ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA190008		11 avril 2019

Objet : avis relatif à un projet d'arrêté royal relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée.

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, 1e 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 la demande d'avis du Ministre de la Justice du 11 février 2019, en vertu de la LPD susmentionnée.

Vu le rapport de Monsieur Koen Gorissen, membre-conseiller de l'Organe de contrôle.

Émet, le 11 avril 2019, l'avis 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 de contrôle. L'article 4, § 2, quatrième alinéa de la loi 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 et 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[4]) de la LPD[5]. 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[6].

---

[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 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] Certains traitements opérationnels peuvent en effet relever quand même du RGPD s'ils ne peuvent ne pas être considérés comme relevant de l'article 27 de la LPD : "*les traitements de données à caractère personnel effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces*". On peut ainsi penser à certaines constatations par la police à la demande du citoyen qui ne peuvent être considérées ni comme (un indice d'une) infraction, ni comme l'exercice des missions de police administrative. Un exemple classique : la constatation à la demande d'une des parties que le règlement relatif aux droits de garde et de visite n'est pas respecté par l'ex-partenaire. De tels constats sont parfois repris dans un procès-verbal, parfois uniquement dans une fiche de notification des banques de données de base.

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

[6] Article 236, § 2 de la LPD.

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[7].

II. Objet de la demande

5. La demande concerne un projet d'arrêté royal (ci-après "AR") relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée.

L'AR exécute l'article 40, § 3 de la LFP qui dispose ce qui suit : "*Art. 40 § 1er. Les plaintes et dénonciations faites aux membres du cadre opérationnel, de même que les renseignements qu'ils ont obtenus et les constatations qu'ils ont faites au sujet d'infractions, ainsi que les constations faites par les membres du cadre administratif et logistique visés à l'article 118 de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, lorsqu'ils sont habilités à dresser des procès-verbaux, font l'objet de procès-verbaux qui sont transmis à l'autorité judiciaire compétente.*

Les procès-verbaux sont établis sous forme matérialisée ou dématérialisée.

§ *2. Le procès-verbal dématérialisé est signé par le verbalisant à l'aide d'une signature électronique qualifiée.*

§ ***3. Par dérogation au § 2, un cachet électronique avancé est utilisé comme signature électronique :***

1° lorsque le verbalisant n'est légalement pas tenu de s'identifier nominativement dans le procès-verbal ;
2° pour les procès-verbaux relatifs aux constatations effectuées dans le cadre des articles 62 et 65, § 1er, de la loi du 16 mars 1968 relative à la police de la circulation routière ;
3° pour certaines catégories de procès-verbaux relatifs à des infractions déterminées qui, en fonction de la nature des faits et des circonstances de l'affaire, ne font pas ou pas encore l'objet de poursuites de la part du ministère public.

Le Collège des procureurs généraux détermine ces catégories dans une directive.

---

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

Les procès-verbaux signés à l'aide d'un cachet électronique avancé sont assimilés aux procès-verbaux signés à l'aide d'une signature manuscrite.

Le Roi fixe les mesures de sécurité et les normes techniques minimales auxquelles doivent répondre les systèmes informatiques policiers qui produisent le cachet électronique avancé, ainsi que les mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée. *..."*

III. Examen du projet

A. Généralités

6. Conformément à l'article 40, § 3 de la LFP, **le Roi fixe les mesures de sécurité et les normes techniques minimales** auxquelles doivent répondre les systèmes informatiques policiers qui produisent le cachet électronique avancé, **ainsi que les mentions** qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée.

En ce qui concerne les mesures de sécurité et les normes techniques, le Rapport au Roi dispose que celles-ci ne peuvent pas être rendues publiques au risque précisément de compromettre la sécurité des systèmes en question. On opte dès lors pour se référer uniquement à la réglementation européenne en vigueur (article 1, § 1) et d'indiquer en des termes généraux que la police fédérale dispose d'une telle liste de mesures de sécurité et de normes techniques. De facto, il revient donc aux ministres de tutelle compétents en charge de l'Intérieur et de la Justice (qui sont d'ailleurs responsables du traitement pour toutes les banques de données policières à l'exception des banques de données particulières) et à la police fédérale de fixer les mesures de sécurité et les normes techniques minimales, et non au Roi. L'Organe de contrôle est conscient du fait que des normes techniques sont par définition sujettes à modifications et que jusqu'à présent, en ce qui concerne le Règlement n° 910/2014[8] (Règlement eIDAS), aucun acte d'exécution n'a encore été adopté en ce qui concerne les normes en matière de cachets avancés[9]. Un AR est toutefois l'instrument par excellence pour intervenir dans un environnement qui change rapidement et il conviendrait d'envisager d'établir au moins un cadre général en matière de mesures de sécurité et le cas échéant de normes techniques (cf. ci-après, point 7).

Dans le projet d'arrêté royal, on utilise la notion de "signataire" (art. 2 et art. 5), tant dans le contexte de la signature électronique que de celui du cachet électronique. À l'article 3 (définitions) du règlement eIDAS, on fait une distinction entre les notions de "signataire" et de "créateur" :

- 9. "signataire" : une personne physique qui crée une signature électronique ;
- 24. "créateur de cachet" : une personne morale qui crée un cachet électronique.

---

[8] RÈGLEMENT (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.*

[9] Les actes d'exécution qui ont bel et bien déjà été adoptés concernent les listes de confiance (CID 2015/1505), les formats de référence des cachets électroniques avancés (CID 2015/1506) et les normes en matière d'évaluation de la sécurité de dispositifs qualifiés (CID 2016/650).

La notion de "signataire" est donc réservée à la désignation de la personne physique qui appose sa signature électronique. Le projet d'arrêté royal devrait donc soit utiliser les termes corrects tels que définis dans le règlement eIDAS, soit ajouter explicitement la définition de "signataire" afin de clarifier l'interprétation de cette notion.

B. Commentaire des articles

Article 1

7. L'article 1, § 1 dispose que les mesures de sécurité et les normes techniques *sont basées* sur le Règlement n° 910/2014, et en particulier son article 36. Le Rapport au Roi affirme ce qui suit à ce sujet : "*il va de soi que celui-ci doit servir pour réaliser les quatre éléments essentiels tels que visés à l'article 36 du règlement eIDAS* ...".

À l'article 3 de la LFP, on retrouve quelques définitions, dont celle de "signature électronique qualifiée" et de "*cachet électronique avancé*" :

... 8° signature électronique qualifiée : la signature visée à l'article 3.12 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

9° cachet électronique avancé : le cachet visé à l'article 3.26 du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Conformément à l'article 3 précité de la LFP, la signature électronique qualifiée et le cachet électronique avancé dont question à l'article 40, § 3 de la LFP doivent être compris au sens du Règlement n° 910/2014.

Il est dès lors recommandé de préciser explicitement à l'article 1 que le règlement eIDAS, dont l'article 36 de ce règlement eIDAS, s'applique intégralement aux mesures de sécurité et aux normes techniques, et non pas qu'elles "*sont basées*" sur celui-ci, ce qui laisse une marge d'interprétation (trop) large. Cette application intégrale est d'ailleurs confirmée dans le Rapport au Roi. On pourrait éventuellement proposer le texte suivant : "*Les mesures de sécurité et les normes techniques relatives à la production du cachet électronique avancé visé à l'article 40, § 3 de la loi du 5 août 1992 sur la fonction de police sont établies conformément et en tenant compte de ... :*"

8. Au § 2 de l'article 1, on dispose que la police fédérale dispose d'une liste de ces mesures et normes techniques. Il convient de prévoir ici que dès sa création, une telle liste doit être transmise d'initiative par la police fédérale à l'Organe de contrôle, afin que celui-ci puisse exécuter correctement sa mission de contrôle, définie au § 3 (on mentionne par erreur le § 2 dans le projet d'arrêté royal). On peut enfin se référer ici au point 6 pour reprendre au moins le cadre général des mesures de sécurité dans le projet d'arrêté royal.

9. Le § 2 qui suit (qui doit donc être le § 3) de l'article 1 du projet d'arrêté royal prévoit enfin une mission contrôle spécifique pour l'Organe de contrôle, ce dernier devrait en effet vérifier si *ces mesures et normes sont adéquates et correctement mises en œuvre*.

Il revient bien entendu en premier lieu au responsable du traitement de veiller à utiliser des mesures de sécurité et des normes techniques appropriées et adéquates et à les mettre en œuvre correctement. Conformément au nouveau cadre de protection des données, le responsable du traitement doit aussi pouvoir démontrer cela à l'Organe de contrôle et non l'inverse : en d'autres termes, ce n'est pas à l'Organe de contrôle de prouver leur caractère inadéquat. L'Organe de contrôle n'est en effet pas l'organe compétent pour déterminer les normes techniques de hardware et de programmes système, donc les *moyens* pour la création d'un cachet électronique avancé, mais peut cependant vérifier a posteriori si les mesures de sécurité pour l'ensemble de l' "environnement" sont adéquates et sont respectées (c'est-à-dire les applications par lesquelles les cachets sont apposés et validés, les systèmes de gestion des accès ainsi que tous les processus de gestion y afférents). Vu les éléments qui précèdent, l'Organe de contrôle demande de limiter sa mission de contrôle aux seules mesures de sécurité, alors que les normes techniques relatives aux moyens de création de cachets électroniques avancés peuvent être auditées par des laboratoires spécialisés à cet effet.

Article 5

10. L'article 5 énonce les mentions que comportent le cachet électronique avancé et la signature électronique qualifiée aussi bien dans un environnement matérialisé que dématérialisé. On prévoit en outre la possibilité de protéger l'identité du signataire dans certains cas par l'utilisation d'un numéro unique[10].

À cet égard, il convient de remarquer qu'en cas d'utilisation d'une signature électronique qualifiée, l'identité des signataires est toujours liée intrinsèquement à la signature numérique. Par exemple en cas d'utilisation de l'eID, cette identité se trouve en effet dans le certificat de l'eID, dont le contenu ne peut pas être modifié. Cette identité peut être masquée lors de la matérialisation ou de l'impression, mais pour le PV doté du cachet *numérique*, le certificat provenant de la carte eID sera toujours nécessaire pour pouvoir valider la signature électronique. Il est recommandé d'en tenir compte si l'on souhaite protéger ou masquer l'identité du verbalisant. Le cas échéant, on peut penser à faire apposer un cachet sur les PV par un délégué habilité du service concerné et non par le verbalisant.

---

[10] Soit le numéro visé à l'article 41, § 2 de la LFP, soit le numéro visé à l'article 112quater du Code d'instruction criminelle.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière,
prie le demandeur de tenir compte des remarques susmentionnées ;
demande de donner suite aux recommandations formulées aux points 6-10.

Avis approuvé par l'Organe de contrôle de l'information policière le 11 avril 2019.

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