'article 222, 1° qu'à l'article 222, 2° de la LPD.

Il résulte de l'article 229, § 2, premier alinéa de la LPD que dans le cadre de telles infractions, qui sont punissables tant pénalement qu'administrativement, tant qu'il n'y a pas de protocole d'accord entre le MP et l'autorité de contrôle compétente (en l'occurrence le COC), la prérogative d'agir est entre les mains du ministère public. Étant donné qu'aucun protocole n'a encore été établi entre le ministère public (MP) et le COC, le MP dispose de deux mois pour communiquer au COC qu'une information ou une instruction a été ouverte ou que des poursuites ont été entamées. Ce n'est que lorsque le MP décide de ne pas donner suite à l'affaire que le COC peut décider de prendre ou non des mesures correctrices.

Dans ce cadre, il convient toutefois de préciser que le COC ne peut prendre ces mesures qu'à l'encontre du service de police ("autorité compétente") et donc qu'il ne peut pas prendre lui-même directement des mesures correctrices[14] à l'encontre du fonctionnaire de police individuel concerné. À cet égard, pour les traitements du fonctionnaire de police, ce serait en l'occurrence l'Autorité de protection des données qui serait compétente (compétence résiduelle). Le cas échéant, l'Autorité de protection des données pourrait infliger au fonctionnaire de police individuel une sanction administrative ou plus exactement des mesures correctrices susmentionnées, à l'exception de l'amende (article 221, § 2, *juncto* article 229, § 2, deuxième alinéa de la LPD).

---

[13] Il convient de remarquer qu'en vertu de l'article 4, § 2, quatrième alinéa de la loi organique du 3 décembre 2017 *portant création de l'Autorité de protection des données*, le COC est également compétent pour les traitements relevant de l'application du RGPD.

[14] Les mesures correctrices sont mentionnées à l'article 58.2 du RGPD (avertir, rappeler à l'ordre, obliger à tenir la personne concernée informée d'une violation, etc.).

En outre, le fait que ce type de consultations illicites puisse aussi constituer une infraction de droit pénal commun, à savoir une violation de l'article 151 du Code pénal, et, en fonction du cas concret, aussi une infraction informatique (article 550*bis* du Code pénal dans toutes ses modalités), qui est d'ailleurs punie sensiblement plus lourdement, c'est l'évidence même qu'il revient au MP, en tant que premier organe, de donner une orientation au dossier. De plus, vu le principe "*non bis in idem*", il faudra aussi établir ensuite si l'Autorité de protection des données peut encore intervenir par le biais de sanctions à l'égard du fonctionnaire de police concerné (si le parquet propose par exemple un accord à l'amiable qui a été accepté, si l'on est déjà intervenu par voie de mesure disciplinaire et/ou s'il y a déjà eu sanction, etc.). Ces aspects ne peuvent toutefois être examinés qu'au cas par cas, étant donné que le principe "*non bis in idem*" requiert systématiquement un examen concret dans le cadre de l'évaluation visant à savoir si les différents mécanismes de sanction existants constituent ou non un ensemble logique et complémentaire ou un cumul non acceptable de sanctions.

Enfin, la question se pose encore de savoir si dans les cas indiqués, il est aussi question de ce qu'on appelle une "data breach" (fuite de données)[15]. En l'occurrence, on peut argumenter qu'il s'agit d'une violation de la sécurité entraînant un accès illicite ou non autorisé à des données enregistrées ou traitées d'une autre manière. Il s'agit quoi qu'il en soit d'un accès illégal à une banque de données dans le chef de sa profession et de sa fonction. Dans ce cas, l'autorité compétente, qui est le service de police concerné du lieu où le fonctionnaire de police a accédé à la BNG, à la DIV, au Registre national, etc., doit en faire une déclaration auprès de l'Organe de contrôle.

Cet aspect sera toutefois examiné plus avant au cours des prochains mois par le COC, notamment pour vérifier la manière dont les zones de police et les entités de la police fédérale peuvent remplir au mieux cette obligation.

[15] Il s'agit d'une "violation de données à caractère personnel". Il s'agit de toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données (article 4, 12) du Règlement).

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

émet l'avis d'initiative susmentionné

Avis approuvé par l'Organe de contrôle de l'information policière le 13 décembre 2018.

Pour l'Organe de contrôle,
Le Président,
(sé.) Philippe ARNOULD