



CONSEIL D'ÉTAT
section de législation

RAAD VAN STATE
afdeling Wetgeving

avis 66.584/2
du 14 octobre 2019

advies 66.584/2
van 14 oktober 2019

sur

over

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'

een ontwerp van koninklijk
besluit 'inzake de
veiligheidsmaatregelen en de
minimale technische normen
voor
politie-informaticasystemen
die het geavanceerd
elektronisch zegel produceren
en inzake de vermeldingen die
voorkomen in het geavanceerd
elektronisch zegel en in de
gekwalficeerde elektronische
handtekening'

Le 13 septembre 2019, le Conseil d'État, section de législation, a été invité par le Vice-Premier Ministre et Ministre de la Justice, chargé de la Régie des bâtiments à communiquer un avis, dans un délai de trente jours, sur 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'.

Le projet a été examiné par la deuxième chambre le 14 octobre 2019. La chambre était composée de Pierre VANDERNOOT, président de chambre, Patrick RONVAUX et Christine HOREVOETS, conseillers d'État, et Béatrice DRAPIER, greffier.

Le rapport a été présenté par Véronique SCHMITZ, auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre VANDERNOOT.

L'avis, dont le texte suit, a été donné le 14 octobre 2019.

*

Op 13 september 2019 is de Raad van State, afdeling Wetgeving, door de Vice-Eerste Minister en Minister van Justitie, belast met de Regie der gebouwen verzocht binnen een termijn van dertig dagen een advies te verstrekken over een ontwerp van koninklijk besluit 'inzake de veiligheidsmaatregelen en de minimale technische normen voor politie-informaticasystemen die het geavanceerd elektronisch zegel produceren en inzake de vermeldingen die voorkomen in het geavanceerd elektronisch zegel en in de gekwalificeerde elektronische handtekening'.

Het ontwerp is door de tweede kamer onderzocht op 14 oktober 2019. De kamer was samengesteld uit Pierre VANDERNOOT, kamervoorzitter, Patrick RONVAUX en Christine HOREVOETS, staatsraden, en Béatrice DRAPIER, griffier.

Het verslag is uitgebracht door Véronique SCHMITZ, auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre VANDERNOOT.

Het advies, waarvan de tekst hierna volgt, is gegeven op 14 oktober 2019.

*

Compte tenu du moment où le présent avis est donné, le Conseil d'État attire l'attention sur le fait qu'en raison de la démission du Gouvernement, la compétence de celui-ci se trouve limitée à l'expédition des affaires courantes. Le présent avis est toutefois donné sans qu'il soit examiné si le projet relève bien de la compétence ainsi limitée, la section de législation n'ayant pas connaissance de l'ensemble des éléments de fait que le Gouvernement peut prendre en considération lorsqu'il doit apprécier la nécessité d'arrêter ou de modifier des dispositions réglementaires.

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique du projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, le projet appelle les observations suivantes.

FORMALITÉS PRÉALABLES

1. Interrogée sur la question de savoir si le texte en projet a été notifié à la Commission européenne, la fonctionnaire déléguée a indiqué que ce n'était pas le cas.

Eu égard à la circonstance qu'il s'agit en l'espèce de mesures de sécurité et de normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et des mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée¹, il revient à l'auteur du texte de notifier celui-ci à la Commission européenne en application de la directive (UE) n° 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 'prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société d'information'.

2.1. L'avis n° 190008 de l'Organe de contrôle de l'information policière (ci-après : « le COC ») a été donné le 11 avril 2019 sur le projet soumis au Conseil d'État.

Cet avis a été communiqué à la section de législation en néerlandais.

¹ Pour rappel, le règlement (UE) n° 910/2014 du Parlement 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' (règlement eIDAS) opère une distinction entre trois types de signature électronique en fonction du niveau de garantie (la signature électronique, la signature électronique avancée et la signature électronique qualifiée, définies par l'article 3, paragraphes 10, 11 et 12, de ce règlement) ; voir aussi les modalités figurant dans la section 4 du chapitre III du règlement, les niveaux les plus sophistiqués constituant un sous-ensemble des niveaux inférieurs. La signature électronique étant réservée, selon le règlement, aux personnes physiques, il est fait référence, le cas échéant, à la notion de cachet électronique pour les personnes morales : voir les définitions inscrites à l'article 3, paragraphes 25, 26 et 27, et les modalités figurant dans la section 5 du chapitre III du même règlement (UE) n° 910/2014.

Dans son avis n° 65.312/2 donné le 4 mars 2019 sur un avant-projet de loi 'relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux', la section de législation a observé qu'il ne se conçoit pas que pareil avis ne soit pas émis tant en néerlandais qu'en français ².

La même critique vaut en l'espèce.

2.2. Comme dans cet avis, la section de législation regrette que le texte soumis au Conseil d'État ne constitue pas une version définitive du projet dans la mesure où celui-ci n'a pas été modifié à la suite de l'avis du COC ou à tout le moins que celui-ci n'est pas pris en compte dans le rapport au Roi.

3. L'alinéa 5 du préambule sera complété car l'Inspection des Finances a rendu un avis sur le texte en projet le 19 avril 2019 mais aussi le 20 avril 2019.

EXAMEN DU PROJET

1.1. Le texte en projet est proposé par le Ministre de la Justice. En raison notamment des articles 1^{er}, § 2, et 4 du projet, il serait utile qu'il soit également proposé et contresigné par le Ministre de l'Intérieur.

1.2. En outre, le projet ne contient pas d'article d'exécution.

Il y a lieu de le compléter par un nouvel article final qui aura cet objet et qui chargera les deux ministres de celle-ci ³.

2. L'arrêté royal en projet trouve son unique fondement juridique dans l'article 40, § 3, alinéa 4, de la loi du 5 août 1992 'sur la fonction de police', tel qu'il a été remplacé par l'article 60 de la loi du 25 mai 2018 'visant à réduire et redistribuer la charge de travail au sein de l'ordre judiciaire' ⁴.

Le premier alinéa du préambule sera rédigé en ce sens et ce, sous la forme d'un visa.

3. Le règlement (UE) n° 910/2014 du Parlement 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' (ci-après : « le règlement eIDAS ») et la loi du 21 juillet 2016 'mettant en œuvre et complétant le

² <http://www.raadvst-consetat.be/dbx/avis/65312.pdf>.

³ *Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet « Technique législative », recommandations n°s 162 à 168, 175 et 176.

⁴ Cette disposition légale a fait l'objet de l'amendement n° 55. Voir *Doc. parl.*, Chambre, 2017-2018, n° 2827/004, pp. 73 à 85 ; n° 2827/006, p. 41 ; n° 2827/007, pp. 23 et 24 ; n° 2827/009, p. 16 ; n° 2827/10, pp. 19 et 20 ; n° 2827/011, pp. 18 et 19.

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, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique' font partie du cadre juridique du texte en projet.

Les considérants qui forment les alinéas 2 et 3 du préambule seront modifiés afin de reprendre les intitulés complets et exacts du règlement et de la loi précitée. Ils seront en outre placés après les visas.

Les intitulés complets et exacts du règlement et de la loi précitée seront également mentionnés dans le dispositif en projet et le rapport au Roi.

4.1. Sur le fond, au regard de l'article 40, § 3, alinéa 4, de la loi du 5 août 1992, qui constitue le fondement juridique du projet, et du cadre juridique en cause, tel qu'il résulte notamment du droit européen, il y a lieu d'observer ce qui suit.

4.2. L'article 40, § 3, alinéa 4, de la loi du 5 août 1992 contient l'habilitation suivante :

« 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 ».

4.3. L'article 1^{er}, § 1^{er}, a pour seul objet de rappeler les règles supérieures applicables en la matière.

Un tel rappel figurera dans le rapport au Roi.

4.4. L'article 1^{er}, § 2, du projet prévoit que la police fédérale « dispose d'une liste de ces mesures et normes techniques appliquées au processus de signature par cachet électronique avancé » (alinéa 1^{er}) et qu'« en cas de sous-traitance, ces mesures et normes sont contractuellement applicables au sous-traitant » (alinéa 2).

L'article 2 du projet est rédigé de la manière suivante :

« Les systèmes informatiques policiers qui produisent le cachet électronique avancé répondent aux mesures de sécurité et aux normes techniques permettant :

1° d'en identifier les utilisateurs et d'en vérifier et gérer leurs fonctions et leurs mandats ;

2° préalablement à la signature par cachet électronique avancé, d'authentifier à l'aide d'un système d'authentification forte, le signataire ;

3° d'établir la date et le moment précis d'utilisation du cachet électronique avancé ;

4° d'établir des fichiers de journalisation au sens de l'article 56 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des données à caractère personnel ».

Dans le rapport au Roi, on peut lire ce qui suit dans le commentaire relatif à l'article 1^{er} :

« Comme nous l'avons indiqué dans l'introduction, le recours au cachet avancé par la police fédérale implique la tenue d'une documentation reprenant les mesures et norme techniques concrètes appliquées à son processus de signature par cachet électronique. Cette documentation sera effectuée de concert entre la direction générale de la gestion des ressources et de l'information, qui est chargée de la préparation des normes techniques et des règles de gestion des systèmes d'information et de communication de la police intégrée (article 6, 3°, b), de l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale) et le Commissariat général de la police fédérale qui est chargé de la détermination de normes et d'une approche standardisée en matière de sécurité de l'information (article 2, e), du même [arrêté royal]). Ces normes techniques se basent d'une part sur les standards généraux de sécurité des systèmes de la police intégrée et d'autre part sur les standards spécifiques d'application en matière de cachet électronique avancé dont bien entendu ceux découlant du Règlement européen eIDAS, et en particulier son article 36. Si comme nous l'avons déjà mentionné, il n'est ni justifié ni opportun de détailler cette liste, il va de soi qu'elle devra servir à opérationnaliser les 4 éléments indispensables visés à l'article 36 du Règlement européen eIDAS et relatifs au cachet électronique avancé [...] ».

L'introduction générale du rapport au Roi précise ce qui suit, en ce qui concerne l'article 2 du projet :

« Il ne pourrait néanmoins pas être question d'uniquement référer à un ensemble de processus et de procédures géré par la police fédérale. C'est pourquoi l'article 2 indique en termes génériques les exigences techniques minimales relatives aux systèmes informatiques policiers qui produisent le cachet électronique avancé. Celles-ci constituent dès lors le socle commun entourant la production et l'utilisation du cachet électronique avancé dans le cadre de la signature des procès-verbaux précisée à l'article 40, § 2, 1° à 3° de la loi sur la fonction de police ».

Dans son avis n° 190008 du 11 avril 2019, le COC relevait ce qui suit (point 6) :

« *De facto* komt het dus aan de bevoegde voogdijministers van Binnenlandse Zaken en Justitie (die overigens verwerkingsverantwoordelijke zijn voor alle politionele databanken behoudens de bijzondere gegevensbanken) en de federale politie toe om de veiligheidsmaatregelen en minimale technische normen te bepalen, en niet aan de Koning. Het Controleorgaan is zich ervan bewust dat technische normen per definitie veranderlijk zijn, en er tot op heden met betrekking tot de Verordening nr. 910/2014 (eIDAS Verordening) nog geen uitvoeringshandeling met betrekking tot normen inzake geavanceerde zegels werd vastgesteld. Een KB is evenwel het instrument bij uitstek om op een snel veranderende omgeving in te spelen, en men zou derhalve dienen te overwegen om minstens een algemeen kader inzake veiligheidsmaatregelen en desgevallend technische normen te bepalen (cfr. *Infra*, onder randnummer 7) ».

Le projet n'exécute pas le fondement juridique invoqué mais se contente soit de renvoyer à des règles supérieures, soit d'énoncer certaines règles vagues⁵ applicables aux systèmes informatiques policiers qui produisent le cachet électronique (article 2 du projet) tout en laissant la possibilité que d'autres règles soient fixées non par le Roi mais au sein de la police (article 1^{er}, § 2, du projet).

Non seulement un tel système est opaque quant à l'ensemble des mesures de sécurité et des normes techniques qui seront réellement imposées en matière de signature par cachet électronique avancé mais, plus fondamentalement, il n'apparaît pas que le législateur ait voulu opérer une telle distinction entre les pouvoirs conférés au Roi et ceux accordés à la police puisque c'est le Roi qu'il a chargé de fixer l'ensemble des règles minimales applicables (article 40, § 3, alinéa 4, de la loi du 5 août 1992).

4.5. Malgré les explications contenues dans le rapport au Roi et sous réserve du caractère technique de la matière, il ne ressort pas non plus clairement du dispositif en projet et en particulier de la combinaison des articles 1^{er}, § 2, et 2 du projet que celui-ci peut être considéré comme assurant sa conformité aux quatre conditions requises par l'article 36 du règlement eIDAS, rédigé comme suit :

« Un cachet électronique avancé satisfait aux exigences suivantes:

- a) être lié au créateur du cachet de manière univoque ;
- b) permettre d'identifier le créateur du cachet ;
- c) avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique ; et
- d) être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable ».

4.6. On peut regretter l'utilisation, dans le projet, d'une terminologie différente de celle définie à l'article 3 du règlement eIDAS.

L'article 36 de ce règlement impose des conditions liées au « créateur du cachet » tel que défini à l'article 3, point 24, de celui-ci comme étant « la personne morale qui crée un cachet électronique ». La « partie utilisatrice » est définie par l'article 3, point 6, du règlement eIDAS comme étant « une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance » tandis que le « signataire » est défini par l'article 3, point 9, du règlement eIDAS comme « une personne physique qui crée une signature électronique ».

Or l'article 2 du projet emploie le terme « utilisateurs » (1°) ou « signataire » (2°) alors qu'il s'agit de désigner « le créateur du cachet », qui, par hypothèse, ne peut être qu'une personne morale au sens du règlement.

⁵ L'article 2, 1°, dispose ainsi que les systèmes informatiques policiers devront prévoir des mesures de sécurité et des normes techniques qui permettront de « gérer (les) fonctions et les mandats » des utilisateurs. De même, le 2° du même article prévoit l'authentification du signataire « à l'aide d'un système d'authentification forte », sans préciser ce que ces notions recouvrent.

À cet égard, la justification de l'amendement à l'origine de l'article 60 de la loi du 25 mai 2018, qui a remplacé l'article 40 de la loi du 5 août 1992, a précisé ce qui suit :

« Il y a cependant des hypothèses où il n'est pas opportun d'identifier (40, § 3, 1^o) ou d'authentifier (40, § 3, 2^o et 3^o) de manière individuelle le verbalisant.

Dans les trois cas de figure mentionnés ci-dessous un autre standard est établi en matière de signature électronique à savoir le recours au cachet électronique avancé.

Il s'agit bien entendu aussi dans ces trois hypothèses d'apporter des garanties au niveau de l'authentification de l'auteur du procès-verbal et de la non-répudiation du contenu du procès-verbal. La différence fondamentale avec la signature électronique (qualifiée) est que dans ces hypothèses, ces garanties ne seront pas apportées au nom d'une personne (l'authentification ne porte pas sur verbalisant, même s'il peut être identifié dans le procès-verbal) mais au nom d'une personne morale (la police fédérale ou les zones de police mono ou pluricommunales).

[...]

Dans les trois cas identifiés au § 3 de l'article 40, la norme établie en matière de signature digitale est dès lors celle liée au cachet électronique avancé au sens de l'article 36 du Règlement européen eIDAS. Cet article précise les exigences liées au cachet électronique.

[...]

Le Règlement eIDAS prévoit que le cachet électronique est réservé aux personnes morales. Ce cachet permet en effet d'établir le lien entre les données électroniques cachetées et une personne morale. Une personne morale est une entité dotée de la personnalité juridique »⁶.

Il résulte de ce qui précède qu'en ce qu'il emploie des termes qui sont liés non pas au cachet électronique avancé mais à la signature électronique qualifiée, l'article 2 du projet est source de confusion et doit également être revu sur ce point.

Il y a lieu de conclure que l'article 1^{er}, §§ 1 et 2, ainsi que l'article 2 doivent être fondamentalement revus. Par voie de conséquence, l'article 4 du projet sera également revu⁷.

4.7. L'article 1^{er}, § 3, charge l'Organe de contrôle de l'information policière de vérifier si « ces mesures et normes sont adéquates et correctement mises en œuvre ».

De deux choses l'une : soit cette mission fait partie des missions limitativement énumérées à l'article 71, § 1^{er}, alinéa 3, 1^o et 2^o, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' et dans ce cas le texte en projet n'a pas à rappeler cette mission, soit il s'agit d'une nouvelle mission

⁶ *Doc. parl.* Chambre, 2017-2018, n° 54-2827/004, pp. 78, 80 et 82.

⁷ L'article 4 du projet est relatif à la conservation, par la police fédérale, des normes « visées aux articles 1^{er} et 2 ». Le segment de phrase qui précise que cette conservation doit se dérouler dans un environnement sécurisé selon « les règles de l'art » n'est pas non plus suffisamment précis et il appartient à l'auteur du texte de définir ce qu'il entend par « règles de l'art » en indiquant quelles normes de conservation il entend respecter.

et il y a lieu d'appliquer l'article 71, § 1^{er}, alinéa 3, 3°, de la loi, ce qui implique que l'ajout d'une autre mission au COC doit être « organisée par ou en vertu d'autres lois »⁸.

En l'espèce, il faut sans doute apporter une nuance et distinguer deux aspects dans la nouvelle mission telle qu'elle est envisagée par l'article 1^{er}, § 3, du projet : le premier, le fait de concevoir et donc de pouvoir vérifier le caractère adéquat des mesures techniques et des normes minimales au moment de leur création, relevant de l'article 71, § 1^{er}, alinéa 3, 3°, de la loi, et le second, le fait de vérifier la correcte application de celles-ci lors de leur mise en œuvre, relevant de l'article 71, § 1^{er}, alinéa 3, 1°, de la loi⁹.

En conclusion, l'attribution au COC d'une nouvelle mission ne peut se faire par arrêté royal mais doit faire l'objet d'une initiative législative pour l'aspect qui n'est pas encore couvert dans ses missions légales actuelles telles que déterminées par l'article 71 de la loi du 30 juillet 2018.

Par conséquent, l'article 1^{er}, § 3, du projet doit être omis.

4.8. Concernant l'article 5, il y a lieu d'observer ce qui suit, dans la ligne des considérations suivantes émises au point 10 de l'avis n° 190008 du COC :

« Artikel 5 bepaalt de vermeldingen die het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening bevatten zowel in een gematerialiseerde als in een gedematerialiseerde omgeving. Tevens wordt de mogelijkheid voorzien om de identiteit van de ondertekenaar in bepaalde gevallen te beschermen door het gebruik van een uniek nummer.

Hierbij dient opgemerkt dat bij gebruik van een gekwalificeerde elektronische handtekening, de identiteit van de ondertekenaars steeds inherent verbonden is aan de digitale handtekening. Bijvoorbeeld in het geval van het gebruik van de e-ID, staat deze identiteit namelijk in het certificaat van de e-ID, waarvan de inhoud niet kan worden gewijzigd. Deze identiteit kan worden verborgen bij het materialiseren of afdrukken, maar aan het digitale verzegelde pv zal steeds het certificaat afkomstig van de e-ID kaart nodig zijn om de elektronische handtekening te kunnen valideren. Het verdient aanbeveling om hiermee rekening te houden indien men de identiteit van de verbalisant wenst te

⁸ L'article 71 est rédigé de la manière suivante :

« § 1^{er}. Il est créé auprès de la Chambre des représentants une autorité de contrôle indépendante de l'information policière, dénommé Organe de contrôle de l'information policière.

Elle succède à l'Organe de contrôle de l'information policière institué par l'article 36ter, § 1^{er}, alinéa 1^{er}, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Elle est, vis-à-vis des autorités compétentes visées à l'article 26, § 1^{er}, 7°, a), d) et f), chargée de :

1° surveiller l'application du présent titre, comme prévu à l'article 26, 15° ;

2° contrôler le traitement des informations et des données à caractère personnel visées aux articles 44/1 à 44/11/13 de la loi du 5 août 1992 sur la fonction de police y compris celles incluses dans les banques de données visées à l'article 44/2 de la même loi ;

3° toute autre mission organisée par ou en vertu d'autres lois.

Elle est également, vis-à-vis de l'autorité compétente visée à l'article 26, § 1^{er}, 7°, e), chargée de surveiller l'application de l'article 281, § 4, de la loi générale sur les douanes et accises du 18 juillet 1977.

§ 2. Le siège de l'Organe de contrôle de l'information policière est établi dans l'arrondissement administratif de Bruxelles-Capitale.

Dans l'exercice de ses missions et des pouvoirs dont elle est investie conformément à la présente loi et d'autres lois, l'Organe de contrôle de l'information policière agit en toute indépendance ».

⁹ Voir l'avis de l'Inspecteur général des Finances du 19 avril 2019, point 2.2 et l'avis n° 190008 du COC du 11 avril 2019, point 9.

beschermen of af te schermen. In voorkomend geval kan worden gedacht om de pv's te laten verzegelen door een gemachtigde afgevaardigde van de betrokken dienst, zij het niet de verbalisant ».

Il ressort en effet de l'article 26 du règlement eIDAS qu'

« [u]ne signature électronique avancée satisfait aux exigences suivantes :

- a) être liée au signataire de manière univoque ;
- b) permettre d'identifier le signataire ;
- c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et
- d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ».

Tout comme dans l'observation formulée à propos de l'article 2 du projet, il est relevé en outre que l'auteur du projet emploie une terminologie qui n'est pas conforme à celle employée par le règlement eIDAS. En effet, l'article 5, § 2, 1^o, et § 3, du projet emploie indistinctement le terme « signataire » ou « verbalisateur » (article 5, § 1^{er}, 2^o, du projet), y compris dans l'hypothèse du cachet électronique avancé.

Enfin, l'article 5, § 3, du projet prévoit que, dans l'hypothèse visée à l'article 40, § 3, 1^o, de la loi du 5 août 1992, le cachet électronique avancé et la signature électronique qualifiée des procès-verbaux comportent un numéro unique attribué au signataire et qui protège son identité réelle. Or, comme il est indiqué dans l'observation relative à l'article 2 du projet, l'article 40, § 3, 1^o, de la loi du 5 août 1992 ne vise que l'hypothèse du cachet électronique avancé, ce que confirment également les travaux préparatoires cités.

L'article 5 du projet sera revu en conséquence.

5. En conclusion, le texte doit être fondamentalement revu afin d'être conforme à son cadre juridique et de mettre en œuvre correctement son fondement juridique.

De ce point de vue, l'attention de l'auteur du projet est plus spécialement attirée sur le fait que le dispositif se contente de procéder par renvoi à des règles supérieures ou se limite à l'énonciation d'objectifs à atteindre par les mesures de sécurité, alors qu'il appartient au Roi, conformément à l'article 40, § 3, alinéa 4, de la loi du 5 août 1992, de fixer Lui-même « les mesures de sécurité [...] minimales auxquelles doivent répondre les systèmes informatiques policiers qui produisent le cachet électronique avancé ». Le projet est même muet quant à la fixation, pourtant requise par cette habilitation, des « normes techniques minimales » en la matière.

*

Rekening houdend met het tijdstip waarop dit advies gegeven wordt, vestigt de Raad van State de aandacht op het feit dat, wegens het ontslag van de regering, de bevoegdheid van deze laatste beperkt is tot het afhandelen van de lopende zaken. Dit advies wordt evenwel gegeven zonder dat wordt nagegaan of het ontwerp onder die beperkte bevoegdheid valt, aangezien de afdeling Wetgeving geen kennis heeft van alle feitelijke gegevens die de regering in aanmerking kan nemen als zij moet beoordelen of het nodig is een verordening vast te stellen of te wijzigen.

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, §1, eerste lid, 2°, van de wetten ‘op de Raad van State’, gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, §3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het ontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het ontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE VORMVEREISTEN

1. De gemachtigde ambtenaar heeft ontkennend geantwoord op de vraag of de ontworpen tekst ter kennis is gebracht van de Europese Commissie.

Aangezien het *in casu* gaat om veiligheidsmaatregelen en minimale technische normen voor politie-informaticasystemen die het geavanceerde elektronische zegel produceren en om de vermeldingen die voorkomen in het geavanceerde elektronische zegel en in de gekwalificeerde elektronische handtekening,¹ dient de steller van het ontwerp de Europese Commissie kennis te geven van de tekst, met toepassing van richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 ‘betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij’.

2.1. Over het ontwerp dat aan de Raad van State is voorgelegd, heeft het Controleorgaan op de politionele informatie (hierna: “het COC”) op 11 april 2019 advies 190008 uitgebracht.

Dat advies is aan de afdeling Wetgeving overgezonden in het Nederlands.

¹ Er wordt aan herinnerd dat verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 ‘betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG’ (eIDAS-verordening) drie soorten elektronische handtekening onderscheidt naargelang het betrouwbaarheidsniveau (de elektronische handtekening, de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening, gedefinieerd in artikel 3, leden 10, 11 en 12, van die verordening); zie ook de regels vervat in afdeling 4 van hoofdstuk III van de verordening: de meest gesofisticeerde niveaus vormen een deelverzameling van de lagere niveaus. Daar de elektronische handtekening volgens de verordening alleen voor natuurlijke personen geldt, wordt voor rechtspersonen in voorkomend geval verwezen naar het begrip “elektronisch zegel”: zie de definities vervat in artikel 3, leden 25, 26 en 27, alsook de regels vervat in afdeling 5 van hoofdstuk III van dezelfde verordening (EU) 910/2014.

In haar advies 65.312/2, op 4 maart 2019 gegeven over een voorontwerp van wet ‘betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt en de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus’ heeft de afdeling Wetgeving opgemerkt dat het ondenkbaar is dat een dergelijk advies niet zowel in het Nederlands als in het Frans zou worden uitgebracht.²

Dezelfde kritiek kan ook *in casu* worden geformuleerd.

2.2. Net als in dat advies betreurt de afdeling Wetgeving dat de tekst die aan de Raad van State is voorgelegd, geen definitieve versie van het ontwerp is, in zoverre hij niet gewijzigd is naar aanleiding van het advies van de COC, of in zoverre niet op zijn minst met dat advies rekening is gehouden in het verslag aan de Koning.

3. Het vijfde lid van de aanhef moet worden aangevuld, aangezien de inspectie van Financiën niet alleen op 19 april 2019, maar ook op 20 april 2019 van advies heeft gediend over de ontworpen tekst.

ONDERZOEK VAN HET ONTWERP

1.1. De ontworpen tekst wordt voorgedragen door de minister van Justitie. Het zou, met name vanwege de artikelen 1, §2, en 4 van het ontwerp, nuttig zijn dat hij ook door de minister van Binnenlandse Zaken wordt voorgedragen en medeondertekend.

1.2. Voorts bevat het ontwerp geen uitvoeringsbepaling.

Het ontwerp dient te worden aangevuld met een nieuw slotartikel dat dienstdoet als uitvoeringsbepaling en waarin beide ministers met de uitvoering van het ontwerp worden belast.³

2. Het ontworpen koninklijk besluit ontleent zijn enige rechtsgrond aan artikel 40, §3, vierde lid, van de wet van 5 augustus 1992 ‘op het politieambt’, zoals het is vervangen bij artikel 60 van de wet van 25 mei 2018 ‘tot vermindering en herverdeling van de werklust binnen de rechterlijke orde’.⁴

Het eerste lid van de aanhef moet in die zin worden geredigeerd, en wel in de vorm van een aanhefverwijzing beginnende met de woorden “Gelet op”.

3. Tot het juridische kader van de ontwerpstekst behoren verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 ‘betreffende elektronische identificatie

² <http://www.raadvst-consetat.be/dbx/adviezen/65312.pdf>.

³ *Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbevelingen 162 tot 168, 175 en 176.

⁴ Die wettelijke bepaling heeft het voorwerp uitgemaakt van amendement 55. Zie *Parl.St.* Kamer 2017-18, 2827/004, 73-85; 2827/006, 41; 2827/007, 23-24; 2827/009, 16; 2827/10, 19-20; 2827/011, 18-19.

en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG' (hierna: "de eIDAS-verordening") en de wet van 21 juli 2016 'tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhabingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht'.

De overwegingen die het tweede en derde lid van de aanhef vormen, moeten worden gewijzigd zodat ze de verordening en de voornoemde wet met hun volledige en correcte opschrift weergeven. Bovendien moeten ze na de aanhefverwijzingen worden geplaatst.

Ook in het ontworpen dispositief en in het verslag aan de Koning moet het volledige en correcte opschrift van de verordening en van de voornoemde wet worden vermeld.

4.1. Op inhoudelijk vlak dienen over artikel 40, §3, vierde lid, van de wet van 5 augustus 1992, die de rechtsgrond van het ontwerp vormt, en over het betreffende juridische kader zoals dat met name uit het Europees recht voortvloeit, de volgende opmerkingen te worden gemaakt.

4.2. Artikel 40, §3, vierde lid, van de wet van 5 augustus 1992 bevat de volgende machtiging:

"De Koning bepaalt de veiligheidsmaatregelen en de minimale technische normen waaraan politie-informaticasystemen moeten voldoen die het geavanceerd elektronisch zegel produceren, evenals de vermeldingen die voorkomen in het geavanceerd elektronisch zegel en in de gekwalificeerde elektronische handtekening".

4.3. Artikel 1, §1, doet niets anders dan de ter zake geldende hogere rechtsregels in herinnering brengen.

Een dergelijke memorering hoort thuis in het verslag aan de Koning.

4.4. In artikel 1, §2, van het ontwerp wordt bepaald dat de federale politie "beschikt over een lijst van die maatregelen en technische normen die worden toegepast op het proces van ondertekening met behulp van het geavanceerd elektronisch zegel" (eerste lid) en dat "[i]n geval van onderaanneming (...) die maatregelen en normen contractueel toepasselijk [zijn] op de onderaannemer" (tweede lid).

Artikel 2 van het ontwerp luidt als volgt:

"De politie-informaticasystemen die het geavanceerd elektronisch zegel produceren, beantwoorden aan de veiligheidsmaatregelen en aan de technische normen die de mogelijkheid bieden

1° de gebruikers ervan te identificeren en hun functies en hun mandaten te controleren en te beheren;

2° voorafgaand aan de ondertekening met behulp van het geavanceerd elektronisch zegel de ondertekenaar met behulp van een systeem van sterke authenticatie te authenticeren;

3° de datum en het precieze tijdstip van gebruik van het geavanceerd elektronisch zegel vast te stellen;

4° logbestanden in de zin van artikel 56 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens bij te houden”.

In het verslag aan de Koning staat in de commentaar betreffende artikel 1 het volgende te lezen:

“Zoals ik in de inleiding heb aangegeven, brengt het gebruik van het geavanceerde zegel door de federale politie het bijhouden van gegevens met zich mee waarbij de concrete maatregelen en technische normen worden overgenomen die van toepassing zijn op de procedure voor ondertekening door middel van het elektronische zegel. Het bijhouden van deze gegevens gebeurt in samenwerking door de Algemene directie van het middelenbeheer en de informatie, die belast is met het voorbereiden van de technische normen en de regels voor het beheer van de informatie- en communicatiesystemen van de geïntegreerde politie (artikel 6, 3°, b), van het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie) en het Commissariaat-generaal van de federale politie, dat belast is met het vaststellen van normen en een standaardbenadering op het gebied van informatieveiligheid (artikel 2, e) van datzelfde KB). De technische normen zijn enerzijds gebaseerd op de algemene veiligheidsstandaarden voor de systemen van de geïntegreerde politie en anderzijds op de specifieke standaarden voor toepassing op het gebied van het geavanceerde elektronische zegel, waaronder uiteraard de standaarden die volgen uit de Europese eIDAS-verordening, in het bijzonder artikel 36 daarvan. Ofschoon het, zoals reeds genoemd, gerechtvaardigd noch passend is om deze lijst uitvoerig te beschrijven, spreekt het vanzelf dat deze moet dienen om de vier noodzakelijke elementen te realiseren zoals bedoeld in artikel 36 van de Europese eIDAS-verordening, die betrekking hebben op het geavanceerde elektronische zegel (...)”.

In de algemene inleiding van het verslag aan de Koning wordt in verband met artikel 2 van het ontwerp het volgende gesteld:

“Er zou echter niet uitsluitend verwezen moeten worden naar een geheel van processen en procedures geleid door de federale politie. Om die reden wordt in artikel 2 in algemene bewoordingen aangegeven wat de minimale technische eisen zijn die worden gesteld aan de informaticasystemen van de politie die het geavanceerde elektronische zegel produceren. Dientengevolge vormen deze de gemeenschappelijke basis voor het produceren en gebruiken van het geavanceerde elektronische zegel in het kader van het ondertekenen van processen-verbaal zoals weergegeven in artikel 40, §2,10 t/m 3° van de wet op het politieambt”.

Het COC heeft in punt 6 van zijn advies 190008 van 11 april 2019 het volgende opgemerkt:

“De facto komt het dus aan de bevoegde voogdijministers van Binnenlandse Zaken en Justitie (die overigens verwerkingsverantwoordelijke zijn voor alle politionele databanken behoudens de bijzondere gegevensbanken) en de federale politie toe om de veiligheidsmaatregelen en minimale technische normen te bepalen, en niet aan de Koning.

Het Controleorgaan is zich ervan bewust dat technische normen per definitie veranderlijk zijn, en er tot op heden met betrekking tot de Verordening nr. 910/2014 (eIDAS Verordening) nog geen uitvoeringshandeling met betrekking tot normen inzake geavanceerde zegels werd vastgesteld. Een KB is evenwel het instrument bij uitstek om op een snel veranderende omgeving in te spelen, en men zou derhalve dienen te overwegen om minstens een algemeen kader inzake veiligheidsmaatregelen en desgevallend technische normen te bepalen (cfr. Infra, onder randnummer 7)."

Het ontwerp geeft geen uitvoering aan de rechtsgrond die wordt opgegeven, maar beperkt zich ertoe hetzij naar hogere regels te verwijzen, hetzij een aantal vage regels⁵ te formuleren die gelden voor de politie-informaticasystemen die het elektronisch zegel produceren (artikel 2 van het ontwerp), waarbij de mogelijkheid opengelaten wordt dat andere regels niet door de Koning maar bij de politie vastgesteld worden (artikel 1, §2, van het ontwerp).

Niet alleen is het met een dergelijke regeling niet duidelijk welke veiligheidsmaatregelen en technische normen inzake ondertekening met behulp van het geavanceerd elektronisch zegel daadwerkelijk opgelegd worden; belangrijker nog is dat de wetgever geen dergelijk onderscheid lijkt te hebben willen maken tussen de bevoegdheden die aan de Koning zijn toegekend en die welke aan de politie zijn toegekend, aangezien hij de Koning ermee belast heeft het geheel van de toepasselijke minimale normen te bepalen (artikel 40, §3, vierde lid, van de wet van 5 augustus 1992).

4.5. In weerwil van de uitleg die in het verslag aan de Koning gegeven wordt en onder voorbehoud van het technisch karakter van de aangelegenheid, blijkt ook niet duidelijk uit het ontworpen dispositief en meer bepaald niet uit de combinatie van de artikelen 1, §2, en 2 van het ontwerp dat ervan uitgegaan kan worden dat het ontwerp voldoet aan de vier voorwaarden gesteld in artikel 36 van de eIDAS-verordening, dat als volgt gesteld is:

“Een geavanceerd elektronisch zegel voldoet aan de volgende eisen:

- a) het is op unieke wijze aan de aanmaker van het zegel verbonden;
- b) het maakt het mogelijk de aanmaker van het zegel te identificeren;
- c) het komt tot stand met gebruikmaking van gegevens voor het aanmaken van elektronische zegels die de aanmaker van het zegel met een hoog vertrouwensniveau onder zijn controle kan gebruiken voor het aanmaken van elektronische zegels; en
- d) het is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.”

4.6. Het is jammer dat in het ontwerp andere terminologie gebruikt wordt dan die welke in artikel 3 van de eIDAS-verordening gedefinieerd wordt.

Artikel 36 van die verordening legt voorwaarden op die verband houden met de “aanmaker van een zegel”, die in artikel 3, punt 24, van die verordening gedefinieerd wordt als “een rechtspersoon die een elektronisch zegel aanmaakt”. Artikel 3, punt 6, van de eIDAS-

⁵ Aldus bepaalt artikel 2, 1°, dat de politie-informaticasystemen zullen moeten voorzien in veiligheidsmaatregelen en technische normen die de mogelijkheid bieden om “[de] functies en [de] mandaten te beheren” van de gebruikers. Zo ook voorziet de bepaling onder 2° van hetzelfde artikel in de authenticatie van de ondertekenaar “met behulp van een systeem van sterke authenticatie” zonder dat wordt gepreciseerd wat die begrippen omvatten.

verordening definieert de “vertrouwende partij” als “een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst”, terwijl artikel 3, punt 9 van de eIDAS-verordening de “ondertekenaar” definieert als “een natuurlijke persoon die een elektronische handtekening aanmaakt”.

In artikel 2 van het ontwerp wordt echter de term “gebruikers” (1°) of “ondertekenaar” (2°) gebezigd om “de aanmaker van het zegel” aan te duiden, die overeenkomstig de verordening enkel een rechtspersoon kan zijn.

In dat verband stond in de verantwoording van het amendement dat aan de basis ligt van artikel 60 van de wet van 25 mei 2018, dat artikel 40 van de wet van 5 augustus 1992 vervangen heeft, het volgende te lezen:

“Er zijn echter gevallen waarin het niet opportuun is de verbalisant individueel te identificeren (40, §3, 1°) of authenticeren (40, §3, 2° en 3°).

In die drie gevallen hieronder vermeld wordt voor de elektronische handtekening een andere standaard vastgelegd, namelijk het gebruik van het geavanceerd elektronisch zegel.

In die drie gevallen moeten natuurlijk ook waarborgen worden geboden inzake de authenticatie van de opsteller van het proces-verbaal en de onweerlegbaarheid van de inhoud van het proces-verbaal. Het fundamentele verschil met de (gekwaliceerde) elektronische handtekening is dat in die gevallen die waarborgen niet in naam van een persoon worden geboden (de authenticatie betreft niet de verbalisant, zelfs al kan hij in het proces-verbaal worden geïdentificeerd), maar in naam van een rechtspersoon (de federale politie of de een- of meergemeentezones).

(...)

In de drie in §3 van artikel 40 opgesomde gevallen, is de norm voor de digitale handtekening dus deze die samenhangt met het geavanceerd elektronisch zegel in de zin van artikel 36 van de Europese Verordening eIDAS. Dit artikel preciseert de eisen voor elektronische zegels.

(...)

De eIDAS-verordening bepaalt dat het elektronische zegel voorbehouden is aan rechtspersonen. Dit zegel maakt het mogelijk om de link te leggen tussen de verzegelde elektronische gegevens en een rechtspersoon. Een rechtspersoon is een entiteit waaraan rechtspersoonlijkheid is toegekend.”⁶

Uit het bovenstaande volgt dat artikel 2 van het ontwerp verwarring schept doordat het termen bezigt die geen verband houden met het geavanceerd elektronisch zegel maar wel met de gekwalificeerde elektronische handtekening en dat het ook op dat punt herzien moet worden.

Er dient geconcludeerd te worden dat artikel 1, §§1 en 2, en artikel 2 grondig herzien moeten worden. Artikel 4 van het ontwerp moet bijgevolg eveneens herzien worden.⁷

⁶ Parl.St. Kamer 2017-18, nr. 54-2827/004, 78, 80 en 82.

⁷ Artikel 4 van het ontwerp heeft betrekking op het bewaren door de federale politie van de normen “bedoeld in de artikelen 1 en 2”. De zinsnede waarin gepreciseerd wordt dat die normen bewaard moeten worden in een volgens “de regels van de kunst” beveiligde omgeving is evenmin voldoende nauwkeurig en het staat aan de steller van de tekst

4.7. Artikel 1, §3, belast het Controleorgaan op de politionele informatie ermee te controleren of “die maatregelen en normen adequaat zijn en correct ten uitvoer worden gelegd”.

Het is van tweeën één: ofwel maakt die opdracht deel uit van de opdrachten die limitatief opgesomd worden in artikel 71, §1, derde lid, 1° en 2°, van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’ en in dat geval behoort die opdracht niet in herinnering te worden gebracht in de ontworpen tekst, ofwel gaat het om een nieuwe opdracht en dient artikel 71, §1, derde lid, 3°, van de wet toegepast te worden, dat zegt dat een andere extra opdracht “door of krachtens andere wetten” aan het COC “verleend” moet worden.⁸

In casu moet waarschijnlijk een nuance aangebracht worden en moeten twee aspecten onderscheiden worden in de nieuwe opdracht, zoals die in artikel 1, §3, van het ontwerp bedoeld wordt: ten eerste het uitwerken van de technische maatregelen en de minimale normen en dus de mogelijkheid om op het ogenblik van de totstandkoming ervan na te gaan of deze adequaat zijn, wat onder artikel 71, §1, derde lid, 3°, van de wet valt, en ten tweede het controleren van de correcte toepassing van die maatregelen en normen bij hun tenuitvoerlegging, wat onder artikel 71, §1, derde lid, 1°, van de wet valt.⁹

Kortom, aan het COC kan geen nieuwe opdracht verleend worden bij koninklijk besluit, maar er moet een wetgevend initiatief genomen worden wat betreft het aspect dat nog niet onder zijn huidige wettelijke opdrachten valt, zoals die bepaald zijn in artikel 71 van de wet van 30 juli 2018.

Artikel 1, §3, van het ontwerp moet bijgevolg weggelaten worden.

om te omschrijven wat hij bedoelt met “regels van de kunst” door aan te geven welke bewaringsnormen hij in acht wil nemen.

⁸ Artikel 71 is als volgt gesteld:

“§1. Bij de Kamer van volksvertegenwoordigers wordt een onafhankelijke toezichthoudende autoriteit op de politionele informatie opgericht, Controleorgaan op de politionele informatie genoemd.

Zij is de rechtsopvolger van het Controleorgaan op de politionele informatie opgericht bij artikel 36ter, §1, eerste lid, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Zij is ten aanzien van de bevoegde overheden bedoeld in artikel 26, §1, 7°, a), d) en f), belast, met:

1° het toezicht op de toepassing van deze titel, zoals voorzien door artikel 26, 15°;

2° de controle van de verwerking van de informatie en de persoonsgegevens bedoeld in de artikelen 44/1 tot 44/11/13 van de wet van 5 augustus 1992 op het politieambt, met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2 van dezelfde wet;

3° elke andere opdracht haar door of krachtens andere wetten verleend.

Zij is eveneens ten aanzien van de bevoegde overheid bedoeld in artikel 26, §1, 7°, e), belast met het toezicht op de toepassing van artikel 281, §4, van de algemene wet inzake douane en accijnzen van 18 juli 1977.

§2. De zetel van het Controleorgaan op de politionele informatie is gevestigd in het administratief arrondissement Brussel-Hoofdstad.

Bij de uitvoering van haar opdrachten en de uitoefening van haar bevoegdheden overeenkomstig deze wet en andere wetten treedt het Controleorgaan op de politionele informatie volledig onafhankelijk op.”

⁹ Zie het advies van de inspecteur-generaal van Financiën van 19 april 2019, punt 2.2 en advies 190008 van het COC van 11 april 2019, punt 9.

4.8. In verband met artikel 5 dient het volgende opgemerkt te worden, in de lijn van de volgende overwegingen die geformuleerd zijn in punt 10 van advies 190008 van het COC:

“Artikel 5 bepaalt de vermeldingen die het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening bevatten zowel in een gematerialiseerde als in een gedematerialiseerde omgeving. Tevens wordt de mogelijkheid voorzien om de identiteit van de ondertekenaar in bepaalde gevallen te beschermen door het gebruik van een uniek nummer.

Hierbij dient opgemerkt dat bij gebruik van een gekwalificeerde elektronische handtekening, de identiteit van de ondertekenaars steeds inherent verbonden is aan de digitale handtekening. Bijvoorbeeld in het geval van het gebruik van de e-ID, staat deze identiteit namelijk in het certificaat van de e-ID, waarvan de inhoud niet kan worden gewijzigd. Deze identiteit kan worden verborgen bij het materialiseren of afdrukken, maar aan het digitale verzegelde pv zal steeds het certificaat afkomstig van de e-ID kaart nodig zijn om de elektronische handtekening te kunnen valideren. Het verdient aanbeveling om hiermee rekening te houden indien men de identiteit van de verbalisant wenst te beschermen of af te schermen. In voorkomend geval kan worden gedacht om de pv's te laten verzegelen door een gemachtigde afgevaardigde van de betrokken dienst, zij het niet de verbalisant.”

Uit artikel 26 van de eIDAS-verordening volgt inderdaad dat

“[e]en geavanceerde elektronische handtekening [...] aan de volgende eisen [voldoet]:

- a) zij is op unieke wijze aan de ondertekenaar verbonden;
- b) zij maakt het mogelijk de ondertekenaar te identificeren;
- c) zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken, en
- d) zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.”

Net als in de opmerking gemaakt over artikel 2 van het ontwerp, wordt er op gewezen dat de steller van het ontwerp terminologie bezigt die niet overeenstemt met de in de eIDAS-verordening gebruikte terminologie. In artikel 5, §1, 2°, en §3, van het ontwerp worden de termen “ondertekenaar” en “verbalisant” (artikel 5, §1, 2°, van het ontwerp) immers door elkaar gebruikt, ook in het geval van het geavanceerd elektronisch zegel.

Tot slot bepaalt artikel 5, §3, van het ontwerp dat in het geval bedoeld in artikel 40, §3, 1°, van de wet van 5 augustus 1992 het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening van de processen-verbaal een aan de ondertekenaar toegekend uniek nummer bevatten dat zijn reële identiteit beschermt. Zoals in de opmerking over artikel 2 van het ontwerp vermeld wordt, heeft artikel 40, §3, 1°, van de wet van 5 augustus 1992 echter alleen betrekking op het geval van het geavanceerd elektronisch zegel, wat ook bevestigd wordt in de aangehaalde parlementaire voorbereiding.

Artikel 5 van het ontwerp moet dienovereenkomstig herzien worden.

5. Het besluit is dat de tekst grondig herzien moet worden opdat hij in overeenstemming is met het juridisch kader ervan en op correcte wijze uitvoering geeft aan de rechtsgrond ervan.

Uit dat oogpunt wordt de aandacht van de steller van het ontwerp meer in het bijzonder gevestigd op het feit dat het dispositief er zich toe bepaalt naar hogere regels te verwijzen of een opsomming te geven van doelstellingen die met de veiligheidsmaatregelen bereikt moeten worden, terwijl het overeenkomstig artikel 40, §3, vierde lid, van de wet van 5 augustus 1992 aan de Koning staat om zelf “de [minimale] veiligheidsmaatregelen (...) [te bepalen] waaraan politie-informaticasystemen moeten voldoen die het geavanceerd elektronisch zegel produceren”. In het ontwerp wordt zelfs niets bepaald in verband met het vaststellen van de “minimale technische normen” ter zake, terwijl dat bij die machtiging is voorgeschreven.

LE GREFFIER – DE GRIFFIER

LE PRÉSIDENT – DE VOORZITTER

Béatrice DRAPIER

Pierre VANDERNOOT