Avis n° 46/2016 du 31 août 2016

Objet : demande d'avis relatif à un projet d'arrêté royal portant exécution de différents articles de la loi *relative à l'internement et à diverses dispositions en matière de Justice* (CO-A-2016-057)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis de Monsieur Koen GEENS, Ministre de la Justice, reçue le 11/07/2016 ;

Vu le rapport de Monsieur Dirk VAN DER KELEN ;

Émet, le 31 août 2016, l'avis suivant :

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général 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 la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

CONTEXTE

1. Le 25 novembre 2015, la Commission a émis un avis défavorable n° 47/2015 *sur l'avant-projet de loi relatif à l'internement et à diverses dispositions en matière de Justice*. Suite aux remarques formulées par la Commission, l'avant-projet initial a été adapté en plusieurs points et la loi du 4 mai 2016 *relative à l'internement et à diverses dispositions en matière de Justice* a été publiée au Moniteur belge le 13 mai 2016.

---

[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)

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 libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC).

2. Le projet d'arrêté royal portant exécution de différents articles de la loi *relative à l'internement et à diverses dispositions en matière de Justice*, ci-après le projet, vise à exécuter les dispositions de la loi susmentionnée relatives à la signification électronique. Il régit plus particulièrement :

- le déroulement d'une signification électronique ;
- les informations qui sont fournies après que la signification électronique a eu lieu ;
- la liste des adresses d'élection de domicile électronique ;
- le registre central des actes authentiques dématérialisés des huissiers de justice (ci-après le registre central).

EXAMEN DU PROJET

3. La signification électronique se fait via des systèmes numériques et va de pair avec le traitement automatisé de données à caractère personnel. Les dispositions de la LVP sont donc applicables.

Chapitre I. Manière de consentir à une signification par voie électronique

4. La signification à une autre adresse électronique que l'adresse électronique judiciaire peut s'avérer très hasardeuse. Il n'est expliqué nulle part la manière dont les huissiers de justice trouveront les adresses électroniques et plus particulièrement le lien entre une telle adresse et une personne physique concrète. Sur la base de test@privacycommission.be, on ne peut établir aucun lien avec Jean 0Janssens, résidant à la rue Pierre Henri, 7 à 1000 Bruxelles, à qui cette adresse électronique appartient. Achètera-t-on des adresses avec les titulaires présumés correspondants ?

5. Il ne fait aucun doute que des demandes de signification seront adressées à de mauvais destinataires. On le reconnaît d'ailleurs explicitement à l'article 4 du projet. La Commission maintient que la mise en œuvre d'un système de signification électronique - qui constitue soit le point de départ d'une procédure judiciaire, soit une étape dans une procédure judiciaire - sur la base de données à caractère personnel de qualité douteuse n'est pas conforme à l'article 4, § 1, 4° de la LVP.

6. Les articles 1er à 5 du projet décrivent le déroulement de la signification électronique qui repose sur le consentement exprès et préalable en vertu de l'article 32, 6° du Code judiciaire. Il en ressort que cette signification est composée des étapes suivantes :

- une demande de signification est envoyée ;
- la personne concernée s'identifie et s'authentifie ;

- après qu'il a été constaté que la personne identifiée et authentifiée correspond à celle à laquelle il faut adresser la signification, cette dernière consent à la signification par voie électronique.

7. Lorsque la signification est effectuée à une autre adresse électronique que l'adresse électronique judiciaire, les traitements de données qui en découlent reposent sur l'article 5, premier alinéa, a) de la LVP. Cela signifie qu'avant de demander au destinataire de fournir la moindre donnée à caractère personnel, ce dernier doit au préalable avoir donné son consentement informé de manière indubitable. Comme cela a déjà été signalé ci-dessus, on insiste également sur cet aspect à l'article 32, 6° du Code judiciaire.

8. Dans le système tel qu'il est conçu dans les articles susmentionnés, des informations sont bel et bien fournies et le consentement est demandé mais au départ, toutes les informations pertinentes ne sont pas fournies et le consentement est demandé alors que des données à caractère personnel de la personne concernée ont déjà été traitées.

9. L'article 2 du projet énumère les mentions que doit obligatoirement contenir la demande de signification. Intrinsèquement, ces mentions ne soulèvent aucune remarque particulière. Elles sont toutefois incomplètes. Une telle demande équivaut à une carte postale qui est déposée dans votre boîte aux lettres traditionnelle. En tant que destinataire, vous êtes libre d'y réagir ou non. Cela vaut également pour une demande de signification. La personne qui trouve une telle demande dans sa boîte aux lettres électronique n'est légalement pas tenue d'y réagir. La formulation actuelle des mentions donne l'impression que l'on est obligé de réagir. Dès lors, avant que le consentement ne soit évoqué, il faut clairement mentionner que l'on n'est pas obligé de réagir et que dans ce cas, il sera procédé à la signification de manière traditionnelle.

10. Afin que la personne concernée puisse donner son consentement indubitable (article 5, premier alinéa, a) de la LVP), toutes les informations pertinentes doivent lui être fournies au préalable. Cela signifie qu'il faut préciser clairement **au préalable** que lorsqu'il apparaît lors de l'authentification que la personne n'est pas celle à qui la signification doit être effectuée, l'opération sera clôturée (pas a posteriori comme l'article 4 du projet le prévoit actuellement). Idem en ce qui concerne l'enregistrement de l'adresse électronique et le délai de conservation. Il ressort des articles 6, 7 et 8 du projet qu'en cas de signification électronique réussie, l'adresse électronique est conservée pendant 30 ans et peut être réutilisée par d'autres huissiers de justice. Il s'agit d'informations qui doivent être

fournies avant de demander le consentement de la personne concernée. À défaut de ces informations, on ne peut pas parler d'un consentement informé[1].

11. S'il s'avère, après l'authentification, que l'on n'est pas à la "bonne adresse", on a inquiété la personne concernée inutilement (un huissier de justice est rarement porteur de bonnes nouvelles). Et les effets négatifs ne s'arrêtent pas là. Certains se demanderont s'ils ne sont pas victimes de "*phishing*" pour leur soutirer des données d'identité. Dans ce cas, il faudrait prévoir que l'huissier de justice concerné reçoive un message avec l'obligation de détruire cette adresse ainsi que les données qu'il y a liées, à la lumière de l'obligation de l'article 4, § 1, 4° de la LVP. Il est inacceptable que la personne concernée reçoive à nouveau ultérieurement une demande de signification qui ne lui est pas destinée.

12. Le consentement pour effectuer une signification électronique doit précéder le processus d'identification et d'authentification et non le suivre comme le prévoit actuellement l'article 5 du projet. Dans le cas contraire, il y a traitement de données à caractère personnel sans qu'il existe à cet effet, comme déjà précisé, une base légale (le consentement).

13. L'article 3 du projet dispose que l'identification et l'authentification se font par voie électronique. Il existe de nombreuses manières de s'identifier et de s'authentifier électroniquement[2] mais elles ne sont pas toutes aussi sûres. Sur la base d'une identification et d'une authentification électroniques réussies, un accès est accordé à des données à caractère personnel judiciaires (= sensibles). Le responsable du traitement doit garantir un niveau de protection adéquat, notamment compte tenu de l'état de la technique et de la nature des données (article 16, § 4 de la LVP). À la lumière de ces éléments, la Commission juge qu'un accès à des données judiciaires ne peut être accordé que sur la base d'un moyen d'identification et d'authentification électronique offrant le niveau de fiabilité le plus élevé. L'article 3 du projet doit donc également aborder le niveau de fiabilité requis du moyen d'identification et d'authentification électronique.

Chapitre II. Communications après une signification par voie électronique

14. L'article 6 du projet peut être compris de 2 façons.

---

[1] Le fait que les §§ 1er et 2 de l'article 32*quater*/2 du Code judiciaire contiennent une référence à cette liste et au délai de conservation ne constitue pas un sauf-conduit pour ne pas informer de manière aussi correcte et aussi complète que possible la personne concernée au préalable.

[2] En ce qui concerne cet aspect, la Commission peut indiquer qu'elle a été sollicitée afin d'émettre un avis sur un avant-projet de loi relative à l'identification électronique. Elle rendra cet avis dans les prochaines semaines et elle invite le demandeur à également l'examiner, étant donné qu'il existe des liens avec le présent dossier.

En outre, la Commission attire l'attention sur le fait qu'au sein de Fedict et de la Banque-carrefour des Entreprises, des projets sont en cours ayant pour but de pourvoir toutes les entreprises et tous les citoyens d'une adresse e-mail fiable qui serait utilisée pour les communications des autorités publiques. Il est souhaitable de contacter ces deux institutions afin d'examiner si des synergies sont possibles.

15. Lors d'une signification électronique réussie, la personne concernée reçoit un message contenant des informations à l'adresse d'élection de domicile électronique, c'est-à-dire une simple adresse e-mail sans mesure de sécurité spécifique. Le premier tiret donne l'impression que ce message, outre une mention que l'acte signifié est enregistré, contient également le contenu de l'acte, plusieurs données à caractère personnel et les moments auxquels certaines étapes du processus de signification électronique ont eu lieu. Si tel est le cas, cela signifie que des données judiciaires sont communiquées via un canal non sécurisé - l'e-mail peut très bien être comparé à une carte postale, tout le monde peut lire ce qui y figure. En outre, cela s'accompagnera souvent d'une transmission à un pays en dehors de l'Union européenne sans niveau de protection adéquat (voir également les points 12 à 14 de l'avis n° 47/2015 de la Commission). À la lumière des articles 16 et 21 de la LVP, un système permettant l'envoi de telles données judiciaires par e-mail serait absolument inacceptable[3].

16. La Commission estime en outre que les pièces à signifier doivent être conservées – de manière cryptée – sur un serveur des autorités publiques et que les e-mails des huissiers de justice ne pourraient reprendre que l'information selon laquelle une nouvelle pièce est disponible pour la personne concernée, après quoi cette dernière pourrait aller la consulter (après identification/authentification) sur ce serveur.

17. Les mentions reprises aux autres tirets qui font en fait référence aux prescriptions légales en la matière ne donnent lieu à aucune remarque spécifique.

Chapitre III. Liste des adresses d'élection de domicile électronique

18. L'article 7 du projet reprend ce qui a déjà été précisé à l'article 32*quater*/2, §§ 1er et 2 du Code judiciaire, à savoir que lors d'une signification électronique réussie à une adresse électronique, cette dernière est enregistrée en tant qu'adresse d'élection de domicile électronique dans une banque de données, ce qu'on appelle la liste des adresses d'élection de domicile électronique, et y est conservée pendant 30 ans.

---

[3] Voir également l'arrêt du Conseil d'État n° 233.777 du 9 février 2016 :

"*24. Le droit au respect de la vie privée et familiale est garanti en tant que droit fondamental à l'article 22 de la Constitution, à l'article 8 de la CEDH et à l'article 17 du Pacte DCP (droits civils et politiques). Il implique aussi le droit au secret de l'information sur la vie privée et la confidentialité de ces informations doit être garantie par les autorités. Afin d'avoir des chances de voir aboutir son recours auprès du Conseil du Contentieux des Étrangers, d'autant plus lorsqu'il s'agit de recours avec pouvoir de réformation à l'encontre d'une décision du Commissariat général aux réfugiés et aux apatrides, l'étranger est souvent contraint de communiquer des informations personnelles sensibles dans sa requête ou son mémoire de synthèse. Lors de la détermination du mode électronique qui devra être choisi pour l'envoi des pièces de procédure au greffe du Conseil du Contentieux des Étrangers, le législateur doit en tenir compte et dès lors opter pour un moyen sûr et fiable.*

Dans le mémoire de réponse, la partie adverse ne conteste pas en soi les éléments avancés par la partie requérante concernant la possibilité d'intercepter les échanges d'e-mails en cours d'envoi et même d'y apporter des modifications.

(...) Si l'utilisation d'un moyen déterminé est imposée pour la communication d'informations sensibles, il faut prévoir les garanties nécessaires que ces informations sont sécurisées. En l'occurrence, de telles garanties font défaut. (...)" [Traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle]

19. Disposer d'une liste reprenant uniquement les adresses d'élection de domicile électronique ne représente rien ou pas grand-chose (voir l'exemple au point 4). Cela signifie qu'outre l'adresse électronique, des données d'identification de la personne physique correspondant à cette adresse doivent également être mentionnées ou qu'au moins, un lien est établi vers ces informations dans le registre central. D'ailleurs, il ressort de l'article 8 du projet que l'adresse est de toute façon couplée au numéro de Registre national, étant donné qu'il constitue le critère de recherche que doit utiliser l'huissier de justice lors de la consultation de la liste. Dans l'arrêté royal, il faut mentionner clairement quelles données contient cette liste ou avec quelles données un lien est établi.

20. L'article 8 du projet permet aux huissiers de justice de consulter la liste et de réutiliser les informations qui y sont reprises afin d'exécuter leurs missions légales. Les missions légales d'un huissier de justice ne sont pas limitées à l'exécution de significations : voir les articles 519 et 520 du Code judiciaire. Vu le fait que seule la signification électronique offre les garanties nécessaires concernant la sécurité des informations et l'identité de la personne qui en prend connaissance, la consultation de la liste ne peut être autorisée qu'en vue de réaliser une signification électronique. Dans tous les autres cas, les mêmes objections que celles formulées aux points 11 à 14 de l'avis n° 47/2015 de la Commission s'appliquent par analogie.

21. L'article 8 du projet oblige (autorise) les huissiers de justice à consulter la liste des adresses à l'aide du numéro de Registre national. La Commission attire l'attention sur le fait que le Roi n'est plus compétent pour autoriser l'utilisation du numéro de Registre national, sauf après avis préalable du Comité sectoriel du Registre national[4]. Vu que sur la base de l'article 5, premier alinéa de la loi du 8 août 1983 *organisant un registre national des personnes physiques*, les huissiers de justice entrent en ligne de compte pour être autorisés par le Comité sectoriel du Registre national, cette mention doit être supprimée.

Chapitre IV. Registre central des actes authentiques dématérialisés des huissiers de justice

22. Le législateur a conféré au registre central la qualité de source authentique. Cela implique que les données qui y sont reprises doivent être de qualité. En vertu de l'article 9 du projet, ce registre ne reprendra pas uniquement les actes qui ont été signifiés par voie électronique mais également les actes "ordinaires" qui seront dématérialisés après leur signification.

[4] Article 8, § 1er, deuxième alinéa de la loi du 8 août 1983 *organisant un registre national des personnes physiques.*

23. Concernant ces derniers actes, la Commission constate toutefois que :

- il n'est mentionné nulle part qui est responsable de la dématérialisation des actes "ordinaires" ;
- il n'est indiqué nulle part quelles garanties ont été élaborées pour éviter que lors de la dématérialisation, des données soient manipulées ; la référence aux "techniques informatiques" est vide de sens ; les techniques informatiques ne sont pas par définition sûres ou de qualité ;
- aucune forme de contrôle de qualité n'est prévue ;
- la manière dont le destinataire d'une signification "ordinaire" est informé de l'enregistrement dans le registre central n'est pas régie, contrairement à la situation du destinataire d'une signification électronique.

24. L'article 10 du projet énumère les informations qui sont enregistrées dans le registre central. À la lumière de la finalité, seules les données qui sont adéquates, pertinentes et non excessives (article 4, § 1, 3° de la LVP) peuvent être traitées.

25. Le sixième tiret de l'article 10 mentionne le fait que le consentement a été refusé. La Commission renvoie à ses remarques relatives au consentement exprès informé qu'elle a formulées dans son examen du Chapitre I du projet. Il faut d'abord informer en détail la personne concernée, on peut ensuite lui demander son consentement et débuter par la suite le traitement de données lors de l'identification et de l'authentification. Ainsi, aucune information excessive n'est enregistrée.

26. Ce tiret indique que même en cas de refus du consentement, des données sont enregistrées. Cela est contraire tant à l'article 5, premier alinéa, a) de la LVP qu'à l'article 32, 6° du Code judiciaire.

27. Le destinataire a le droit de consulter les données qui ont été enregistrées lors de la signification électronique. Cela signifie qu'il pourra donc également voir qui est le donneur d'ordre. Il ressort du 11e tiret de l'article 10 qu'en ce qui concerne le donneur d'ordre, outre le nom et le prénom, le numéro de Registre national est également enregistré. La Commission attire l'attention sur le fait que ce numéro doit être masqué, vu qu'un destinataire n'est généralement pas autorisé à utiliser ce numéro (cette remarque vaut également pour les actes "ordinaires" qui sont dématérialisés après signification).

PAR CES MOTIFS,

la Commission,

émet un avis **défavorable**.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere