

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

4 septembre 2020

PROPOSITION DE LOI
contenant le Code de procédure pénale

AVIS DE L'AUTORITÉ
DE PROTECTION DES DONNÉES
N° 77/2020 DU 24 AOÛT 2020

Voir:

Doc 55 **1239/ (2019/2020)**:
001: Proposition de loi de M. Verherstraeten et Mme Slegers.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

4 september 2020

WETSVOORSTEL
houdende het Wetboek van Strafprocesrecht

ADVIES VAN
DE GEGEVENSBECHERMINGSAUTORITEIT
NR. 77/2020 VAN 24 AUGUSTUS 2020

Zie:

Doc 55 **1239/ (2019/2020)**:
001: Wetsvoorstel van de heer Verherstraeten en mevrouw Slegers.

03060

N-VA	: Nieuw-Vlaamse Alliantie
Ecolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
PS	: Parti Socialiste
VB	: Vlaams Belang
MR	: Mouvement Réformateur
CD&V	: Christen-Democratisch en Vlaams
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Open Vld	: Open Vlaamse liberalen en democraten
sp.a	: socialistische partij anders
cdH	: centre démocrate Humaniste
DéFI	: Démocrate Fédéraliste Indépendant
INDEP-ONAFH	: Indépendant - Onafhankelijk

Abréviations dans la numérotation des publications:		Afkorting bij de numering van de publicaties:	
DOC 55 0000/000	Document de la 55 ^e législature, suivi du numéro de base et numéro de suivi	DOC 55 0000/000	Parlementair document van de 55 ^e zittingsperiode + basisnummer en volgnummer
QRVA	Questions et Réponses écrites	QRVA	Schriftelijke Vragen en Antwoorden
CRIV	Version provisoire du Compte Rendu Intégral	CRIV	Voorlopige versie van het Integraal Verslag
CRABV	Compte Rendu Analytique	CRABV	Beknopt Verslag
CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)	CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)
PLEN	Séance plénière	PLEN	Plenum
COM	Réunion de commission	COM	Commissievergadering
MOT	Motions déposées en conclusion d'interpellations (papier beige)	MOT	Moties tot besluit van interpellaties (beigegekleurig papier)



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 77/2020 du 24 août 2020

Objet: Demande d'avis concernant une proposition de loi contenant le Code de procédure pénale (CO-A-2020-059)

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

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

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

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

Vu la demande d'avis du Président de la Chambre des Représentants, Monsieur Patrick DEWAELE, reçue le 16 juin 2020;

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

Émet, le 24 août 2020, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Président de la Chambre des Représentants a introduit auprès de l'Autorité une demande d'avis concernant une proposition de loi contenant le Code de procédure pénale (CO-A-2020-059) (ci-après « la proposition »). Cette proposition est le résultat du processus de réforme du droit pénal initié par un arrêté ministériel du 30 octobre 2015 ayant conduit à la désignation, conformément à l'Accord de gouvernement du 10 octobre 2014, de deux commissions pluridisciplinaires : l'une chargée de la réforme du droit pénal, l'autre de la réforme du droit de la procédure pénale. Ce sont les fruits des travaux de la seconde que concerne la demande d'avis.
2. En quelques mots repris de l'exposé des motifs de la proposition, car il est impossible de synthétiser ici et en tous ses aspects, la réforme entreprise, la proposition poursuit l'objectif suivant. Elle instaure « un seul type d'enquête[, à charge et à décharge,¹] sous la direction du ministère public et le contrôle d'un juge[, le juge de l'enquête], qui ne dirigera plus lui-même l'enquête mais sera renforcé dans sa fonction juridictionnelle et de contrôle à l'égard de l'enquête préliminaire »². La réforme gomme en conséquence les différences de garanties de protection des droits de la défense des justiciables résultant en droit positif, des différences entre les règles régissant l'instruction et l'information, et recherche la cohérence dans la procédure pénale.
3. Elle supprime par ailleurs, la possibilité de l'engagement de l'action publique par une plainte avec constitution de partie civile en mains du juge d'instruction, qu'elle remplace par un régime alternatif incluant un recours devant la Chambre de l'enquête (actuelle Chambre des mises en accusation) contre un éventuel classement sans suite par le ministère public³, qui doit garantir aux victimes le maintien d'une protection juridique⁴.
4. Si l'institution du juge d'instruction disparaît, la proposition souligne que « l'autorisation préalable du [juge de l'enquête] continuera bien évidemment d'être requise pour toutes les mesures de contrainte qui sont actuellement soumises à contrôle judiciaire », et « même davantage, puisque certaines mesures intrusives qui sont ou ont été susceptibles d'être ordonnées par le Parquet (comme l'infiltration et l'observation systématique de plus de cinq jours ou avec des moyens techniques ou l'extension de la recherche informatique au-delà du support saisi) seraient à l'avenir soumises à l'autorisation du juge »⁵. Ce qui se révèle être d'une importance toute particulière dans le domaine des droits fondamentaux à la vie privée et à la protection des données.

¹ Voir l'exposé des motifs de la proposition, pp. 11 et s.

² Exposé des motifs de la proposition, p. 6.

³ Voir à ce sujet l'exposé des motifs de la proposition, p. 15.

⁴ Exposé des motifs de la proposition, p. 6.

⁵ Exposé des motifs de la proposition, p. 9 et note de bas de page n° 10.

5. Enfin, il est à noter que toutes les dispositions actuelles du Code d'instruction criminelle, dont celles relatives au casier judiciaire central, à l'effacement des condamnations et à la réhabilitation en matière pénale, ne sont pas reprises dans la proposition de Code de procédure pénale⁶. L'exposé des motifs de la proposition explique que ces dispositions qui concernent « la mémoire et l'oubli des peines » trouveraient plus logiquement leur place dans un Code d'exécution des peines ou des lois particulières⁷.
6. Le présent avis traite tout d'abord de la question de la compétence de l'Autorité (II) et explicite ensuite la portée de l'analyse qui est menée (III). Cette dernière suit enfin (IV).

II. COMPÉTENCE DE L'AUTORITÉ

7. Dans le domaine 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, l'article 45, 2. de la directive (UE) n° 2016/680⁸ [la directive n° 2016/680] prévoit que « Chaque État membre prévoit que chaque autorité de contrôle n'est pas compétente pour *contrôler les opérations de traitement* effectuées par les juridictions dans l'exercice de leur *fonction juridictionnelle*. Les États membres peuvent prévoir que leur autorité de contrôle n'est pas compétente pour *contrôler les opérations de traitement* effectuées par d'autres autorités judiciaires indépendantes lorsqu'elles agissent dans l'exercice de leur *fonction juridictionnelle* » (italiques ajoutés par l'Autorité)⁹.
8. Le considérant n° 80 de cette directive explique que « Bien que la présente directive s'applique également aux activités des juridictions nationales et autres autorités judiciaires, *la compétence* des autorités de contrôle ne devrait pas s'étendre au traitement des données à caractère personnel effectué par les juridictions dans l'exercice de leur *fonction juridictionnelle*, *afin de préserver l'indépendance des juges dans l'accomplissement de leurs missions judiciaires*. Il convient que cette exception soit *limitée aux activités judiciaires dans le cadre d'affaires portées devant les juridictions* et qu'elle ne s'applique pas aux autres activités auxquelles les juges pourraient être associés conformément au droit d'un État membre. Les États membres devraient aussi pouvoir prévoir que la compétence de l'autorité de contrôle ne s'étend pas aux traitements de données à caractère personnel effectués par *d'autres autorités judiciaires indépendantes* dans l'exercice de leur fonction juridictionnelle, par exemple le

⁶ Voir l'exposé des motifs de la proposition, p. 350.

⁷ P. 351.

⁸ La Directive (UE) n° 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.

⁹ L'article 55, 2. du RGPD dispose également que « Les autorités de contrôle ne sont pas compétentes pour *contrôler les opérations de traitement* effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle » (italiques ajoutés par l'Autorité).

Avis 77/2020 - 4/24

ministère public. En tout état de cause, le respect des règles de la présente directive par les juridictions et autres autorités judiciaires indépendantes fait toujours l'objet d'un contrôle indépendant conformément à l'article 8, paragraphe 3, de la Charte » (italiques ajoutés par l'Autorité)¹⁰.

9. L'article 28, 2. de la directive n° 2016/680 prévoit que « Les États membres prévoient que l'autorité de contrôle est consultée dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative qui se rapporte au traitement ».
10. En droit belge, l'article 4, § 1^{er}, alinéa 2 de la LCA dispose que « Le *contrôle organisé par la présente loi* ne porte pas *sur les traitements effectués par les cours et tribunaux* ainsi que le ministère public dans l'exercice de leur fonction juridictionnelle » (italiques ajoutés par l'Autorité). L'exposé des motifs du projet de la LCA explique quant à cette disposition que « La Belgique utilise ici la marge laissée par le Règlement 2016/679 pour préciser que cette *incompétence* s'étend également au ministère public pour l'ensemble de ses missions ainsi qu'en ce qui concerne ses mandats pénaux et civils. La notion "dans l'exercice de leur fonction juridictionnelle" doit être interprétée au sens large afin de garantir une application uniforme de cette exclusion. Par exemple, les traitements de données dans le cadre de la gestion du personnel de ces autorités judiciaires sont aussi compris dans les traitements nécessaires à l'exercice de leur fonction juridictionnelle »¹¹ (italiques ajoutés par l'Autorité).
11. Cette exclusion de la compétence de l'autorité de contrôle à l'égard des traitements liés à la fonction juridictionnelle vise le « contrôle » des « traitements » en ce domaine et ce, en vue de garantir l'indépendance du pouvoir judiciaire, et non « toute compétence » de l'Autorité à l'égard généralement, de la matière pénale. Autrement dit, elle n'exclut pas une compétence d'avis sur une législation, telle que celle en cause en l'espèce – le code de procédure pénal –, se trouvant au cœur de la fonction juridictionnelle pénale.
12. En effet premièrement, il ne s'agit pas de contrôler un traitement du ministère public ou d'une cour ou d'un tribunal *in concreto*, mais bien de rendre un avis sur un acte du législateur, à savoir un acte relevant de la fonction (du pouvoir) législative (législatif). Et deuxièmement, l'exercice d'une compétence d'avis dans le processus législatif ne pourrait avoir d'impact sur l'indépendance du pouvoir

¹⁰ Le considérant n° 20 du RGPD quant à lui, précise que « Bien que le présent règlement s'applique, entre autres, aux activités des juridictions et autres autorités judiciaires, le droit de l'Union ou le droit des États membres pourrait préciser les opérations et procédures de traitement en ce qui concerne le traitement des données à caractère personnel par les juridictions et autres autorités judiciaires. La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de *préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires, y compris lorsqu'il prend des décisions*. Il devrait être possible de confier le contrôle de ces opérations de traitement de données à des organes spécifiques au sein de l'appareil judiciaire de l'État membre, qui devraient notamment garantir le respect des règles du présent règlement, sensibiliser davantage les membres du pouvoir judiciaire aux obligations qui leur incombent en vertu du présent règlement et traiter les réclamations concernant ces opérations de traitement de données » (italiques ajoutés par l'Autorité).

¹¹ *Doc. Parl.*, 2016-2017, Chambre des Représentants, Doc. (54) n° 2648/001pp. 13-14.

judiciaire dans l'exercice de ses fonctions de poursuivre et juger : il n'y a aucune interférence avec celles-ci.

13. Par conséquent, l'Autorité est compétente pour analyser la proposition soumise pour avis et ce, en application de l'article 4, § 2, alinéa 2 de la LCA qui consacre la compétence résiduelle de l'Autorité qui est « l'autorité de contrôle compétente lorsqu'aucune autre loi n'en dispose autrement ».
14. Les développements précités sont l'occasion de rappeler qu'en droit positif, aucune autorité n'est compétente pour contrôler la conformité des traitements dont sont responsables les autorités judiciaires, pénales en l'occurrence, aux règles de protection des données. Il s'agit d'une lacune importante du droit belge. Pour rappel, l'article 8, 3. de la Charte des droits fondamentaux de l'Union européenne prévoit lui-même que le respect des règles de protection des données doit être soumis au contrôle d'une autorité indépendante.

III. PORTEE DE L'AVIS

15. L'exposé des motifs de la proposition¹² rappelle qu'en la matière, s'applique le Titre 2 de la LTD¹³ qui transpose la directive n° 2016/680. L'article 37, § 4 de la LTD dispose que :

« Les droits visés au présent chapitre, pour ce qui concerne les traitements de données des cours et tribunaux de droit commun et du ministère public, *sont exercés exclusivement dans les limites et conformément aux règles et modalités précisées dans le Code judiciaire, le Code d'instruction criminelle, les lois particulières relatives à la procédure pénale et leurs arrêtés d'exécution* » (italiques ajoutés par l'Autorité).

16. Sont ainsi concernés les droits à l'information de la personne concernée¹⁴, son droit d'accès¹⁵, son droit à la rectification, à l'éventuelle complétion ou à l'effacement des données inexacts¹⁶, droits qui en substance, en application de l'article 41, alinéa 1^{er} de la LTD, si la loi (le décret ou l'ordonnance) en disposait ainsi, pourraient être exercés par l'intermédiaire de l'autorité de contrôle compétente. Dans une telle hypothèse, en vertu de l'alinéa 2 de ce même article, le responsable du traitement devrait informer la personne concernée qu'elle exerce ses droits par l'intermédiaire de l'autorité de contrôle compétente.

¹² P. 56.

¹³ Voir l'article 27 de la LTD.

¹⁴ Article 37 de la LTD.

¹⁵ Article 38 de la LTD.

¹⁶ Article 39 de la LTD.

17. Sur ce dernier point toutefois, ni le droit positif comme cela vient d'être rappelé (plus haut, considérant n° 14), ni la proposition soumise pour avis ne désignent une autorité compétente à cet effet.

18. L'article 44 de la LTD dispose encore que :

« Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou faisant l'objet d'un *traitement lors d'une enquête judiciaire et d'une procédure pénale*, les droits visés aux articles 37, 38, § 1er, 39 et 41, alinéa 2, *sont exercés conformément au Code judiciaire, au Code d'instruction criminelle, aux lois particulières relatives à la procédure pénale ainsi qu'à leurs arrêtés d'exécution* » (italiques ajoutés par l'Autorité).

19. Enfin concernant l'action en cessation consacrée dans l'article 209 de la LTD, l'article 210 de la LTD prévoit que :

« A partir du moment où le traitement visé par l'article 209 concerne des données à caractère personnel traitées *lors d'une information, d'une instruction, d'une procédure pénale* devant le juge de fond ou d'une procédure d'exécution d'une peine pénale, la décision concernant la rectification, l'effacement ou l'interdiction d'utiliser les données à caractère personnel, ou la limitation du traitement, appartient toutefois exclusivement, *suivant la phase de la procédure, au ministère public ou au juge pénal compétent* » (italiques ajoutés par l'Autorité).

20. Dans ce contexte législatif, l'exposé des motifs de la proposition¹⁷ souligne cependant plus généralement que « L'aspect du traitement des données à caractère personnel n'a pas encore été intégré dans le projet de Code de procédure pénale ».

21. Concernant les droits de la personne concernée, l'exposé des motifs de la proposition expose et reconnaît ce qui suit¹⁸ :

« Dans le cadre de l'information actuelle, *il n'existe que le droit de consultation et de prise d'une copie du dossier pénal* (article 21bis du C.i.cr.) ainsi que le droit de demander la levée d'un acte d'information dans le chef d'une personne lésée par celui-ci quant à ses biens (art. 28sexies du C.i.cr.). *En ce qui concerne l'exercice des droits d'une personne dont les données à caractère personnel sont traitées dans le cadre d'une information*, en particulier s'il s'agit, par exemple, d'une demande de complétion, de rectification ou d'effacement de ces données, *les règles du Code d'instruction criminelle actuel sont insuffisantes.*

¹⁷ P. 56.

¹⁸ Pp. 57-58.

Comme indiqué, le présent projet de Code de procédure pénale introduit une seule forme d'enquête préliminaire sous la direction du ministère public. Les suspects et personnes lésées concernés bénéficient des mêmes droits, dont celui de demander une enquête complémentaire. Chaque droit est en outre associé à la possibilité de former un recours auprès d'un juge contre le refus ou l'inaction du ministère public. Il est renvoyé à l'examen du Titre IV consacré aux droits des personnes concernées durant l'enquête. *La transposition des droits d'une personne dont les données à caractère personnel sont traitées requiert une intervention relativement mineure dans le système proposé.*

Compte tenu de la teneur de l'article 41 de la loi du 30 juillet 2018 précitée, il est néanmoins *recommandé de connaître l'opinion du législateur quant à la création éventuelle d'une autorité de contrôle compétente avant de procéder à une adaptation du projet.* Les motifs de refus précités sous les points 1, 2 et 5 correspondent en effet en grande partie aux motifs de refus applicables à l'exercice des droits des personnes concernées durant l'enquête pénale, ce qui rend primordiale la demande de création d'une autorité de contrôle » (italiques ajoutés par l'Autorité).

22. L'Autorité prend par conséquent acte du fait que quant à la protection des données à caractère personnel et en particulier, quant aux droits des personnes concernées ainsi que quant à la désignation d'une autorité de contrôle compétente afin de contrôler le ministère public et les tribunaux et les cours impliqués dans la procédure pénale, la proposition est incomplète. L'Autorité part par conséquent du principe qu'elle sera de nouveau consultée en la matière.
23. Pour le reste, ces lacunes n'empêchent pas qu'il appartienne à l'Autorité de se pencher sur cette proposition. En effet, premièrement, malgré ces lacunes, la proposition porte néanmoins sur l'accès au dossier, comme l'évoque son exposé des motifs juste cité (plus haut, considérant n° 21). Certes, si l'accès au dossier en matière pénale n'est pas pensé sous l'angle de la protection des données à caractère personnel (il résulte plutôt des droits de la défense et du droit à un recours effectif), sa ressemblance avec le droit d'accès en matière de protection des données conduit à s'y intéresser, d'autant plus au regard de l'article 44 de la LTD¹⁹.
24. Et deuxièmement plus généralement, il ne peut être *a priori* exclu que la proposition ait néanmoins un impact concernant le traitement de données à caractère personnel, soit en créant ou modifiant des règles régissant des flux de données à caractère personnel ou des bases de données contenant de telles données, soit en modifiant ou créant des règles régissant les pouvoirs et compétences des

¹⁹ Il pourrait être envisagé de concevoir le droit d'accès en matière de protection des données sur la base des règles régissant l'accès au dossier.

Avis 77/2020 - 8/24

autorités compétentes dans le cadre de la procédure pénale et en l'occurrence principalement, le ministère public. Pour rappel quant à ce dernier point, l'article 8, 2. de la directive n° 2016/680, à lire en combinaison avec le 1. de ce même article et l'article 33 de la LTD²⁰, prévoient que « Une disposition du droit d'un État membre qui régit le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement ». De telles règles s'inscrivent directement dans la rencontre des droits fondamentaux à la vie privée (consacrés dans les articles 8 de la CEDH, 22 de la Constitution et 7 de la Charte des droits fondamentaux de l'Union européenne) et à la protection des données (consacré dans l'article 8 de la Charte des droits fondamentaux de l'Union européenne), et nécessitent un contrôle de la part de l'Autorité²¹.

25. Interrogé en ce sens plus généralement sur les éventuelles évolutions législatives apportées par le nouveau Code de procédure pénale et susceptibles d'avoir un impact concernant la protection des données à caractère personnel, le demandeur a notamment répondu ce qui suit :

*« Het wetsvoorstel houdende het Wetboek van Strafprocesrecht (DOC 55 1239/001) bevat in essentie **geen enkele nieuwe transfer van persoonsgegevens of databanken**.*

Het vergroot de rechten van de partijen betrokken in het strafonderzoek, maar het verleent wel een ruimere bevoegdheid aan de rechter van het onderzoek die een rol speelt over het ganse strafonderzoek en niet meer zoals de onderzoeksrechter enkel over een aantal dossiers die in onderzoek worden gesteld.

In essentie is er, wat de eigenlijke verwerking van persoonsgegevens betreft, geen fundamenteel verschil met de huidige strafrechtspleging » (gras dans le texte).

26. Dans un tel contexte, l'Autorité limitera son analyse à quelques dispositions qui, n'étant par ailleurs principalement pas des codifications à droit constant de règles déjà existantes dans le Code d'instruction criminelle, sont susceptibles d'avoir un impact sur la protection des données. Elle ne listera pas, dans son analyse, l'ensemble des points qui doivent encore être abordés en matière de protection des données dans le contexte de la procédure pénale.

²⁰ Selon lequel : « § 1er. Le traitement est licite si :

1° il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente pour les finalités énoncées à l'article 27; et

2° s'il est fondé sur une obligation légale ou réglementaire.

§ 2. L'obligation légale ou réglementaire régit au moins les catégories de données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement ».

²¹ Voir par exemple, pour une approche similaire, l'Avis n° 21/2016 de la Commission de la Protection de la Vie Privée du 18 mai 2016, concernant un avant-projet de loi relatif à l'amélioration des méthodes particulières de recherche et certaines méthodes d'enquête concernant Internet, les communications électroniques et les télécommunications.

IV. EXAMEN

IV.1. Principes de transparence et de légalité : finalités et responsables des traitements

27. **Rappel des principes.** En exécution de l'article 8, 2. de la directive n° 2016/680, lu en combinaison avec les articles 22 de la Constitution et 8 de la CDEH²², une norme de rang législatif doit déterminer les éléments essentielles d'un traitement de données nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Lorsque le traitement de données constitue une ingérence importante dans les droits et libertés des personnes concernées, ce qui est le cas du traitement de données résultant de la mise en œuvre, par le ministère public, des règles de procédure pénale régissant ses pouvoirs en vue de la prévention et de la détection des infractions pénales, il est nécessaire que les éléments essentiels suivants soient déterminés par le législateur : la (les) finalité(s) précise(s)²³ à la lecture de laquelle (desquelles) on peut déjà apercevoir les traitements de données qui seront mis en place pour sa (leur) réalisation, l'identité du (des) responsable(s) du traitement, le type de données qui sont nécessaires à la réalisation de cette (ces) finalité(s), le délai de conservation des données²⁴, les catégories de personnes concernées dont les données seront traitées, les instances, ou catégories d'instances, chargées d'une mission d'intérêt public (ou investies de l'autorité publique) relevant de cette (ces) finalité(s) et ayant accès à ces données/cette banque de données, ainsi que l'éventuelle limitation des obligations du responsable du traitement et/ou des droits des personnes concernées visé(e)s dans la directive n° 2016/680. Au regard de ces principes et des limites de l'analyse de l'Autorité (plus haut, considérant n° 26), la proposition appelle les commentaires suivants.

28. **Concept de responsable du traitement.** A propos du responsable du traitement pour rappel, l'article 26, 8° de la LTD lui-même²⁵ précise que lorsque « la finalité et les moyens de ce traitement sont déterminés par la loi, le décret ou l'ordonnance, le responsable du traitement est l'entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance ». Quant au concept de responsable du traitement, l'Autorité a déjà pu rappeler la nécessité d'appréhender ce concept dans une perspective factuelle. Il importe de désigner la (ou les) entité(s) qui, dans les faits, poursui(ven)t la finalité du traitement visé et en assure(nt) la maîtrise. Dans le secteur public, le

²² Il existe également des principes de légalité et de prévisibilité spécialement applicables à la procédure pénale en application de l'article 12, alinéa 2 de la Constitution.

²³ Voir aussi l'article 6.3 du RGPD.

²⁴ La Cour constitutionnelle a déjà reconnu que « le législateur pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation », Arrêt n° 29/2018 du 15 mars 2018, point B. 23.

²⁵ Voir également l'article 3, 8° de la directive n° 2016/680.

Avis 77/2020 - 10/24

responsable du traitement est généralement l'organe en charge de la mission de service public pour laquelle le traitement de données visé est mis en place.

29. Par ailleurs, l'objectif de la définition large du concept de responsable du traitement²⁶ est d'assurer une protection efficace et complète des personnes concernées²⁷. Selon les faits, une responsabilité conjointe de traitement peut lier plusieurs acteurs, la personne concernée pouvant alors exercer ses droits à l'égard de et contre chacun d'entre eux²⁸. Toutefois, « l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente [...] et a]u contraire, [l]es opérateurs peuvent être impliqués à différents stades du traitement de données et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce »²⁹. C'est dans « le cadre de ses responsabilités, de ses compétences et de ses possibilités » que le responsable conjoint veillera à la conformité de son activité aux règles de protection des données³⁰.

30. **L'enquête et l'action publique (articles 85, 101 et 103).** La proposition prévoit clairement que l'enquête (qu'elle définit en son article 85, alinéa 1^{er}) est « conduite sous la direction et l'autorité du procureur du Roi compétent. Il en assume la responsabilité »³¹, et que le « procureur du Roi veille à la légalité des moyens de preuve et à la loyauté avec laquelle les preuves sont rassemblées »³². Elle dispose encore, en son article 2, que le ministère public exerce l'action publique de manière indépendante, au nom de la société et dans l'intérêt public, en agissant dans le respect des droits visés dans l'article 1^{er} de la proposition, le ministère public ne pouvant recevoir aucune instruction ou directive concernant l'instruction d'une affaire individuelle³³. Autrement dit, lorsqu'elle abordera les aspects liés à la protection des données, la proposition explicitera que le procureur du Roi est le responsable du traitement des données nécessaires aux fins de l'enquête et de l'exercice de l'action publique, dans l'exécution des pouvoirs, compétences et obligations dont il dispose et est débiteur dans le présent Code.

²⁶ Les notions de responsable du traitement et de sous-traitant sont définies à l'article 4, 7) et 8) du RGPD. Lire également l'avis G29 n° 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant" (WP169), 16 février 2010.

²⁷ CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, considérant n° 34 ; CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIM GMBH), aff. C-210/16, considérant n° 28.

²⁸ Article 26, 3., du RGPD.

²⁹ CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIM GMBH), aff. C-210/16, considérant n° 43. Lire également, notamment, G29, Avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, p. 20.

³⁰ CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, considérant n° 38.

³¹ Article 85, alinéa 2, de la proposition.

³² Article 85, alinéa 3 de la proposition.

³³ Quant à cette indépendance, la proposition appelle à une réforme de la Constitution (voir son exposé des motifs, p. 13). Voir également l'article 2, alinéa 2 de la proposition, spécifiant que les directives de politique criminelle ne peuvent avoir pour effet de supprimer l'appréciation d'une affaire individuelle par le magistrat du ministère public. Sur la responsabilité du procureur du Roi, voir également l'exposé des motifs de la proposition, pp. 64-66.

31. La proposition devra en outre clairement identifier s'il existe d'autres hypothèses dans lesquelles d'autres autorités publiques sont susceptibles d'exercer de manière autonome et ainsi, en dehors de l'hypothèse d'instructions du procureur du Roi/ministère public, les pouvoirs qu'elle leur attribuerait. En particulier, l'Autorité attire l'attention de l'auteur de la proposition sur les pouvoirs que les officiers de police judiciaire pourraient exercer de manière autonome. Ainsi, si le procureur du Roi a le droit de requérir les officiers de police judiciaire (et les services de police) pour accomplir les actes de police judiciaire nécessaires à l'enquête (article 101, § 1^{er}, de la proposition), il semble que ces officiers disposent également de pouvoirs autonomes (voir par exemple l'article 150 de la proposition, visant la conservation rapide de données informatiques, et son article 171, concernant la recherche dans un système informatique). Si ces officiers peuvent agir en dehors de l'hypothèse d'une enquête sous la responsabilité du procureur du Roi, une norme du rang de loi devra clairement identifier leur responsabilité éventuellement autonome (ou conjointe) ou en tout cas, celle de l'autorité dont ils dépendent.
32. L'Autorité suppose à ce sujet, qu'il en ira le cas échéant potentiellement d'une responsabilité (conjointe, selon l'autonomie dont jouissent les officiers de police judiciaire) du procureur général près la cour d'appel ou du procureur fédéral. En effet, l'article 103, § 1^{er} de la proposition prévoit que « Tous les officiers de police judiciaire sont soumis à la surveillance, selon la distinction établie par la loi, du procureur général près la cour d'appel ou du procureur fédéral. Tous ceux qui, d'après l'article 107, sont, à raison de fonctions, même administratives, appelés par la loi à faire quelques actes de police judiciaire, sont, sous ce rapport seulement, soumis à la même surveillance »³⁴.
33. **L'enquête pénale d'exécution (articles 416 et s.).** *Mutatis mutandis*, ce qui vient d'être expliqué pour l'enquête pénale « classique » (plus haut, considérant n° 30), vaut également pour l'enquête pénale d'exécution. Ainsi, la proposition pourrait clarifier que le « magistrat EPE » est le responsable du traitement des données nécessaires à l'exécution de l'enquête pénale d'exécution³⁵, dès lors qu'il s'agit du magistrat du ministère public qui « mène l'EPE » et qui « veille à la légalité des actes d'exécution »³⁶. La proposition prévoit encore que « L'EPE est menée par et sous l'autorité et la direction du magistrat EPE compétent pour l'exécution de la condamnation coulée en force de chose jugée. Ce magistrat en porte la responsabilité »³⁷.

³⁴ Voir notamment l'exposé des motifs de la proposition, p. 128, expliquant pourquoi ne sont pas reprises dans l'article 107 les dispositions relatives aux gardes champêtres particuliers et aux gardes forestiers.

³⁵ A savoir, selon l'article 416, § 1^{er}, « l'ensemble des actes qui tendent à la recherche, l'identification et la saisie du patrimoine sur lequel la condamnation au paiement d'une amende, d'une confiscation spéciale ou des frais de justice peut être exécutée ».

³⁶ Article 416, § 2 de la proposition.

³⁷ Article 417, § 1^{er}. Voir toutefois également le § 3 du même article qui prévoit que « Le membre du ministère public près une cour d'appel qui mène l'EPE est revêtu de la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi. Il exerce cette fonction *sous la surveillance du procureur général* » (italiques ajoutés par l'Autorité).

34. La proposition pourra également clarifier dans quelle mesure le magistrat de l'Organe central pour la saisie et la confiscation [OCSC] éventuellement chargé d'une EPE ainsi que le directeur de l'OCSC, supportent une responsabilité propre ou conjointe (avec le magistrat EPE) au regard des traitements de données réalisés³⁸.
35. **Le registre d'écrou (article 487).** L'article 487 de la proposition prévoit que chaque prison a l'obligation de tenir un registre d'écrou dans lequel toutes les personnes incarcérées sont enregistrées et qui peut être consulté à tout moment par le procureur du Roi et que ce registre peut être sous forme électronique.
36. La finalité du registre d'écrou ressort clairement de l'exposé des motifs de la proposition mais devrait être explicitée dans son dispositif : « Dans le cadre du système développé de l'enquête pénale unifiée sous la direction du ministère public, le procureur du Roi doit avoir un aperçu de l'ensemble de la détention préventive et de l'exécution des peines »³⁹ ; « [...] nécessaire afin de garder une vue d'ensemble de toutes les personnes qui se trouvent en détention préventive ou exécutent leur peine et de pouvoir suivre la situation individuelle de chaque personne en détention »⁴⁰.
37. En l'état, l'article 487 de la proposition ne désigne pas de responsable du traitement. Si c'est à charge de « chaque prison » qu'existe l'obligation de disposer d'un registre d'écrou, l'exposé des motifs de la proposition précise que, vu l'objectif du registre de fournir au procureur du Roi un aperçu de l'ensemble des détentions, « Il est dès lors indiqué que le procureur du roi supervise le registre ». La proposition clarifiera, au regard des principes exposés précédemment (plus haut, considérants nos 28-29), qui est le responsable du traitement (ou qui sont le cas échéant les responsables conjoints du traitement) lié au registre d'écrou.
38. Cela étant précisé, l'Autorité relève que l'exposé des motifs de la proposition explique que dans la pratique, le registre papier a été remplacé par un registre électronique dans « Sidis-Suite » et que partant, le droit doit être adapté à la situation actuelle et à la technologie utilisée sur le terrain⁴¹. C'est également actuellement, dans la pratique, dans ce même système d'information, que les libérations sont enregistrées⁴².
39. Bien que l'exposé des motifs n'y fasse pas référence, la banque de données « Sidis-Suite » est créée auprès du SPF Justice par l'article 3 de la loi du 5 mai 2019 portant dispositions diverses en matière

³⁸ Voir l'article 418 de la proposition et en particulier, ses §§ 2 (responsabilité du magistrat), 3, alinéa 1^{er} (direction et autorité du directeur, sans préjudice de l'article 417, § 1^{er}) et 4, alinéa 1^{er} (compétences).

³⁹ P. 353.

⁴⁰ P. 354.

⁴¹ P. 353.

⁴² Exposé des motifs de la proposition, p. 354.

d'informatisation de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés, et poursuit notamment pour finalité la mission légale de l'administration pénitentiaire des exécutions des peines et mesures privatives de liberté, notamment l'application de toutes les règles relatives à la durée de la détention, ainsi qu'à la sortie temporaire ou non de l'établissement. Cette loi définit d'ailleurs plus précisément les données qui sont traitées via cette banque de données⁴³, et elle prévoit que le ministère public et les secrétaires de parquet ont accès aux données traitées⁴⁴. Pour rappel, l'Autorité a émis, par le passé, des doutes – qu'elle réitère – quant à la désignation du SPF Justice comme responsable du traitement par la loi précitée⁴⁵.

40. Par conséquent dans un tel contexte, la proposition doit articuler son article 487 avec les dispositions pertinentes de la loi du 5 mai 2019 portant dispositions diverses en matière d'informatisation de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés, de manière telle que tant les finalités, que les données et le responsable du traitement (ou les responsables conjoints du traitement) concernés par le traitement visé à l'article 487, soient clairement identifiés. La proposition identifiera ce responsable du traitement (ou les responsables conjoints du traitement), conformément aux principes exposés précédemment (plus haut, considérants nos 28-29).

IV.2. Commentaires liés à certains articles de la proposition

41. **Droit à la protection des données (article 1^{er}).** L'article 1^{er} de la proposition s'énonce comme suit :

« Sans préjudice des droits fondamentaux consacrés dans la Constitution, les conventions internationales et le droit de l'Union européenne, et des principes généraux du droit, le Code de procédure pénale s'applique dans le respect de la légalité et de la loyauté de la procédure pénale, des droits à l'égalité de traitement et à la non-discrimination, du droit à la liberté individuelle, des droits de défense, du droit à un tribunal indépendant et impartial, du droit à un procès équitable et à un jugement rendu dans un délai raisonnable, et du droit au respect de la vie privée. En conformité avec ces droits, les dispositions du présent Code sont appliquées en observant les principes de proportionnalité et de subsidiarité ».

42. L'Autorité rappelle que le droit d'une personne à la protection des données à caractère personnel la concernant est un droit fondamental reconnu de manière *autonome*, par rapport au droit au respect de la vie privée, par la Charte des droits fondamentaux de l'Union européenne en son article 8. Le droit

⁴³ Voir son article 5.

⁴⁴ Article 7, § 1^{er}, 5^o.

⁴⁵ Voir son article 4. Voir également l'Avis de l'APD n° 120/2018 du 7 novembre 2018, p. 3, considérant n° 10.

à la protection des données n'est pas seulement lié au droit à la vie privée : plus largement, ce sont *les droits et libertés des personnes physiques* qu'il tend plus généralement à garantir, à l'égard du traitement des données à caractère personnel⁴⁶. Autrement dit, une référence au respect de ce droit dans le cadre de la procédure pénale est à tout le moins tout aussi pertinente qu'une référence au droit au respect de la vie privée dans l'article 1^{er} de la proposition de Code de procédure pénale. Outre le fait que la protection des données aille au-delà de la protection de la vie privée, il sera en effet systématiquement recouru au traitement de données à caractère personnel (tant pour la collecte des données que pour leur exploitation) dans le cadre de la procédure pénale, comme d'ailleurs plus généralement, dans le cadre de l'exercice de nombreuses missions d'intérêt public (ou relevant de l'exercice de l'autorité publique) par les autorités publiques compétentes.

43. L'Autorité est par conséquent d'avis qu'il convient d'ajouter dans la première phrase de cette disposition, une référence au droit à la protection des données.
44. **Admissibilité de la preuve (articles 11 et 12).** La proposition de Code adopte une approche rejoignant le système de la règle de l'exclusion relative de la preuve⁴⁷. *Mutatis mutandis*, le même commentaire que celui concernant l'article 1^{er} de la proposition, vaut à propos de l'article 11 de la proposition. Ce dernier régit, en matière de sanction de la preuve irrégulière, l'admissibilité éventuelle d'informations obtenues en violation, notamment, des droits de la défense ou du droit à la vie privée.
45. Ne pas intégrer le droit à la protection des données dans cette disposition reviendrait à imposer l'exercice périlleux de distinguer parmi les violations des règles de protection des données celles qui constitueraient également ou pas une violation du droit à la vie privée (ce qui est source d'insécurité juridique et de distinctions potentiellement artificielles)⁴⁸, dès lors que les atteintes aux droits qui ne sont pas visées à l'article 11 de la proposition, sont soumises à un régime d'admissibilité des preuves *plus souple* prévu à l'article 12 de la proposition⁴⁹. Or l'Autorité est d'avis qu'en vue d'une protection

⁴⁶ Voir par exemple, le considérant n° 7 et les articles 1^{er}, 2, a), 19, 20, 27, 28, 29, 30, 31 et 36, 2., a) de la directive n° 2016/680. En 1981 déjà, l'article 1^{er} de la Convention n° 108 du Conseil de l'Europe (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) disposait que : « Le but de la présente Convention est de *garantir*, sur le territoire de chaque Partie, *à toute personne physique*, quelles que soient sa nationalité ou sa résidence, *le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée*, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données ») » (italiques ajoutés par l'Autorité). Cette approche a encore été confirmée plus récemment dans le cadre de la modernisation de la Convention n° 108 du Conseil de l'Europe, dans l'article 1^{er} de la Convention n° 108+ : « Le but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, *contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée* » (italiques ajoutés par l'Autorité).

⁴⁷ Voir l'exposé des motifs de la proposition, pp. 69 et s.

⁴⁸ Certes, dans la jurisprudence de la Cour européenne des droits de l'homme, c'est (logiquement) systématiquement par le truchement de l'article 8 CEDH que la protection des données (et le cas échéant, la Convention n° 108 du Conseil de l'Europe) sont invoquées, s'agissant de la disposition la plus pertinente de la Convention en la matière. Voir notamment, Cour européenne des droits de l'homme, « Guide sur l'article 8 de la Convention européenne des droits de l'homme, Droit au respect de la vie privée et familiale », 2019, mis à jour au 31 août 2019, paragraphes nos 159 et s.

⁴⁹ Selon celui-ci : « En dehors des cas visés aux articles 9 à 11, les informations obtenues de manière irrégulière peuvent être admises aux débats sauf si le juge constate que leur utilisation dans une décision de justice porte atteinte à l'intégrité de la Justice ». L'exposé des motifs de la proposition (p. 78) explique à ce sujet que : « Cet article dispose que en dehors des cas

efficace des personnes à l'égard du traitement des données à caractère personnel dans le cadre de la procédure pénale, c'est du régime consacré dans l'article 11 de la proposition que les violations du droit à la protection des données doivent relever.

46. En particulier à propos de l'article 11 de la proposition, l'Autorité prend acte des modifications apportées par cette disposition à la jurisprudence et à la doctrine Antigone entre-temps entérinée en droit positif⁵⁰. Ainsi en vertu du Code de procédure pénale proposé, une information⁵¹ obtenue en violation du droit à la vie privée est en principe exclue des débats, de même que les informations qui en sont dérivées, sauf si le juge constate trois conditions cumulatives : l'irrégularité ne résulte pas d'une méconnaissance consciente ou inexcusable du droit ou de la valeur protégée ; le degré d'atteinte au droit ou à la valeur protégée est, concrètement, de moindre gravité que l'intérêt public à la poursuite de l'infraction en question et à la sanction éventuelle de son auteur ; et l'utilisation de la preuve irrégulière ne porte pas atteinte à l'intégrité de la Justice.
47. L'Autorité, bien qu'elle soit favorable à l'approche suivie dans l'article 11 de la proposition, relève qu'il n'est plus directement fait référence, comme actuellement dans l'article 32 du titre préliminaire du code de procédure pénale, à l'hypothèse où l'irrégularité commise « a entaché la fiabilité de la preuve » (hypothèse distinguée, dans ce texte, de celle de la violation du droit à un procès équitable).
48. Or en matière de protection des données, un tel critère fait échos aux principes de qualité des données et de sécurité, d'autant plus cruciaux qu'il s'agit d'établir la preuve : les données traitées doivent notamment être exactes et mises à jour, et traitées de façon à garantir une sécurité appropriée⁵². Dans le domaine de la preuve et de la sécurité de l'information, au titre de la fiabilité de la preuve, une attention particulière devra être apportée aux garanties entourant la disponibilité et l'intégrité des

visés aux articles 9 à 11, les informations obtenues de manière irrégulière peuvent être admises aux débats sauf si le juge constate que leur utilisation dans une décision de justice porte atteinte à l'intégrité de la Justice. Il s'agit de cas d'irrégularités moins intrusifs qui ne relèvent pas de la réglementation décrite à l'article 11, car ils ne portent pas atteinte aux droits fondamentaux qui y sont énumérés. Si les informations ont été obtenues de manière irrégulière à l'époque, il peut être accepté qu'elles soient admises aux débats, sauf si le juge constate que leur utilisation porte atteinte à l'intégrité de la Justice ».

⁵⁰ L'article 32 du titre préliminaire du Code de procédure pénale dispose que : « La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si :

- le respect des conditions formelles concernées est prescrit à peine de nullité, ou ;
- l'irrégularité commise a entaché la fiabilité de la preuve, ou ;
- l'usage de la preuve est contraire au droit à un procès équitable ».

⁵¹ Sur le concept « d'information », l'exposé des motifs de la proposition (p. 20), précise que « Vu qu'une distinction a été établie dans la jurisprudence entre les informations permettant d'ouvrir ou d'orienter une enquête d'une part et celles qui visent à prouver les faits d'autre part, et que de ce fait certaines informations ne sont pas considérées comme une preuve et échappent ainsi à un contrôle judiciaire au sens de l'article 32 du Titre préliminaire du Code d'instruction criminelle, la Commission estime que si des informations sont prises en considération par le juge dans son appréciation ou qu'il ressort de l'élaboration de la preuve et de la motivation qu'elles ont joué un rôle dans la décision, ces informations doivent être soumises au même régime qu'une preuve. C'est la raison pour laquelle la réglementation légale utilise le terme "informations", plus large, plutôt que le terme classique de "preuves" ». Voir également plus en détails, pp. 74-76.

⁵² Voir notamment les articles 4, 1., d) et f), 7, 19, 25 et 29 de la directive n° 2016/680. Voir également notamment, les articles 50, 51, 56 et 60 de la LTD.

données à caractère personnel traitées⁵³ (à côté de la nécessité d'en garantir bien entendu également, la confidentialité⁵⁴).

49. En bref, l'Autorité est d'avis qu'il conviendrait d'ajouter aux trois critères cumulatifs précités, celui selon lequel la fiabilité de la preuve n'est pas entachée, ou à tout le moins, est d'avis que l'exposé des motifs devrait préciser duquel de ces critères relèvent les hypothèses où la fiabilité de la preuve est mise en péril⁵⁵.
50. Ceci étant dit, l'Autorité rappelle que les graves violations de la vie privée telles que le recours à un pouvoir intrusif, par le procureur du Roi, nécessitant l'autorisation du juge de l'enquête, *sans l'autorisation* de ce juge, sont systématiquement sanctionnées par une exclusion des débats des informations obtenues sur cette base ainsi que des informations qui en ont été dérivées, et ce en application de l'article 10 de la proposition. L'exposé des motifs de la proposition souligne que « tous les actes d'enquête nécessitant aujourd'hui une décision judiciaire ne pourront dans l'avenir être exécutés que moyennant une autorisation judiciaire »⁵⁶. Une autorisation du juge de l'enquête est notamment nécessaire (sauf exception limitée telle le cas de flagrance) pour les actes d'enquête suivants : le repérage et la localisation des communications électroniques (article 184 de la proposition) ; l'interception, la prise de connaissance, l'exploration et l'enregistrement des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci (articles 185 à 192) ; les perquisitions (articles 205 à 211)⁵⁷.
51. **Droit d'accès au dossier (articles 87, § 4, 216, 229, 232 et 233 ; article 416, § 5).** Le droit d'accès au dossier⁵⁸ peut être rapproché du droit d'accès de la personne concernée en matière de protection des données mais comme les développements suivants l'illustreront, il ne répond toutefois pas à l'ensemble des exigences des articles 14 et 15 de la directive n° 2016/680.

⁵³ Voir en particulier l'article 29, 2., b), c), h), j) de la directive n° 2016/680.

⁵⁴ Pour des hypothèses où les mesures en vue de garantir la confidentialité des données sont particulièrement importantes pour les personnes concernées, voir par exemple articles 193 et s. de la proposition concernant le témoignage anonyme, et les articles 108, 109 et 119 de la proposition, concernant la protection de l'identité de membres de services de police dans certains cas.

⁵⁵ *A priori*, le critère de l'atteinte à l'intégrité de la justice semblerait être ouvert à cette fin mais l'exposé des motifs ne permet pas de l'affirmer (ce critère semble par ailleurs recherché en droit étranger). Selon l'exposé des motifs de la proposition (p. 77) : « Le troisième critère porte sur l'intégrité de la Justice. Il s'inspire de l'article 24 (2) de la Charte canadienne des droits et libertés, qui prévoit que les éléments de preuve sont écartés s'il est établi que leur utilisation est susceptible de déconsidérer l'administration de la justice ou, plus précisément, qu'ils impliquent une violation de l'intégrité de la Justice. Il s'agit d'un principe d'intégrité (integrity principle), que l'on retrouve également dans la jurisprudence anglaise et galloise, comme dans un arrêt de la Chambre des Lords du 8 décembre 2005[...] » (référence omise).

⁵⁶ P. 24.

⁵⁷ Pour la classification des trois types d'actes d'enquête (ceux relevant de la compétence exclusive du procureur du Roi, ceux qui sont mixtes et selon les circonstances nécessitent une autorisation du juge de l'enquête, et enfin, les actes nécessitant toujours une autorisation du juge de l'enquête), voir l'exposé des motifs de la proposition, pp. 25 et s.

⁵⁸ A ce propos, voir l'exposé des motifs de la proposition, pp. 181 et s.

52. L'exposé des motifs de la proposition⁵⁹ explique que le « projet prévoit de moduler les droits et procédures applicables en fonction de la gravité des infractions en cause. Un équilibre doit être recherché, en l'espèce, entre la garantie d'une procédure suffisamment rapide et efficace et la sauvegarde des droits des parties ». A cette fin, concernant l'accès au dossier, une distinction est établie selon que le dossier porte ou non sur des infractions punissables d'une peine privative de liberté.
53. L'article 216 de la proposition constitue la disposition la plus aboutie en matière de droit d'accès au dossier⁶⁰. Il prévoit notamment que la décision du procureur du Roi en la matière est susceptible de faire l'objet d'un recours auprès du juge de l'enquête⁶¹. Pour être complet, cet article est à lire en combinaison avec : l'article 229, § 1^{er} visant la clôture de l'enquête par le procureur du Roi, hypothèse dans laquelle le dossier est automatiquement mis à disposition ; l'article 232 visant l'extinction de l'action publique moyennant le paiement d'une somme d'argent (la transaction pénale), hypothèse dans laquelle l'accès au dossier est également prévue (§ 2, à l'attention du suspect et de la victime) ; l'article 233 visant l'extinction de l'action publique moyennant l'exécution de mesures et le respect de conditions, hypothèse additionnelle où le dossier est encore accessible au suspect et à la victime (§ 2) ; et enfin l'article 87, § 4, alinéa 1^{er} de la proposition dont il sera question ci-après (considérant n° 57).
54. L'accès au dossier consacré dans l'article 216 du projet est soumis en substance, aux conditions suivantes :
- il n'est ouvert qu'au suspect et à la personne lésée⁶² (article 216, § 1^{er})⁶³ ;
 - il n'est applicable que lorsque le dossier porte sur des infractions punissables d'une peine privative de liberté (article 216, § 1^{er}) ;
 - à peine d'irrecevabilité, la requête doit être motivée (article 216, § 2, alinéa 1^{er}) ;
 - elle doit contenir élection de domicile en Belgique si le requérant n'y a pas de domicile, et l'adresse e-mail « éventuelle » à laquelle la décision peut être communiquée (article 216, § 2, alinéa 1^{er}) ;
 - elle ne peut être expédiée (ou déposée) qu'après l'expiration d'un délai d'un mois à partir de la rédaction du premier procès-verbal (article 216, § 2, alinéa 2) ;

⁵⁹ P. 16.

⁶⁰ Voir également l'article 416, § 5, concernant l'enquête pénale d'exécution.

⁶¹ Voir les articles 216, § 5, et 221 de la proposition.

⁶² Selon l'article 70 de la proposition, en substance, acquiert la qualité de personne lésée celle qui déclare avoir subi un dommage découlant d'une infraction (la déclaration doit se faire sur la base d'un formulaire ad hoc et comporter une série d'informations). Et toute personne qui est lésée par une infraction dispose de l'action civile (voir l'article 71 de la proposition). Exerce l'action civile, la partie civile (article 72 de la proposition).

⁶³ Dans le cadre de l'enquête pénale d'exécution, le droit de consulter ou copier le dossier est ouvert au condamné et aux tiers justifiant d'un intérêt. Pour rappel selon l'article 416, § 3, « L'EPE est menée à l'égard de l'auteur condamné, dénommé ci-après "le condamné", et à l'égard de tiers qui conspirent sciemment et volontairement avec le condamné afin de soustraire son patrimoine à l'exécution des condamnations exécutoires ».

- le requérant ne peut avoir adressé (ou déposé) une même requête dans les trois mois à compter de la dernière décision portant sur le même objet (article 216, § 6) ;
- une double condition porte également sur l'intérêt du requérant : en effet, le procureur du Roi peut refuser la consultation si « le requérant ne justifie pas d'un motif légitime pour consulter le dossier » (article 216, § 3, alinéa 1^{er}) ; et il peut limiter la consultation ou la copie à la partie du dossier pour laquelle le requérant « peut justifier d'un intérêt » (article 216, § 3, alinéa 2).

55. Pour le surplus, le procureur du Roi peut refuser la consultation ou la copie du dossier si les nécessités de l'enquête le requièrent, si la consultation présente un danger pour les personnes ou porte gravement atteinte à leur vie privée ou si le dossier ne contient que la déclaration ou la plainte dont le requérant ou son avocat a déjà reçu une copie⁶⁴.

56. L'article 216, § 3, alinéa 3 de la proposition prévoit par ailleurs que la consultation ou la copie du dossier⁶⁵ ne peut en principe plus être refusée lorsque six mois se sont écoulés depuis la rédaction du premier procès-verbal, sauf dans deux hypothèses :

- si le procureur du Roi considère que le requérant n'a pas la qualité de suspect ou de personne lésée, ou
- s'il a obtenu du juge de l'enquête, conformément à l'article 220 de la proposition, une prolongation du caractère secret de l'enquête au motif que l'accès à tout ou partie du dossier pourrait sérieusement compromettre le déroulement de l'enquête ou la protection de personnes.

57. Enfin, l'article 216, § 4, alinéa 2 consacre une restriction à l'utilisation qui peut être faite des « renseignements » obtenus : « Le requérant ne peut faire usage des renseignements obtenus par la consultation ou la copie que dans l'intérêt de sa défense, à la condition de respecter la présomption d'innocence ainsi que les droits de la défense de tiers, la vie privée et la dignité de la personne, sans préjudice du droit prévu à l'article 217 de solliciter l'accomplissement de devoirs complémentaires ».

58. Dans l'hypothèse où le demandeur envisagerait de construire le droit d'accès des personnes concernées sur la base du dispositif juste exposé et prévu principalement par l'article 216 de la proposition (voir plus haut, considérant n° 15), l'Autorité attire son attention sur les quatre commentaires suivants.

⁶⁴ Article 216, § 3, alinéa 1^{er} de la proposition.

⁶⁵ La proposition devrait être clarifiée quant au point de savoir si cette règle s'applique bien également aux dossiers qui portent sur des infractions *qui ne sont pas* punissables d'une peine privative de liberté. En effet, si l'exposé des motifs de la proposition le laisse entendre (p. 183, « Les infractions non punissables d'une peine privative de liberté sont exclues de cette disposition. Cela n'empêche toutefois pas qu'il peut être demandé à consulter le dossier et à en prendre copie par simple requête, sans possibilité de recours, également pour les infractions non punissables d'une peine privative de liberté. *En outre*, il est parti du principe que le droit de consultation est automatiquement accordé six mois après le premier procès-verbal, ce qui permet à toutes les parties de bénéficier, rapidement et sur un pied d'égalité, d'un droit de consultation garanti », italiques ajoutés par l'Autorité), la structure de l'article 216 permet d'en douter. De fait, le paragraphe premier semble bien limiter le champ d'application de l'ensemble de l'article et l'alinéa 3 de son paragraphe 3 n'y déroge pas.

59. Premièrement, en tant que tel, ce droit d'accès au dossier ne vaut que pour le suspect et la personne lésée. Or un dossier pénal est susceptible de concerner d'autres personnes concernées également⁶⁶. Pour ces autres personnes concernées, seul l'article 87, § 4, alinéa 1^{er}⁶⁷ de la proposition est susceptible d'être pertinent. Celui-ci prévoit uniquement que « sans préjudice des articles 216, 229, 232 et 233, le procureur du Roi peut également autoriser une personne justifiant d'un intérêt légitime à prendre connaissance ou copie de tout ou partie des actes de la procédure. Il peut mettre des conditions à cette autorisation. Sa décision n'est pas susceptible d'appel. La personne peut elle-même et par ses propres moyens, en prendre une copie gratuitement, sur place ». Une telle disposition ne répond pas aux exigences consacrées dans les articles 14 et 15 de la directive n° 2016/680, notamment en ce qu'elle ne limite pas les motifs de refus d'accès, ni quant à leur teneur, ni quant à leur nécessité (notamment d'un point de vue temporel).
60. Deuxièmement, c'est ce même article 87, § 4 de la proposition qui s'appliquera lorsque le dossier concerne une infraction qui n'est pas punissable d'une peine privative de liberté. L'exposé des motifs de la proposition⁶⁸ explique que la « disposition en projet se limite aux infractions punissables d'une peine privative de liberté, afin de parvenir à une réglementation réalisable du point de vue de l'économie de procédure ». L'Autorité est d'avis qu'en matière de droit d'accès, une telle limitation systématique ne se justifierait pas. A titre d'illustration, un responsable du traitement (personne physique) qui ferait l'objet d'une enquête pénale ne pourrait que se référer à l'article 87, § 4 de la proposition dès lors que seules des amendes pourraient lui être infligées⁶⁹.
61. Troisièmement, la directive n° 2016/680 ne permet pas de soumettre, sur le plan du principe, le droit d'accès à la condition que la personne concernée justifie d'un intérêt ou motive sa demande, autrement qu'en justifiant de son identité⁷⁰. Une telle motivation ne pourrait être exigée que et dans la mesure où elle apparaîtrait nécessaire à l'appréciation *in concreto*, des motifs visés à l'article 15, 1. de la directive 2016/680.
62. Quatrièmement, les limitations quant à l'utilisation des « renseignements » obtenus ne pourraient pas empêcher la personne concernée d'utiliser ces derniers aux fins de l'exercice de son droit à la protection des données à caractère personnel (p. ex., afin d'obtenir l'éventuelle mise en conformité du traitement de données en question), s'agissant là de la finalité même du droit d'accès : « Une personne physique

⁶⁶ Voir par exemple l'article 6 de la directive n° 2016/680 et l'article 31 de la LTD qui identifient quatre catégories de personnes concernées (dont les victimes et les tiers à l'infraction concernée).

⁶⁷ L'alinéa 2 vise les expéditions et copies des actes d'instruction et de procédure des juridictions et des parquets militaires supprimés concernant des dossiers définitivement jugés ou sur lesquels il a été statué par l'auditeur militaire ou l'auditeur général au 31 décembre 2003.

⁶⁸ P. 183.

⁶⁹ Voir les articles 222 à 227 de la LTD qui ne prévoient pas de peine(s) privative(s) de liberté.

⁷⁰ Voir également l'article 12, 5. de la directive n° 2016/680.

devrait avoir le droit d'accéder aux données qui ont été collectées la concernant et d'exercer ce droit facilement, à des intervalles raisonnables, *afin de prendre connaissance du traitement et d'en vérifier la licéité*. [...] Pour que ce droit soit respecté, il suffit que la personne concernée dispose d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme qui lui permette de prendre connaissance de ces données et *de vérifier si elles sont exactes et traitées conformément à la présente directive, de sorte qu'elle puisse exercer les droits que lui confère la présente directive* » (italiques ajoutés par l'Autorité)⁷¹.

63. **Extension de la recherche dans un système informatique (article 171, § 3).** En la matière, la proposition entend donner suite à l'arrêt n° 174/2018 du 6 décembre 2018 de la Cour constitutionnelle qu'elle avait anticipé. Dans cet arrêt, la Cour constitutionnelle a appliqué les articles 22 de la Constitution et 8 de la CEDH à la loi du 25 décembre 2016⁷², notamment en ce que celle-ci régissait l'extension de la recherche dans un système informatique. La Cour relève⁷³ que « L'extension de la recherche permet aux enquêteurs d'avoir accès non seulement à l'ensemble des données enregistrées ou sauvegardées sur l'appareil qui constitue le point de départ de la recherche, *mais également à tous les documents stockés sur les systèmes informatiques atteints par connexion via cet appareil, ainsi qu'à toutes les communications entretenues par son utilisateur avec des tiers*, en ce compris les nouveaux messages reçus ou en cours de réception dont l'utilisateur n'a pas encore pris connaissance » (italiques ajoutés par l'Autorité). Elle explique ensuite que la modification législative attaquée permet au procureur du Roi de procéder à l'extension de la recherche dans un système informatique sans autorisation du juge d'instruction, alors qu'un tel pouvoir ne devrait pouvoir être autorisé que par le juge d'instruction, au cours d'une instruction eu égard à la gravité de l'ingérence et aux caractères secret et non contradictoire de l'information⁷⁴. La Cour relève encore que le transfert de la compétence du juge d'instruction vers le procureur du Roi n'a pas été assorti de garanties supplémentaires destinées à protéger de manière effective la vie privée et les droits de la défense de la personne concernée et qui soient de nature à compenser la suppression de l'intervention préalable d'un juge indépendant et impartial⁷⁵. La Cour conclut qu'en « raison de la gravité de l'ingérence dans le droit au respect de la vie privée qu'elle implique, la mesure consistant à étendre une recherche dans un système informatique ou une partie de celui-ci, entamée dans un système informatique qui a été saisi ou qui peut être saisi par le procureur du Roi, vers un système informatique ou une partie de celui-ci qui se

⁷¹ Considérant n° 43 de la directive n° 2016/680.

⁷² Loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherches et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales ».

⁷³ Au considérant n° B.11.2. de l'arrêt.

⁷⁴ Voir les considérants nos B.13.1. à B.16.1 de l'arrêt.

⁷⁵ Considérant n° B.16.2. de l'arrêt.

trouve dans un autre lieu que celui où la recherche est effectuée, ne peut être autorisée que dans les mêmes conditions que celles qui concernent les actes d'instructions visés en B.14.2.^[76] ».

64. L'article 171, § 3 de la proposition réglemente désormais l'extension de la recherche informatique et s'aligne sur la jurisprudence juste évoquée en prévoyant la nécessité d'une autorisation du juge de l'enquête et maintien un certain pouvoir du procureur du Roi en cas de flagrant délit⁷⁷. Il s'en écarte toutefois en permettant une possibilité additionnelle d'extension de la recherche dans le système informatique au procureur du Roi et à l'officier de police judiciaire à condition (outre les conditions visées à l'article 171, § 3, alinéa 1^{er} de la proposition) : qu'il ait l'accord écrit et éclairé de l'utilisateur habituel du système informatique ; qu'il ait informé au préalable ce dernier de l'étendue possible de l'extension de la recherche et de sa finalité ; et que l'extension de la recherche présente un caractère ponctuel en lien direct avec l'objet de l'enquête.
65. L'Autorité en prend acte et relève ce qui suit. Elle rappelle qu'un tel accord ne sera pas une base de licéité du traitement de données à caractère personnel en tant que tel⁷⁸ mais qu'il peut en effet bien constituer une certaine garantie, relative eu égard au contexte du traitement (une enquête pénale), pour le suspect concerné. L'Autorité note également qu'une telle garantie ne sera pas une garantie pour *les tiers* (émetteurs d'éventuelles communications, etc.) dont les données à caractère personnel seront traitées dans ce contexte⁷⁹.

⁷⁶ A savoir notamment, les perquisitions et l'interception, la prise de connaissance, l'exploration et l'enregistrement, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci (voir l'article 90^{ter} du Code d'instruction criminelle).

⁷⁷ Quant à la recherche informatique, voir l'exposé des motifs de la proposition, pp. 157-163.

⁷⁸ Considérant n° 35 de la directive n° 2016/680 : « [...] Dans le cadre de l'exécution des missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée, au sens du règlement (UE) 2016/679, ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes. Lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix ; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté. Cela ne devrait pas empêcher les États membres de prévoir par la loi que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de la présente directive, par exemple pour des tests ADN dans des enquêtes pénales ou le suivi de sa localisation au moyen de dispositifs électroniques dans le cadre de l'exécution de sanctions pénales ».

⁷⁹ L'article 171, § 7, de la proposition prévoit que « Sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, le procureur du Roi informe dans les plus brefs délais, *le responsable du système informatique* de la recherche dans le système informatique ou de son extension. Il lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées » (italiques ajoutés par l'Autorité). Pour rappel, dans l'arrêt de la Cour constitutionnelle n° 174/2018 du 6 décembre 2018, la Cour, au considérant n° B.22.2 de son arrêt, juge que « la notion de 'responsable du système informatique' doit être comprise comme désignant la personne ou les personnes responsables des données ou des communications enregistrées sur l'appareil saisi ou qui peut l'être et des données ou des communications dont il peut être pris connaissance via les réseaux qui sont visés par l'extension de la recherche entamée dans l'appareil précité, cette ou ces personnes n'étant pas nécessairement les propriétaires ou les détenteurs des appareils concernés. Comme il est dit en B.15.2., cette notion vise également le suspect dont les données font l'objet de la recherche lorsqu'il n'exerce pas lui-même le contrôle effectif du système informatique concerné ».

66. Enfin, à la page 159 de l'exposé des motifs, troisième paragraphe, version française, les mots « ou l'utilisation de fausses clés » doivent être ajoutés après les mots « mots de passe supplémentaires » afin d'aligner la version française du texte sur sa version néerlandaise (« *of valse sleutels gebruikt* »).

PAR CES MOTIFS,

Compte-tenu du fait que la proposition soumise pour avis est incomplète concernant le traitement de données à caractère personnel dans le contexte de la procédure pénale, son analyse, qui est par conséquent non exhaustive et pour partie prématurée, se limite à l'une et l'autre de ses dispositions pertinentes en matière de protection des données (**considérants nos 20-26**) ;

1. Lacunes du droit positif. L'Autorité rappelle que, si elle est compétente, dans le cadre du processus d'adoption d'une norme législative ou réglementaire, pour rendre un avis concernant une réglementation telle que la proposition de Code de procédure pénale, en droit positif, aucune autorité n'est compétente pour contrôler *in concreto* la conformité des traitements dont sont responsables les autorités judiciaires, pénales en l'occurrence, aux règles de protection des données (**considérants nos 7-14**). Il s'agit d'une lacune importante du droit belge qui sur ce point, manque à l'article 8, 3. de la Charte des droits fondamentaux de l'Union européenne.

Une telle lacune a également pour effet, comme le met en évidence l'exposé des motifs de la proposition, qu'il n'est pas possible de prévoir que les personnes concernées exercent leurs droits par l'intermédiaire de l'autorité de contrôle compétente (**considérants nos 15-17**).

L'autorité est d'avis que le demandeur doit combler cette lacune.

2. Responsables du traitement et finalités. L'Autorité souligne qu'en exécution des principes de transparence et de légalité (**considérant n° 27**), la proposition devra identifier explicitement les responsables des traitements et les finalités de ces derniers.

En particulier en l'espèce, elle confirmera tout d'abord, le cas échéant, que le procureur du Roi est le responsable du traitement des données nécessaires aux fins de **l'enquête** et de l'exercice de l'action publique, dans l'exécution des pouvoirs, compétences et obligations dont il dispose et est débiteur dans le présent Code (**considérant n° 30**).

Elle identifiera également l'éventuelle responsabilité autonome au regard du traitement (ou conjointe, le cas échéant avec une autre autorité publique) des **officiers de police judiciaire (considérants nos 31-32)**.

Il en ira encore de même pour ce qui concerne le contexte de **l'enquête pénale d'exécution**, et les responsabilités du magistrat EPE ainsi que, le cas échéant, du magistrat de l'Organe central pour la saisie et la confiscation (**considérants nos 33-34**).

Enfin, eu égard à l'exposé des motifs de la proposition concernant le **registre d'écrou**, cette dernière devra articuler son article 487 avec les dispositions pertinentes de la loi du 5 mai 2019 portant dispositions diverses en matière d'informatisation de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés (qui notamment, crée la banque de données Sidis-Suite), de manière telle que tant les finalités, que les données et le responsable du traitement (ou les responsables conjoints du traitement) concernés par le traitement visé à l'article 487, soient clairement identifiés (**considérants nos 35-40**).

3. Droit à la protection des données. Le droit à la protection des données étant un droit fondamental autonome et à tout le moins aussi pertinent, dans le cadre de la procédure pénale, que celui au droit à la vie privée, l'Autorité est d'avis qu'il convient de s'y référer dans l'article 1^{er} de la proposition (**considérants nos 41-43**).

4. Droit à la protection des données et admissibilité de la preuve. Dans le même sens, concernant le régime d'exclusion relative de la preuve mis en place par la proposition, en vue d'une protection efficace des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre de la procédure pénale, l'Autorité est d'avis qu'il conviendrait de faire référence au droit à la protection des données dans l'article 11 de la proposition, et de s'assurer que les cas où l'irrégularité commise a entaché la fiabilité de la preuve continuent d'entraîner, comme en droit positif, une exclusion des informations concernées (**considérants nos 44-50**).

5. Droit d'accès au dossier. Tel qu'actuellement organisé dans la proposition, le droit d'accès au dossier pénal ne répond pas à l'ensemble des exigences consacrées dans les articles 14 et 15 de la directive n° 2016/680. L'Autorité relève certains points à l'attention du demandeur dans l'hypothèse où il envisagerait de construire le droit d'accès de la personne concernée sur cette base (**considérants nos 51-62**).

6. Extension de la recherche (non secrète) dans un système informatique. L'Autorité prend acte des modifications apportées par la proposition, dans la suite de l'arrêt rendu par

Avis 77/2020 - 24/24

la Cour constitutionnelle en la matière et relève seulement que l'accord de l'utilisateur habituel du système ne constitue pas en lui-même, une garantie pour le respect des droits des tiers dont les données sont concernées par l'extension de la recherche (**considérants nos 63-65**). Enfin, à la page 159 de l'exposé des motifs, troisième paragraphe, version française, les mots « ou l'utilisation de fausses clés » doivent être ajoutés après les mots « mots de passe supplémentaires » afin d'aligner la version française du texte sur sa version néerlandaise (« *of valse sleutels gebruikt* ») (**considérant n° 66**).



Alexandra Jaspar
Directrice du Centre de Connaissances





Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 77/2020 van 24 augustus 2020

Betreft: Adviesaanvraag over een wetsvoorstel houdende het Wetboek van Strafprocesrecht (CO-A-2020-059)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid op artikel 23 en 26 (hierna "WOG");

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verzoek om advies van de heer Patrick Dewael, Voorzitter van de Kamer van Volksvertegenwoordigers, ontvangen op 16 juli 2020;

Gelet op het verslag van mevrouw Alexandra Jaspar, Directeur van het Kenniscentrum van de Gegevensbeschermingsautoriteit ;

Brengt op 24 augustus 2020 het volgende advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De Voorzitter van de Kamer van Volksvertegenwoordigers verzoekt de Autoriteit om advies over een wetsvoorstel houdende het Wetboek van Strafprocesrecht (CO-A-2020-059) (hierna "het voorstel"). Dit voorstel is het resultaat van een hervormingsproces van het strafrecht dat werd opgestart bij ministerieel besluit van 30 oktober 2015 dat overeenkomstig het Regeerakkoord van 10 oktober 2014, twee multidisciplinair samengestelde commissies aanstelde: De ene commissie werd belast met de hervorming van het strafrecht, terwijl de andere commissie werd belast met de hervorming van het strafprocesrecht. Deze adviesaanvraag handelt over de resultaten van de werkzaamheden van deze tweede commissie.
2. In het kort overgenomen uit de toelichting bij het voorstel, aangezien het onmogelijk is om hier en in al zijn aspecten de ondernomen hervorming samen te vatten, heeft het voorstel het hiernavolgende doel. Het stelt één type van onderzoek in [a charge en a décharge¹] onder de leiding van het openbaar ministerie en onder de controle van een rechter [onderzoeksrechter], die echter niet langer zelf het onderzoek zal leiden maar die tegelijk zal worden versterkt in zijn controlerende en rechtsprekende functie ten aanzien van het vooronderzoek.² Bijgevolg maakt de hervorming een einde aan de verschillen in garanties voor de bescherming van de rechten van de verdediging van de rechtsonderhorigen die voortvloeien uit de verschillen tussen de regels inzake het opsporings- en gerechtelijk onderzoek, en wordt gestreefd naar consistentie in de strafprocedure.
3. Het schaft ook de mogelijkheid af om de strafvordering in te stellen door een klacht met burgerlijke partijstelling in te dienen bij de onderzoeksrechter en vervangt het door een alternatief systeem met inbegrip van een beroep voor de kamer van het onderzoek (momenteel de kamer van inbeschuldigingstelling) tegen een seponering door het openbaar ministerie³, wat de slachtoffers een blijvende rechtsbescherming moet garanderen⁴.
4. Hoewel de instelling van onderzoeksrecht verdwijnt, benadrukt het voorstel het volgende "De voorafgaande machtiging van die rechter [onderzoeksrechter] zal uiteraard nog steeds vereist zijn voor alle maatregelen die dwang impliceren en die momenteel aan rechterlijke controle onderworpen zijn" en "En zelfs meer nog, vermits bepaalde intrusieve maatregelen die kunnen of konden worden bevolen door het parket (zoals infiltratie en systematische observatie gedurende meer dan vijf dagen of met technische middelen of de uitbreiding van de zoeking in een informaticasysteem tot buiten de in beslag

¹ Zie de Toelichting, blz. 11 ev.

² Toelichting bij het voorstel, blz 6.

³ Zie hierover de Toelichting bij het voorstel, blz 15.

⁴ Toelichting bij het voorstel, blz. 6.

genomen drager) voortaan ter goedkeuring aan de rechter zouden worden voorgelegd"⁵. En dit blijkt nu van zeer groot belang te zijn op het gebied van het grondrecht op privacy en gegevensbescherming.

5. Tot slot moet worden opgemerkt dat niet alle huidige bepalingen van het Wetboek van Strafvordering waaronder de bepalingen betreffende het centrale strafregister, het uitwissen van veroordelingen en het herstel in eer en rechten in strafzaken, in het voorgestelde Wetboek van Strafrecht zijn opgenomen⁶. De toelichting bij het voorstel legt uit dat deze bepalingen betrekking hebben op "het herinneren en vergeten van straffen", en logischerwijze veeleer thuishoren in een Wetboek van Strafvordering of in bijzondere wetten⁷.
6. In dit advies wordt eerst ingegaan op de kwestie van de bevoegdheid van de Autoriteit (II) en vervolgens wordt de reikwijdte van de uitgevoerde analyse toegelicht (III). Uiteindelijk volgt deze laatste (IV).

II. BEVOEGDHEID VAN DE AUTORITEIT

7. Op het gebied van de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, is artikel 45.2 van de Richtlijn (EU) nr. 2016/680⁸ van toepassing. Richtlijn nr. 2016/680 bepaalt: "*Elke lidstaat schrijft voor dat elke toezichthoudende autoriteit belast is met het toezicht op verwerkingen door gerechten in het kader van hun rechterlijke taken. De lidstaten mogen bepalen dat hun toezichthoudende autoriteit niet bevoegd is om toe te zien op de verwerkingen door andere onafhankelijke autoriteiten bij de uitoefening van hun rechterlijke taken*" (italic toegevoegd door de Autoriteit)⁹.
8. Overweging 80 van deze richtlijn legt uit dat : "Hoewel deze richtlijn ook van toepassing is op de activiteiten van nationale gerechten en andere rechterlijke autoriteiten, dient *de competentie* van de toezichthoudende autoriteiten zich niet uit te strekken tot de verwerking van persoonsgegevens door gerechten in het kader van hun taken, teneinde de *onafhankelijkheid, van rechters bij de uitvoering van hun gerechtelijke taken te vrijwaren*. Die vrijstelling dient beperkt *te blijven tot gerechtelijke activiteiten in het kader van rechtszaken* en niet te gelden voor andere activiteiten die rechters

⁵ Toelichting bij het voorstel, blz. 9 en voetnoot blz. 10.

⁶ Zie ook de Toelichting bij het voorstel, blz. 350.

⁷ Blz. 351.

⁸ Richtlijn (EU) nr. 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

⁹ Artikel 55, 2 van de AVG bepaalt eveneens dat "toezichthoudende autoriteiten niet bevoegd zijn om *toe te zien op verwerkingen door gerechten bij de uitoefening van hun rechterlijke taken*" (italic toegevoegd door de Autoriteit).

Advies 77/2020 4/25

overeenkomstig het lidstatelijke recht verrichten. De lidstaten moeten ook kunnen bepalen dat de bevoegdheid van de toezichthoudende autoriteit zich niet uitstrekt tot de verwerking van persoonsgegevens door andere *onafhankelijke rechterlijke autoriteiten in het kader van hun gerechtelijke taken*, bijvoorbeeld het openbaar ministerie. De naleving van de regels van deze richtlijn door gerechten en andere onafhankelijke rechterlijke autoriteiten is in elk geval altijd onderworpen aan onafhankelijk toezicht in overeenstemming met artikel 8, lid 3, van het Handvest" (italic toegevoegd door de Autoriteit)¹⁰.

9. Artikel 28.2 van de richtlijn nr. 2016/680 bepaalt: "De lidstaten voorzien erin dat de toezichthoudende autoriteit wordt geraadpleegd bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking".
10. In Belgisch recht bepaalt artikel 4, § 1, lid 2 van de WOG "Het *toezicht dat door deze wet wordt georganiseerd heeft geen betrekking op de verwerkingen door de hoven en rechtbanken* alsook door het openbaar ministerie bij de uitoefening van hun gerechtelijke taken" (italic toegevoegd door de Autoriteit). In de toelichting bij het ontwerp WOG wordt deze bepaling als volgt uitgelegd "België maakt hierbij gebruik van de marge die de Verordening 2016/679 biedt om te verduidelijken dat deze *onbevoegdheid* zich ook uitstrekt tot het openbaar ministerie voor het geheel van haar opdrachten, zowel wat betreft haar strafrechtelijke als burgerrechtelijke taken. Het begrip "bij de uitoefening van hun gerechtelijke taken" moet overigens ruim worden geïnterpreteerd teneinde een uniforme toepassing van deze uitsluiting te waarborgen. Zo moet bijvoorbeeld de verwerking van gegevens in het kader van het personeelsbeheer van deze gerechtelijke autoriteiten ook begrepen worden als behorende tot verwerkingen die noodzakelijk zijn voor de uitoefening van hun rechterlijke taken"¹¹ (italic toegevoegd door de Autoriteit).
11. Deze uitsluiting van de bevoegdheid van de toezichthoudende autoriteit met betrekking tot verwerkingen in verband met de gerechtelijke taken verwijst naar "toezicht" op de "verwerkingen" op dit gebied, om de onafhankelijkheid van de rechterlijke macht te waarborgen, en niet naar "elke bevoegdheid" van de Autoriteit met betrekking tot strafzaken in het algemeen. Met andere woorden, het staat de bevoegdheid niet in de weg om zich uit te spreken over wetgeving zoals die welke in het

¹⁰ Overweging nr. 20 van de AVG bepaalt dat "hoewel de onderhavige verordening onder meer van toepassing is op de activiteiten van gerechten en andere rechterlijke autoriteiten, zouden in het Unierecht of het lidstatelijke recht de verwerkingen en verwerkingsprocedures met betrekking tot het verwerken van persoonsgegevens door gerechten en andere rechterlijke autoriteiten nader kunnen worden gespecificeerd. De competentie van de toezichthoudende autoriteiten mag zich niet uitstrekken tot de verwerking van persoonsgegevens door gerechten in het kader van hun gerechtelijke taken, zulks teneinde *de onafhankelijkheid van de rechterlijke macht bij de uitoefening van haar rechterlijke taken, waaronder besluitvorming, te waarborgen*. Het toezicht op die gegevensverwerkingen moet kunnen worden toevertrouwd aan specifieke instanties binnen de rechterlijke organisatie van de lidstaat, die met name de naleving van de regels van deze verordening moeten garanderen, leden van de rechterlijke macht van hun verplichtingen krachtens deze verordening sterker bewust moeten maken, en klachten met betrekking tot die gegevensverwerkingen moeten behandelen" (italic toegevoegd door de Autoriteit).

¹¹ Parl. ST. 2016-2017, Kamer van Volksvertegenwoordigers, Doc. (54) n° 2648/001 blz. 13-14.

onderhavige geval aan de orde is - het wetboek van strafprocesrecht - die de kern van de rechterlijke taken" vormt.

12. Het gaat er in de eerste plaats niet om een verwerking door het openbaar ministerie of een rechtbank te controleren *in concreto*, maar om een advies uit te brengen over een handeling van de wetgever, dat wil zeggen een handeling die onder de wetgevende taken (wetgevende macht) valt. En ten tweede kan de uitoefening van een adviserende bevoegdheid in het wetgevingsproces geen invloed hebben op de onafhankelijkheid van de rechterlijke macht bij de uitoefening van haar taken op het gebied van vervolging en berechting: zij staan elkaar niet in de weg.
13. Bijgevolg is de Autoriteit bevoegd om het voor advies ingediende voorstel te analyseren ingevolge artikel 4, § 2, lid 2 van de WOG waarin de residuele bevoegdheid van de Autoriteit is vastgelegd: "De Gegevensbeschermingsautoriteit is de bevoegde toezichthoudende autoriteit wanneer geen andere wet anders bepaalt".
14. Bovengenoemde overwegingen bieden de gelegenheid om eraan te herinneren dat in het positief recht geen enkele autoriteit bevoegd is om de naleving van de regels inzake gegevensbescherming te controleren bij verwerkingen waarvoor de gerechtelijke autoriteiten, in dit geval de strafrechtelijke autoriteiten, verantwoordelijk zijn. Dit is een belangrijke leemte in de Belgische wetgeving. Ter herinnering: artikel 8.3 van het Handvest van de grondrechten van de Europese Unie zelf bepaalt dat de naleving van de regels inzake gegevensbescherming door een onafhankelijke autoriteit moet worden gecontroleerd.

III. TOEPASSINGSGEBIED VAN HET ADVIES

15. De Toelichting bij het voorstel¹² herinnert eraan dat hier Titel 2 van de WVG¹³, die de omzetting is van de richtlijn nr. 2016/680, van toepassing is. Artikel 37, § 4 van de WVG bepaalt dat:

"De rechten bedoeld in dit hoofdstuk, voor wat betreft de gegevensverwerkingen van de hoven en rechtbanken van het gemeen recht en het openbaar ministerie, *worden uitsluitend uitgeoefend binnen de grenzen en conform de regels en nadere regels van het Gerechtelijk Wetboek, het, Wetboek van strafvordering, de bijzondere wetten die betrekking hebben op de strafrechtspleging* en de uitvoeringsbesluiten ervan (italic toegevoegd door de Autoriteit).

¹² Blz. 56.

¹³ Zie artikel 27 van de WVG.

16. Het gaat om het recht op informatie van de betrokkene¹⁴, het recht op toegang¹⁵, het recht op rectificatie, het recht om onjuiste gegevens aan te vullen of te verwijderen¹⁶, rechten die krachtens artikel 41, lid 1, van het WVG, indien de wet (decreet of verordening) daarin voorziet, in wezen via de bevoegde toezichthoudende autoriteit kunnen worden uitgeoefend. In een dergelijk geval dient de verwerkingsverantwoordelijke overeenkomstig lid 2 van hetzelfde artikel de betrokkene ervan in kennis te stellen dat hij zijn rechten uitoefent via de bevoegde toezichthoudende autoriteit.
17. Wat dit laatste punt betreft, wordt echter noch in het materiële recht, zoals zojuist in herinnering is gebracht (overweging 14), noch in het voor advies ingediende voorstel, een bevoegde autoriteit voor dit doel aangewezen.
18. Artikel 44 van de WVG bepaalt verder:
- "Wanneer de persoonsgegevens in een rechterlijke beslissing of een gerechtelijk dossier zijn opgenomen of in het *kader van strafrechtelijke onderzoeken en procedures worden verwerkt*, worden de in de artikelen 37, 38, § 1, 39 en 41, tweede lid, *bedoelde rechten* uitgeoefend overeenkomstig het *Gerechtelijk Wetboek*, het *Wetboek van strafvordering*, de *bijzondere wetten die betrekking hebben op de strafrechtspleging en de uitvoeringsbesluiten ervan*".
19. Ten slotte voorziet artikel 210 van de WVG met betrekking tot het verbod van artikel 210 van de WVG in het volgende:
- "Vanaf het moment dat de verwerking bedoeld in artikel 209, persoonsgegevens betreft die worden verwerkt in de *loop van een opsporingsonderzoek, van een gerechtelijk onderzoek, een strafrechtelijke procedure* voor de bodemrechter of een procedure voor de uitvoering van een strafrechtelijk vonnis, behoort de beslissing over de rectificatie, de wissing of het verbod op gebruik van de persoonsgegevens, of de beperking van de verwerking, echter uitsluitend, *naar gelang de fase van de procedure, tot het openbaar ministerie* of de bevoegde strafrechter" (italic toegevoegd door de Autoriteit).
20. In deze wetgevingscontext wordt in de toelichting bij het voorstel¹⁷ echter meer in het algemeen benadrukt dat het "aspect van de verwerking van persoonsgegevens nog niet in het ontwerp van het wetboek van strafprocesrecht is opgenomen".

¹⁴ Artikel 37 WVG.

¹⁵ Artikel 38 WVG.

¹⁶ Artikel 39 WVG.

¹⁷ Blz. 56.

21. Wat de rechten van de betrokkene betreft, wordt in de toelichting bij het voorstel het volgende uiteengezet en erkend¹⁸.

In het raam van het huidige opsporingsonderzoek bestaat enkel het recht tot inzage en het nemen van een afschrift van het strafdossier (artikel 21bis Sv.) evenals het recht om de opheffing te vragen van een opsporingshandeling in hoofde van een persoon die daardoor geschaad wordt met betrekking tot zijn goederen (art. 28sexies Sv.). Voor de uitoefening van de rechten van een persoon wiens persoonsgegevens worden verwerkt in het raam van een opsporingsonderzoek, inzonderheid indien het bijvoorbeeld gaat om een vraag tot aanvulling, verbetering of het wissen vandie gegevens, zijn de regels van het huidige Wetboek van Strafvordering ontoereikend.

Zoals aangegeven wordt met dit ontwerp van wetboek van strafprocesrecht één enkele vorm van vooronderzoek onder leiding van het Openbaar Ministerie ingevoerd. De betrokken verdachten en benadeelden hebben dezelfde rechten, met inbegrip van het recht om een nader onderzoek te verzoeken. Elk recht is bovendien gekoppeld aan de mogelijkheid om in beroep te gaan bij de rechter tegen de weigering of het niet-handelen van het openbaar ministerie. Er wordt verwezen naar het onderzoek van Titel IV dat gewijd is aan de rechten van de betrokkenene gedurende het onderzoek. *De omzetting van de rechten van een persoon wiens persoonsgegevens worden verwerkt, vereist een relatief kleine ingreep in het voorgestelde systeem.*

Gelet op de inhoud van artikel 41 van voornoemde wet van 30 juli 2018 wordt niettemin *aanbevolen om het standpunt van de wetgever te kennen over de eventuele oprichting van een bevoegde toezichthoudende autoriteit alvorens over te gaan tot de aanpassing van het ontwerp.* De in de punten 1, 2 en 5 genoemde weigeringsgronden komen grotendeels overeen met de weigeringsgronden die van toepassing zijn op de uitoefening van de rechten van de betrokkenen tijdens het strafrechtelijk onderzoek, waardoor het verzoek tot oprichting van een toezichthoudende autoriteit van het grootste belang is" (italic toegevoegd door de Autoriteit).

22. De Autoriteit neemt daarom nota van het feit dat het voorstel onvolledig is wat betreft de bescherming van persoonsgegevens en met name wat betreft de rechten van de betrokkenen en de aanwijzing van een bevoegde toezichthoudende autoriteit om het openbaar ministerie en de bij strafrechtelijke procedures betrokken rechtbanken en gerechtshoven te controleren. De Autoriteit gaat er dan ook van uit dat zij hierover opnieuw zal worden geraadpleegd.

¹⁸ Blz. 57-58.

Advies 77/2020 8/25

23. Voor het overige beletten deze leemtes de Autoriteit niet om dit voorstel in overweging te nemen. In de eerste plaats heeft het voorstel ondanks deze tekortkomingen toch betrekking op de toegang tot het dossier, zoals zojuist vermeld in de geciteerde toelichting (hierboven, overweging 21). Toegegeven, hoewel de toegang tot het dossier in strafzaken niet werd uitgedacht vanuit het oogpunt van de bescherming van persoonsgegevens (dit vloeit veeleer voort uit de rechten van de verdediging en het recht op een doeltreffende voorziening in rechte), leidt de gelijkenis ervan met het recht op toegang ertoe dat wij er aandacht aan besteden, zeker in het licht van artikel 44 van de WVG¹⁹.
24. Ten tweede, en meer in het algemeen, kan niet *a priori* worden uitgesloten dat het voorstel toch gevolgen heeft voor de verwerking van persoonsgegevens, hetzij door het opstellen of wijzigen van regels voor gegevensverkeer of databanken die dergelijke gegevens bevatten, hetzij door het wijzigen of opstellen van regels voor de bevoegdheden van de bevoegde autoriteiten in het kader van strafrechtelijke procedures, en in dit geval voornamelijk van het openbaar ministerie. Ter herinnering voor wat dit laatste punt betreft, bepalen artikel 8.2 van de richtlijn nr. 2016/680, samen gelezen met 1 van ditzelfde artikel en artikel 33 van de WVG²⁰ "In het lidstatelijke recht dat verwerking binnen het toepassingsgebied van deze richtlijn regelt, worden ten minste de verwerkingsdoeleinden, de te verwerken persoonsgegevens en de doeleinden van de verwerking gespecificeerd". Dergelijke regels hebben rechtstreeks betrekking op het snijpunt van het grondrecht op privacy (vastgelegd in artikel 8 van het EVRM, artikel 22 van de Grondwet en artikel 7 van het Handvest van de grondrechten van de Europese Unie) en gegevensbescherming (vastgelegd in artikel 8 van het Handvest van de grondrechten van de Europese Unie), en vereisen toezicht door de Autoriteit²¹.
25. Meer in het algemeen bevraagd naar mogelijke ontwikkelingen in de wetgeving als gevolg van het nieuwe wetboek van strafprocesrecht die gevolgen kunnen hebben voor de bescherming van persoonsgegevens, antwoordde de aanvrager in het bijzonder het volgende :

*«Het wetsvoorstel houdende het Wetboek van Strafprocesrecht (DOC 55 1239/001) bevat in essentie **geen enkele nieuwe transfer van persoonsgegevens of databanken**.*

¹⁹ Er zou kunnen worden overwogen om het recht van toegang op het gebied van gegevensbescherming vast te stellen op basis van de regels voor de toegang tot het dossier.

²⁰ Dat bepaalt: "§ 1 De verwerking is rechtmatig indien :

1° ze noodzakelijk is voor de uitvoering van een opdracht uitgevoerd door een overheid bevoegd voor de in artikel 27, bedoelde doeleinden; en

2° ze gebaseerd is op een wettelijke of reglementaire verplichting.

§ 2. De wettelijke of reglementaire verplichting regelt ten minste de categorieën van persoonsgegevens die verwerkt moeten worden en de doeleinden van de verwerking".

²¹ Zie bijvoorbeeld voor een gelijkaardige benadering het Advies nr. 21/2016 van 18 mei 2016 over het voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties.

Advies 77/2020 9/25

Het vergroot de rechten van de partijen betrokken in het strafonderzoek, maar het verleent wel een ruimere bevoegdheid aan de rechter van het onderzoek die een rol speelt over het ganse strafonderzoek en niet meer zoals de onderzoeksrechter enkel over een aantal dossiers die in onderzoek worden gesteld.

In essentie is er, wat de eigenlijke verwerking van persoonsgegevens betreft, geen fundamenteel verschil met de huidige strafrechtspleging » (vet in de tekst).

26. In een dergelijke context zal de Autoriteit haar analyse beperken tot enkele bepalingen die - aangezien het niet hoofdzakelijk gaat om codificaties in de vaste wetgeving van reeds bestaande regels in het Wetboek van Strafvordering - waarschijnlijk van invloed zullen zijn op de gegevensbescherming. Zij zal in haar analyse niet alle kwesties opsommen die nog moeten worden aangepakt op het gebied van gegevensbescherming in het kader van strafrechtelijke procedures.

IV. ONDERZOEK

IV.1. Transparantie- en rechtmatigheidsbeginselen: doeleinden en verwerkingsverantwoordelijken

27. . Herhaling van de principes²². Overeenkomstig artikel 8.2. van richtlijn nr. 2016/680, gelezen in samenhang met artikel 22 van de Grondwet en artikel 8 van de EVRM, moet een norm voor de wettelijke rangorde de essentiële elementen bepalen van een gegevensverwerking die nodig is voor de uitvoering van een taak van algemeen belang of voor de uitoefening van het openbaar gezag die aan de verwerkingsverantwoordelijke is opgedragen. Wanneer de verwerking van gegevens een wezenlijke inbreuk vormt op de rechten en vrijheden van de betrokkenen, wat het geval is bij gegevensverwerking die voortvloeit uit de toepassing door het Openbaar Ministerie van de strafprocesregels - die zijn bevoegdheden inzake preventie en opsporing van strafbare feiten regelen - moeten de volgende essentiële elementen worden vastgesteld door wetgever: het)(de) precieze doeleinde(n)²³, waarvan bij lezing reeds kan worden afgeleid welke gegevensverwerkingsverrichtingen zullen worden ingevoerd voor de verwezenlijking ervan, de identiteit van de verwerkingsverantwoordelijke(n), het soort gegevens die noodzakelijk zijn voor de verwezenlijking van (dit) (deze) doeleinde(n), de bewaartermijn van de gegevens²⁴, de categorieën betrokkenen van wie de gegevens zullen worden verwerkt, de instanties of categorieën instanties belast met een opdracht van algemeen belang (of belast met het openbaar gezag) die onder dit doeleinde of doeleinden vallen

²² Er zijn ook beginselen van wettigheid en voorspelbaarheid die specifiek van toepassing zijn op de strafrechtelijke procedure overeenkomstig artikel 12, lid 2, van de Grondwet.

²³ Het Grondwettelijk Hof heeft erkend dat "de wetgever (...) de bewaring van persoonsgegevens en de duur van die bewaring op een algemene wijze (vermocht) te regelen", Arrest nr. 29/2018 van 15 maart 2018, punt B.23.

²⁴ Zie ook artikel 6.3. van de AVG.

Advies 77/2020 10/25

en die toegang hebben tot deze databank en ook de eventuele beperking van de verplichtingen van de verwerkingsverantwoordelijke en/of rechten van de betrokkenen bedoeld in de richtlijn nr. 2016/680. In het licht van deze beginselen en de beperkingen van de analyse van de Autoriteit (zie overweging 26) roept het voorstel de volgende opmerkingen op.

28. **Concept Verwerkingsverantwoordelijke** Wat de verwerkingsverantwoordelijke betreft, bepaalt artikel 26, 8° van de WVG zelf²⁵ het volgende: "indien het doel en de middelen voor de verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, de verantwoordelijke voor de verwerking diegene is die door of krachtens de wet, het decreet of de ordonnantie als dusdanig wordt aangewezen". Wat het begrip "verwerkingsverantwoordelijke" betreft, heeft de Autoriteit reeds kunnen herhalen dat dit begrip vanuit een feitelijk perspectief moet worden benaderd. Het is derhalve noodzakelijk de entiteit of entiteiten aan te wijzen die in feite het doel van de verwerking nastreven en de controle erover uitoefenen. In de overheidssector is de verwerkingsverantwoordelijke gewoonlijk het orgaan dat belast is met de openbare dienstverleningstaak waarvoor de gegevensverwerking is opgezet.
29. Overigens is de bedoeling van een brede definitie van het concept verwerkingsverantwoordelijke²⁶ een efficiënte en volledige bescherming te verzekeren van de betrokkenen²⁷. Afhankelijk van de feiten kan een gezamenlijke verwerkingsverantwoordelijkheid meerdere actoren binden, waarbij de betrokkene zijn of haar rechten ten opzichte van en tegen elk van hen kan uitoefenen²⁸. Dit gezegd zijnde, « het bestaan van een gezamenlijke verantwoordelijkheid uit zich niet noodzakelijkerwijs in een gelijkwaardige verantwoordelijkheid [... en] deze actoren kunnen juist in verschillende stadia en in verschillende mate bij deze verwerking betrokken zijn, zodat het niveau van verantwoordelijkheid van elk van hen moet worden beoordeeld in het licht van alle relevante omstandigheden van het geval »²⁹. Het is « in het kader van zijn verantwoordelijkheden, zijn bevoegdheden en zijn mogelijkheden » dat de medeverantwoordelijke zal waken over de conformiteit van zijn activiteit met de regels inzake gegevensbescherming³⁰.

²⁵ Zie ook artikel 3, 8° van de Richtlijn 2016/680.

²⁶ De begrippen verwerkingsverantwoordelijke en verwerker zijn gedefinieerd in artikelen 4, 7), en 8), van de AVG. Lees eveneens het Advies G29, nr. 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", (WP169), 16 februari 2010.

²⁷ EHvJ, (Gr. Kam.), 13 mei 2014 (GOOGLE SPAIN SL, GOOGLE INC. v/ AEPD), aff. C-132/12, punt 34. EHvJ, (Gr. Kam.), 5 juni 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN v/ Wirtschaftsakademie SCHLESWIG-HOLSTEIN GmbH), aff. C-210/16, punt 16.

²⁸ Artikel 26, 3., AVG.

²⁹ EHvJ, (Gr. Kam.), 5 juni 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN v/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GmbH), aff. C-210/16, punt 16. Lees eveneens het Advies G29, 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, p. 20.

³⁰ EHvJ, (Gr. Kam.), 13 mei 2014 (GOOGLE SPAIN SL, GOOGLE INC. v/ AEPD), aff. C-132/12, punt 38.

30. **Het onderzoek en de strafvordering (artikelen 85, 101 en 103).** Het voorstel bepaalt duidelijk dat het onderzoek (dat in artikel 85, 1ste lid wordt gedefinieerd) "wordt gevoerd onder de leiding en het gezag van de bevoegde procureur des Konings. Hij draagt hiervoor de verantwoordelijkheid"³¹, en de "procureur des Konings waakt over de wettigheid van de bewijsmiddelen en de loyaliteit waarmee de bewijzen worden verzameld"³². Artikel 2 bepaalt voorts dat het openbaar ministerie onafhankelijk, in naam van de maatschappij en in het algemeen belang handelt, met inachtneming van de in artikel 1 van het voorstel bedoelde rechten, en dat het openbaar ministerie geen instructies of richtlijnen mag ontvangen met betrekking tot het onderzoek van een individueel geval³³. Met andere woorden, bij de bespreking van de gegevensbeschermingsaspecten zal het voorstel duidelijk maken dat de procureur des Konings de persoon is die verantwoordelijk is voor de verwerking van de gegevens die nodig zijn voor het onderzoek en de uitoefening van de strafvordering, in de uitvoering van de bevoegdheden, competenties en verplichtingen die hij heeft en waaraan hij gebonden is door dit Wetboek.
31. In het voorstel zal ook duidelijk moeten worden aangegeven of los van het opsporingsonderzoek van de procureur des Konings/openbaar ministerie er andere gevallen bestaan waarin andere overheden de bevoegdheden autonoom kunnen uitoefenen die het voorstel aan hen zou toekennen. De Autoriteit vestigt met name de aandacht van de auteur van het voorstel op de bevoegdheden die de gerechtelijke politie autonoom zou kunnen uitoefenen. Indien het openbaar ministerie het recht heeft om de officieren van gerechtelijke politie (en de politiediensten) te verzoeken de voor het onderzoek noodzakelijke gerechtelijke politiehandelingen te verrichten (artikel 101, § 1, van het voorstel), lijkt het erop dat deze officieren ook autonome bevoegdheden hebben (zie bijvoorbeeld artikel 150 van het voorstel, betreffende de snelle bewaring van informaticagegevens, en artikel 171, betreffende de zoeking in een informaticasysteem). Indien deze officieren kunnen optreden buiten het geval van een onderzoek onder de verantwoordelijkheid van de procureur des Konings, moet een norm van de rangorde van de wet duidelijk hun eventuele autonome (of gezamenlijke) verantwoordelijkheid aangeven of in ieder geval die van de autoriteit waartoe zij behoren.
32. De Autoriteit gaat er in dit verband van uit dat er in voorkomend geval sprake zal zijn van een mogelijke verantwoordelijkheid (gezamenlijk, afhankelijk van de autonomie van de gerechtelijke politieagenten) van de procureur-generaal bij het Hof van Beroep of de federale procureur-generaal. Artikel 130, § 1 van het voorstel bepaalt immers "Alle officieren van gerechtelijke politie staan onder toezicht van, al naar gelang van het door de wet gemaakte onderscheid, de procureur-generaal bij het hof van beroep of de federale procureur. Al degenen die, volgens artikel 107, uit hoofde van een

³¹ Artikel 85, lid 2 van het voorstel.

³² Artikel 85, lid 3 van het voorstel.

³³ Wat deze onafhankelijkheid betreft, wordt in het voorstel gepleit voor een hervorming van de Grondwet (zie de toelichting, blz. 13). Zie ook artikel 2, lid 2, van het voorstel, waarin wordt bepaald dat richtlijnen inzake het strafrechtelijk beleid niet tot gevolg mogen hebben dat de beoordeling van een individueel geval door de magistraat van het openbaar ministerie wordt geschrapt. Zie voor de verantwoordelijkheid van de procureur des Konings ook de toelichting bij het voorstel, blz. 64-66.

Advies 77/2020 12/25

ambt, zelfs van een bestuursambt, door de wet belast zijn met het verrichten van sommige daden van gerechtelijke politie, staan, doch alleen in dit verband, onder hetzelfde toezicht"³⁴.

33. **Strafrechtelijk uitvoeringsonderzoek (artikelen 416 en v.).** De uitleg over het "klassieke" strafonderzoek (hierboven, overweging nr. 30) geldt *Mutatis mutandis* in principe ook voor het strafrechtelijk uitvoeringsonderzoek. Zo zou het voorstel kunnen verduidelijken dat de "SUO-magistraat" de verwerkingsverantwoordelijke is voor de gegevens die noodzakelijk zijn voor het strafrechtelijke uitvoeringsonderzoek³⁵, omdat het gaat om een magistraat van het openbaar ministerie die het "SUO voert" en die "waakt over de wettigheid van de uitvoeringshandelingen"³⁶. Verder leert het voorstel ons dat "Het SUO wordt gevoerd door en onder het gezag en de leiding van de SUO-magistraat die bevoegd is voor de uitvoering van de in kracht van gewijsde gegane veroordeling. Deze magistraat draagt hiervoor de verantwoordelijkheid"³⁷.
34. Het voorstel kan ook verduidelijken in hoeverre de magistraat van het Centraal Orgaan voor de Inbeslagneming ende Verbeurdverklaring (COIV) die eventueel belast is met een SUO alsook de directeur van het COIV, alleen of samen (met de SUO-magistraat) de verantwoordelijkheid dragen voor de uitgevoerde gegevensverwerkingen.³⁸
35. **Het opsluitingsregister (artikel 487).** Artikel 487 van het voorstel bepaalt dat elke gevangenis verplicht is een opsluitingsregister te houden waarin alle opgesloten personen opgenomen zijn en dat te allen tijde door de procureur des Konings kan worden geraadpleegd en dat dit register onder elektronische vorm mag gehouden worden.
36. Het doel van het opsluitingsregister blijkt duidelijk uit de toelichting bij het voorstel, maar moet expliciet worden vermeld in het beschikkend gedeelte: "In het raam van het ontworpen systeem van het aangemaakt strafonderzoek onder leiding van het openbaar ministerie dient de procureur des Konings een overzicht te hebben over het geheel van de voorlopige hechtenis en de strafuitvoering"³⁹; "[...] vermits ze nodig is om een overzicht te kunnen behouden over alle personen die in voorhechtenis of

³⁴ Zie met name de toelichting bij het voortel, blz. 128, waarin wordt uitgelegd waarom de bepalingen inzake bijzondere veldwachters en boswachters niet in artikel 107 zijn opgenomen.

³⁵ Meer bepaald volgens artikel 416, § 1 "het geheel van handelingen dat strekt tot de opsporing, de identificatie en de inbeslagneming van het vermogen waarop de veroordeling tot betaling van een geldboete, een bijzondere verbeurdverklaring of de gerechtskosten kan worden uitgevoerd".

³⁶ Artikel 416 § 2 van het voorstel.

³⁷ Artikel 417, §1. Zie evenwel ook § 3 van hetzelfde artikel dat bepaalt "Het lid van het openbaar ministerie bij een hof van beroep dat het SUO voert, is bekleed met de hoedanigheid van officier van gerechtelijke politie, hulpofficier van de procureur des Konings. Hij oefent het ambt van officier van gerechtelijke politie uit *onder het toezicht van de procureur-generaal*" (italic toegevoegd door de Autoriteit).

³⁸ Zie artikel 418 van het voorstel en in het bijzonder §§ 2 (verantwoordelijkheid van de magistraat), 3, lid 1 (leiding en gezag van de directeur, onverminderd artikel 417, § 1) en 4, lid 1 (bevoegdheden).

³⁹ Blz. 45.

in strafuitvoering verblijven, en om toestand individueel van elke gehechte persoon te kunnen opvolgen"⁴⁰.

37. In zijn huidige vorm wordt in artikel 487 van het voorstel geen verwerkingsverantwoordelijke aangewezen. Indien "elke gevangenis" verantwoordelijk is voor de verplichting om een opsluitingsregister te hebben, stelt de toelichting bij het voorstel dat, gelet op het doel van het register om de procureur des Konings een overzicht te geven van alle aanhoudingen, "daarom vermeldt wordt dat de procureur des Konings toezicht houdt op register". Het voorstel zal, in het licht van de hierboven uiteengezette beginselen (overwegingen 28-29), verduidelijken wie de verwerkingsverantwoordelijke (of, in voorkomend geval, wie de gezamenlijke verwerkingsverantwoordelijken zijn) is voor het opsluitingsregister.
38. De Autoriteit merkt echter op dat in de toelichting bij het voorstel wordt uitgelegd dat het papieren register in de praktijk is vervangen door een elektronisch register in "Sidis-Suite" en dat de wet daarom moet worden aangepast aan de huidige situatie en de in het veld gebruikte technologie⁴¹. In de praktijk is het momenteel ook zo dat invrijheidstellingen in hetzelfde informatiesysteem worden geregistreerd⁴².
39. Hoewel de toelichting er niet naar verwijst, is de databank "Sidis-Suite" bij de FOD Justitie opgericht bij artikel 3 van de wet van 5 mei 2019 **houdende diverse bepalingen inzake informatisering van Justitie, modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële aktebank**, met onder meer als doel de uitoefening van de wettelijke opdrachten van de penitentiaire administratie, bij de uitvoering van van vrijheidsstraffen en vrijheidsbenemende maatregelen met inbegrip van de toepassing van alle regels betreffende de duur van de detentie en het al dan niet tijdelijk verlaten van de inrichting. Deze wet bepaalt overigen nader de gegevens die via deze gegevensbank⁴³ worden verwerkt en bepaalt dat het openbaar ministerie en de parketsecretarissen toegang hebben tot de verwerkte gegevens⁴⁴. Ter herinnering, de Autoriteit heeft in het verleden twijfels geuit - die zij herhaalt - over de aanwijzing van de FOD Justitie als verwerkingsverantwoordelijke van voormelde wet⁴⁵.
40. Daarom moet het voorstel in een dergelijke context artikel 487 in overeenstemming brengen met de relevante bepalingen van de wet van 5 mei 2019 houdende diverse bepalingen inzake informatisering van Justitie, modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële

⁴⁰ Blz. 354.

⁴¹ Blz. 353.

⁴² Toelichting bij het voorstel, blz. 354.

⁴³ Zie artikel 5.

⁴⁴ Artikel 7, § 1, 5°.

⁴⁵ Zie artikel 4. Zie ook het Advies de GBA, nr. 120/2018 van 7 november 2018, blz. 3, overweging nr. 10.

Advies 77/2020 14/25

aktebank, op zodanige wijze dat zowel de doeleinden, de gegevens als de verwerkingsverantwoordelijke (of de gezamenlijke verwerkingsverantwoordelijken) waarop de verwerking krachtens artikel 487 betrekking heeft, duidelijk worden omschreven. In het voorstel wordt deze verwerkingsverantwoordelijke (of de gezamenlijke verwerkingsverantwoordelijken) geïdentificeerd, overeenkomstig de hierboven uiteengezette beginselen (zie de overwegingen 28-29).

IV.2. Commentaar bij sommige artikelen van het voorstel

41. Recht op gegevenbescherming (artikel 1). Artikel 1 van het voorstel luidt als volgt:

Onverminderd de fundamentele rechtengehuldigd in de Grondwet, de internationale verdragen en het recht van de Europese Unie en de algemene rechtsbeginselen, wordt het Wetboek van Strafrechtspleging toegepast met inachtneming van de wettelijkheid en de loyaliteit van de strafrechtspleging, van het recht op gelijke behandeling en niet-discriminatie, van het recht op individuele vrijheid, van het recht van verdediging, van het recht op een onafhankelijke en onpartijdige rechterlijke instantie, van het recht op een eerlijk proces en op een uitspraak binnen een redelijke termijn, en met respect voor het privéleven. In overeenstemming met deze rechten worden de bepalingen van dit Wetboek toegepast met inachtneming van de beginselen van proportionaliteit en subsidiariteit".

42. De Autoriteit herinnert eraan dat het recht van een persoon op bescherming van zijn persoonsgegevens een grondrecht is dat in artikel 8 van het Handvest van de grondrechten van de Europese Unie *autonoom* wordt erkend ten opzichte van het recht op bescherming van de persoonlijke levenssfeer. Het recht op gegevensbescherming is niet alleen gekoppeld aan het recht op privacy : breder dan dit zijn het *de rechten en vrijheden van natuurlijke personen* die het wil garanderen met betrekking tot de verwerking van persoonsgegevens⁴⁶. Met andere woorden, een verwijzing naar de eerbiediging van dit recht in het kader van een strafrechtelijke procedure is minstens even relevant als een verwijzing naar het recht op privacy in artikel 1 van het voorgestelde Wetboek van strafprocesrecht. Naast het feit dat gegevensbescherming verder gaat dan de bescherming van de persoonlijke levenssfeer, zal de verwerking van persoonsgegevens (zowel voor het verzamelen van gegevens als voor het gebruik ervan) inderdaad systematisch worden gebruikt in het kader van strafrechtelijke procedures, alsook

⁴⁶ Zie bijvoorbeeld overweging nr. 7 en de artikelen 1, 2, a), 19, 20, 27, 28, 29, 30, 31 en 36, 2, a) van de richtlijn 2016/680. Reeds in 191 bepaalde artikel 1 van het Verdrag 108 van de Raad van Europa (tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens) het volgende: "Dit Verdrag heeft tot doel op het grondgebied van elke Partij *aan iedere natuurlijke persoon*, ongeacht zijn nationaliteit of verblijfplaats, de eerbiediging van zijn rechten en fundamentele vrijheden *te waarborgen en met name zijn recht op persoonlijke levenssfeer* ten opzichte van de geautomatiseerde verwerking van persoonsgegevens hem betreffend ("gegevensbescherming") (italic toegevoegd door de Autoriteit). Deze aanpak is verder bevestigd in het kader van de modernisering van Verdrag nr. 108 van de Raad van Europa, in artikel 1 van Verdrag nr. 108+ : "Het doel van dit verdrag is de bescherming van personen, ongeacht hun nationaliteit of verblijfplaats, met betrekking tot de verwerking van persoonsgegevens, en aldus bij te dragen tot de eerbiediging van hun mensenrechten en fundamentele vrijheden, in het bijzonder hun recht op privacy (italic toegevoegd door de Autoriteit).

meer in het algemeen bij de uitoefening van vele taken in het algemeen belang (of bij de uitoefening van het openbaar gezag) door de bevoegde overheidsinstanties.

43. De Autoriteit is daarom van mening dat in de eerste zin van deze bepaling een verwijzing naar het recht op gegevensbescherming moet worden toegevoegd.
44. **Toelaatbaarheid van het bewijs (artikelen 11 en 12).** In het voorgestelde wetboek wordt een benadering gevolgd die in overeenstemming is met het systeem van de regel van relatieve uitsluiting van bewijsmateriaal⁴⁷. Mutatis mutandis, is dezelfde opmerking als bij artikel 1 van het voorstel van toepassing op artikel 11 van het voorstel. Dit laatste regelt, met betrekking tot de bestraffing van onregelmatige bewijzen, de eventuele toelaatbaarheid van informatie die is verkregen in strijd met, in het bijzonder, het recht op verdediging of het recht op privacy.
45. Het niet opnemen van het recht op gegevensbescherming in deze bepaling zou neerkomen op het opleggen van de gevaarlijke oefening om onder de schendingen van de regels inzake gegevensbescherming deze te onderscheiden die al dan niet ook een schending van het recht op privacy zouden vormen (wat een bron van rechtsonzekerheid en potentieel artificieel onderscheid is)⁴⁸, aangezien voor inbreuken op rechten die niet onder artikel 11 van het voorstel vallen, *een soepeler* regeling voor de ontvankelijkheid van bewijsmateriaal geldt, zoals bepaald in artikel 12 van het voorstel⁴⁹. De Autoriteit is echter van mening dat voor een doeltreffende bescherming van personen met betrekking tot de verwerking van persoonsgegevens in het kader van strafrechtelijke procedures, schendingen van het recht op gegevensbescherming onder de in artikel 11 van het voorstel vastgelegde regeling moeten vallen.
46. Wat met name artikel 11 van het voorstel betreft, neemt de Autoriteit nota van de wijzigingen die door deze bepaling in de jurisprudentie en de Antigone-doctrine zijn aangebracht en die intussen in het positieve recht zijn bevestigd⁵⁰. Op grond van het voorgestelde wetboek van strafprocesrecht is

⁴⁷ Zie de Toelichting, blz. 69 ev.

⁴⁸ Toegegeven, in de jurisprudentie van het Europees Hof voor de Rechten van de Mens wordt (logischerwijs) systematisch via artikel 8 EVRM de gegevensbescherming (en, indien van toepassing, Verdrag nr. 108 van de Raad van Europa) ingeroepen als de meest relevante bepaling van het Verdrag in dit verband. Zie onder meer het Europees Hof voor de Rechten van de Mens, "Guide on Article 8 of the European Convention on Human Rights, Right to Privacy and familiale", 2019, bijgewerkt tot 31 augustus 2019, punten 159 en volgende.

⁴⁹ Buiten de in de artikelen 9 tot 11 bepaalde gevallen kan de informatie die op onregelmatige wijze werd verkregen, worden toegelaten tot de debatten tenzij de rechter vaststelt dat het gebruik ervan in een gerechtelijke beslissing afbreuk doet aan de integriteit van Justitie. Volgens deze: "Toelichting bij het voorstel (blz. 78) verduidelijkt hierover dat: "Dit artikel bepaalt dat buiten de in de artikelen 9 tot 11 bedoelde gevallen de informatie die op onrechtmatige wijze wordt verkregen, kan worden toegelaten tot de debatten tenzij de rechter vaststelt dat het gebruik ervan in een gerechtelijke beslissing afbreuk doet aan de integriteit van Justitie". Het gaat hier om minder indringende gevallen van onregelmatigheid die niet onder de in artikel 11 beschreven regeling vallen omdat ze de erin opgesomde fundamentele rechten niet aantasten. Wanneer informatie alsdan op onregelmatige wijze werd verkregen, kan worden aanvaard dat deze wordt toegelaten tot de debatten, tenzij de rechter vaststelt dat het gebruik ervan afbreuk doet aan de integriteit van justitie."

⁵⁰ Artikel 32 van de voorafgaande titel van het Wetboek van Strafvordering bepaalt: "Tot nietigheid van onregelmatig verkregen bewijselement wordt enkel besloten indien :

- de naleving van de betrokken vormvoorwaarden wordt voorgeschreven op straffe van nietigheid, of;

Advies 77/2020 16/25

informatie⁵¹ die in strijd met het recht op privacy is verkregen in principe dus uitgesloten van de debatten, net als informatie die daaruit is afgeleid, tenzij de rechter drie cumulatieve voorwaarden vaststelt : dat de onregelmatigheid niet het resultaat is van een bewuste of onverschoonbare miskenning van het recht of de beschermde waarde; dat de ernst van de schending van het recht of de beschermde waarde concreet minder zwaarwichtig is dan het maatschappelijk belang bij de vervolging van het betrokken misdrijf en bij de eventuele sanctionering van de dader van het misdrijf; en dat het gebruik van het onregelmatig bewijs geen afbreuk doet aan de integriteit van Justitie.

47. Hoewel de Autoriteit gunstig staat tegenover de in artikel 11 van het voorstel gevolgde aanpak, merkt ze op dat er niet langer een rechtstreekse verwijzing is, zoals momenteel het geval is in artikel 32 van de voorafgaande titel van het wetboek van strafvordering, naar het geval waarin de begane onregelmatigheid de "betrouwbaarheid van het bewijs heeft aangetast" (een geval dat in deze tekst wordt onderscheiden van de schending van het recht op een eerlijk proces).
48. Op het gebied van gegevensbescherming komt een dergelijk criterium echter overeen met de beginselen van kwaliteit en veiligheid van de gegevens, die met het oog op het vaststellen van het bewijs nog belangrijker zijn: De verwerkte gegevens moeten met name nauwkeurig en actueel zijn en op zodanige wijze worden verwerkt dat een passende beveiliging is gewaarborgd⁵². Op het gebied van bewijsmateriaal en informatiebeveiliging zal in het kader van de betrouwbaarheid van het bewijsmateriaal bijzondere aandacht moeten worden besteed aan garanties met betrekking tot de beschikbaarheid en de integriteit van de verwerkte persoonsgegevens⁵³ (uiteraard naast de noodzaak om de vertrouwelijkheid te waarborgen⁵⁴).
49. Kortom, de Autoriteit is van mening dat naast de bovengenoemde drie cumulatieve criteria het criterium dat de betrouwbaarheid van het bewijsmateriaal niet in het gedrang mag komen, moet worden toegevoegd, of zij is ten minste van mening dat in de toelichting moet worden gespecificeerd

-
- de begane onregelmatigheid de betrouwbaarheid van het bewijs heeft aangetast, of;
 - het gebruik van het bewijs in strijd is met het recht op een eerlijk proces".

⁵¹ De toelichting bij het voorstel verduidelijkt over het begrip "opsporing" (blz. 20) het volgende "Gelet op het feit dat de rechtspraak een onderscheid heeft gemaakt tussen de inlichtingen die toelaten een onderzoek te starten of te oriënteren enerzijds en degene die strekken tot het bewijs van de feiten anderzijds, en dat daardoor bepaalde inlichtingen niet als een bewijs worden beschouwd en zodoende ontsnappen aan een rechterlijke controle in de zin van artikel 32 van de Voorafgaande Titel van het Wetboek van Strafvordering, meent de Commissie dat indien de informatie door de rechter in zijn oordeelsvorming wordt betrokken of indien uit de bewijsconstructie en de motivering blijkt dat deze een rol heeft gespeeld bij de beslissing, deze informatie aan hetzelfde regime als een bewijs dient te worden onderworpen. Om deze reden werd in de wettelijke regeling de bredere term "informatie" gebruikt in plaats van de klassieke term "bewijs". Zie ook voor meer details, blz. 74-76.

⁵² Zie met name de artikelen 4.1., d) en f), 71 19, 25 en 29 van de Richtlijn 2016/680. Zie ook met name de artikelen 50, 51, 56 en 60 van de WVG.

⁵³ Zie in het bijzonder het artikel 29,2, b), c), h), j) van de richtlijn nr. 2016/680.

⁵⁴ Voor gevallen waarin maatregelen om de vertrouwelijkheid van gegevens te waarborgen van bijzonder belang zijn voor de betrokkenen, zie bijvoorbeeld artikel 193 en volgende van het voorstel betreffende anonieme getuigenissen, en de artikelen 108, 109 en 119 van het voorstel betreffende de bescherming van de identiteit van de leden van de politiediensten in bepaalde gevallen.

welke van deze criteria betrekking hebben op de gevallen waarin de betrouwbaarheid van het bewijsmateriaal in het gedrang komt⁵⁵.

50. De Autoriteit herinnert er evenwel aan dat ernstige schendingen van de persoonlijke levenssfeer, zoals het gebruik van indringende bevoegdheden door het openbaar ministerie, waarvoor de toestemming van de onderzoeksrechter nodig is, zonder toestemming van die rechter, systematisch worden bestraft met de uitsluiting van de procedure van informatie die op basis daarvan is verkregen en van informatie die daaruit is afgeleid, overeenkomstig artikel 10 van het voorstel. De toelichting bij het voorstel benadrukt dat "alle onderzoeksdaden waarvoor nu een rechterlijke beslissing vereist is ook in de toekomst slechts na rechterlijke machtiging zullen kunnen worden verricht"⁵⁶. Met name voor onderzoekshandelingen is toestemming van de onderzoeksrechter vereist (met beperkte uitzonderingen zoals in gevallen van ontdekking bij heterdaad) : opsporen van verkeersgegevens van elektronische communicatiemiddelen (artikel 184 van het voorstel); onderscheppen van voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen, of er kennis van nemen, doorzoeken en opnemen of de zoeking in een informaticasysteem of een deel ervan uitbreiden (artikelen 185 tot 192); de huiszoekingen (205 tot 211)⁵⁷.

51. Recht op toegang tot het dossier (artikelen 87 §4, 216, 229,232 en 233; artikel 416, § 5)

Het recht op toegang tot het dossier⁵⁸ kan worden aangepast aan het recht van de betrokkene op gegevensbescherming, maar zoals uit de volgende overwegingen blijkt, voldoet het niet aan alle eisen van de artikelen 14 en 15 van Richtlijn 2016/680.

52. In de toelichting bij het voorstel⁵⁹ wordt uitgelegd "Het ontwerp voorziet in de differentiatie van de rechten en procedures die van toepassing zijn volgens de ernst van de misdrijven in het geding. Het evenwicht moet hier worden gezocht tussen de wens van een voldoende snelle en efficiënte procedure en het waarborgen van de rechten van de partijen". Daartoe wordt bij de toegang tot het dossier onderscheid gemaakt naargelang het dossier al dan niet betrekking heeft op strafbare feiten waarop een vrijheidsstraf staat.

⁵⁵ A priori lijkt het criterium van de aantasting van de integriteit van de rechtspleging daartoe open te staan, maar de toelichting maakt het niet mogelijk dit te beweren (dit criterium lijkt ook in het buitenlands recht te worden nagestreefd). Volgens de toelichting bij het voorstel (blz. 77) "Het derde criterium houdt verband met de integriteit van Justitie. Het is een criterium dat is geïnspireerd op artikel 24 (2) van het Canadese handvest van de rechten en vrijheden dat voorziet in een uitsluiting van het bewijs indien het de rechtsbedeling in diskrediet zou brengen of, meer precies, een schending inhoudt van de integriteit van Justitie. Het betreft het integriteitsbeginsel (integrity principle) dat ook terug te vinden is in de rechtspraak in Engeland en Wales, zo in een arrest van het House of Lords van 8 december 2005[...] (referentie weggelaten).

⁵⁶ Blz. 24.

⁵⁷ Voor de indeling van de drie soorten onderzoekshandelingen (deze die onder de exclusieve bevoegdheid van de procureur des Konings vallen, deze die gemengd zijn en afhankelijk van de omstandigheden machtiging van de onderzoeksrechter vereisen, en ten slotte deze waarvoor altijd machtiging van de onderzoeksrechter nodig is), zie de toelichting bij het voorstel, blz. 25 en volgende.

⁵⁸ Zie ook de Toelichting bij het voorstel, blz. 181 ev.

⁵⁹ Blz. 16.

53. Artikel 216 van het voorstel is de meest verstrekkende bepaling inzake het recht op toegang tot het dossier⁶⁰. Er wordt met name bepaald dat tegen de beslissing van de procureur des Konings beroep kan worden aangetekend bij de onderzoeksrechter⁶¹. Om volledig te zijn, moet dit artikel worden gelezen in combinatie met : het artikel 229, §1 dat het afsluiten beoogt van het onderzoek door de procureur des Konings, in welk geval het dossier automatisch ter beschikking wordt gesteld; artikel 232 dat de uitdoving betreft van de strafvordering middels het betalen van een geldsom (straftransactie) in welk geval ook in de toegang tot het dossier is voorzien (§ 2 ter attentie van de dader en het slachtoffer); artikel 233, dat voorziet in de beëindiging van de strafvordering door het nemen van maatregelen en het vervullen van voorwaarden, in welk bijkomende geval het dossier nog steeds toegankelijk is voor de dader en het slachtoffer (§ 2); en tot slot artikel 87, §4, lid 1 van het voorstel dat hierna wordt besproken (overwegingen nr. 57).

54. De toegang tot het dossier waaraan artikel 216 van het ontwerp is gewijs, is inhoudelijk onderworpen aan de volgende voorwaarden:

- het is slechts toegankelijk voor de verdachte en de benadeelde⁶² (artikel 216, § 1)⁶³ ;
- slechts van toepassing in het dossier dat betrekking heeft op misdrijven strafbaar met een vrijheidsstraf (artikel 216, §1) ;
- Op straffe van niet-ontvankelijkheid moet het verzoekschrift gemotiveerd zijn (artikel 216, §2, lid 1) ;
- het houdt de keuze van woonplaats in België in, indien de verzoeker er zijn woonplaats niet heeft. Het verzoekschrift bevat het "eventuele" e-mail adres waar de beslissing op kan worden meegedeeld (artikel 216, §1, lid 1) ;
- Het mag pas worden toegezonden of neergelegd nadat één maand verstreken is sinds het opstellen van het eerste proces-verbaal (artikel 216, § 2, lid 2);
- De verzoeker kan geen verzoekschrift met hetzelfde voorwerp toezenden (of neerleggen) vooraleer een termijn van drie maanden is verstreken te rekenen van de laatste beslissing die betrekking heeft op hetzelfde voorwerp (artikel 216, § 6);
- een dubbele voorwaarde heeft ook betrekking op het belang van de verzoeker: de procureur des Konings kan immers een inzage weigeren als "de verzoeker geen rechtmatige beweegredenen tot het raadplegen van het dossier doet blijken" (artikel 216, §3, lid 1); en hij

⁶⁰ Zie ook artikel 416, § 5 betreffende het strafuitvoeringsonderzoek.

⁶¹ Zie de artikelen 216, § 5 en 221 van het voorstel.

⁶² Blijkens artikel 70 van het voorstel verkrijgt iemand de hoedanigheid van benadeelde persoon die verklaart schade te hebben geleden veroorzaakt door een misdrijf (de verklaring gebeurt met een formulier ad hoc en moet bepaalde informatie bevatten). en elke persoon die benadeeld is door een misdrijf beschikt over een burgerlijke rechtsvordering (artikel 71 van het voorstel). de burgerlijke partij oefent de burgerlijke strafvordering uit (artikel 72 van het voorstel).

⁶³ In het kader van het strafrechtelijk uitvoeringsonderzoek staat het recht om het dossier te raadplegen of te kopiëren open voor de veroordeelde en voor derden die een belang aantonen. Ter herinnering bepaalt artikel 416, §3 "Het SUO wordt gevoerd ten aanzien van de veroordeelde dader, hierna "de veroordeelde" genoemd, en de derden die wetens en willens met de veroordeelde samenspannen om zijn vermogen te onttrekken aan de tenuitvoerlegging van de uitvoerbare veroordelingen".

kan de inzage of het nemen van een afschrift beperken tot het gedeelte van het dossier waarvoor de verzoeker een "belang kan doen gelden" (artikel 216, §3, lid 2).

55. Voorts kan de procureur des Konings de inzage of het nemen van een afschrift van het dossier weigeren indien de noodwendigheden van het onderzoek dit vereisen, indien de inzage een gevaar oplevert voor personen of een ernstige schending van hun privéleven zou inhouden of indien het dossier enkel de verklaring of de klacht bevat, waarvan de verzoeker of zijn advocaat reeds een afschrift heeft ontvangen⁶⁴.
56. Artikel 216, §3, lid 3, van het voorstel bepaalt ook dat de raadpleging of het afschrift van het dossier⁶⁵ in beginsel niet meer mag worden geweigerd wanneer zes maanden zijn verstreken sinds de opstelling van het eerste proces-verbaal, behalve in twee gevallen :
- indien hij van oordeel is dat de verzoeker niet beschikt over de hoedanigheid van verdachte of benadeelde, of
 - indien hij overeenkomstig artikel 220 van het voorstel, van de rechter van het onderzoek een verlenging van het geheime karakter ervan heeft verkregen omdat de toegang tot het gehele dossier of een deel ervan het verloop van het onderzoek ernstig in het gedrang zou kunnen brengen of de bescherming van personen.
57. Ten slotte is artikel 216, § 4, lid 2 gewijd aan een beperking op het gebruik dat kan worden gemaakt van de verkregen "inlichtingen": "De verzoeker kan de door de inzage of het nemen van een afschrift verkregen inlichtingen alleen gebruiken in het belang van zijn verdediging, op voorwaarde dat hij het vermoeden van onschuld in acht neemt, alsook de rechten van verdediging van derden, het privéleven en de waardigheid van de persoon, onverminderd het in artikel 217 bedoelde recht om het verrichten van bijkomende onderzoekshandelingen te vragen".
58. Indien de aanvrager overweegt het recht van toegang voor de betrokkenen op te bouwen op basis van het zojuist uiteengezette dispositief waarin voornamelijk in artikel 216 van het voorstel is voorzien (zie overweging 15 hierboven), vestigt de Autoriteit de aandacht op de volgende vier opmerkingen.

⁶⁴ Artikel 216, § 3, 1ste lid van het voorstel.

⁶⁵ In het voorstel moet worden verduidelijkt of deze regel ook van toepassing is op gevallen waarin sprake is van misdrijven *die niet* met een vrijheidsstraf kunnen worden bestraft. Immers, de Toelichting bij het voorstel laat dit verstaan (blz. 183 "De misdrijven niet strafbaar met vrijheidsstraf worden uitgesloten van deze regeling. Dit sluit echter niet uit dat er een verzoek wordt gedaan om het dossier te raadplegen en er op eenvoudig verzoek een kopie van te maken, zonder mogelijkheid tot beroep, ook voor feiten waarop geen vrijheidsstraf staat. *Bovendien* wordt ervan uitgegaan dat het recht op raadpleging zes maanden na het eerste proces-verbaal automatisch wordt toegekend, zodat alle partijen snel en op voet van gelijkheid kunnen profiteren van een gewaarborgd raadplegingsrecht " (cursief toegevoegd door de Autoriteit), laat de structuur van artikel 216 ruimte voor twijfel. In feite lijkt paragraaf 1 namelijk de reikwijdte van het hele artikel te beperken en lid 3 van §3 lijkt daar niet van af te wijken.

59. Ten eerste geldt dit recht van toegang tot het dossier als zodanig alleen voor de verdachte en de benadeelde partij. Maar een strafdossier kan ook betrekking op andere betrokkenen⁶⁶. Voor deze andere betrokkenen is waarschijnlijk alleen artikel 87, §4, eerste lid⁶⁷, van het voorstel relevant. Deze bepaalt alleen het volgende "Onverminderd de toepassing van artikelen 216, 229, 232 et 233, kan de procureur des Konings tevens aan een persoon die van een wettig belang doet blijken, toestemming verlenen om alle akten van rechtspleging van het dossier of een gedeelte ervan te raadplegen of een kopie daarvan te verkrijgen. Hij kan voorwaarden verbinden aan deze toestemming. Zijn beslissing is niet vatbaar voor hoger beroep. De persoon kan zelf met zijn eigen middelen kosteloos een kopie ervan nemen ter plaatse". Een dergelijke bepaling voldoet niet aan de vereisten van de artikelen 14 en 15 van richtlijn 2016/680, met name omdat zij de gronden voor weigering van toegang niet beperkt, noch wat de inhoud ervan betreft, noch wat de noodzaak ervan betreft (met name in de tijd).
60. Ten tweede zal hetzelfde artikel 87 § 4, van het voorstel van toepassing zijn wanneer de zaak betrekking heeft op een strafbaar feit waarop geen vrijheidsstraf staat. De toelichting bij het voorstel⁶⁸ legt uit dat "De ontworpen regeling wordt beperkt tot de misdrijven strafbaar met vrijheidsstraf, teneinde te komen tot een proceseconomisch haalbare regeling". De Autoriteit is van mening dat, wat het recht op toegang betreft, een dergelijke systematische beperking niet gerechtvaardigd zou zijn. Ter illustratie: een verwerkingsverantwoordelijke (natuurlijke persoon) die het voorwerp is van een strafrechtelijk onderzoek zou alleen kunnen verwijzen naar artikel 87, § 4, van het voorstel, aangezien hem alleen boetes kunnen worden opgelegd.⁶⁹
61. Ten derde staat Richtlijn 2016/680 niet toe dat het recht op toegang in beginsel afhankelijk wordt gesteld van de voorwaarde dat de betrokkene een belang heeft of een motivering geeft voor het verzoek, anders dan door het bewijs van zijn of haar identiteit⁷⁰. Een dergelijke motivering kan alleen worden verlangd en voor zover dit noodzakelijk blijkt voor de concrete beoordeling van de in artikel 15.1 van richtlijn 2016/680 bedoelde redenen.
62. Ten vierde kunnen de beperkingen op het gebruik van de verkregen "inlichtingen" de betrokkene niet beletten deze te gebruiken voor de uitoefening van zijn recht op bescherming van persoonsgegevens (bijvoorbeeld om de eventuele inovereenstemming van de gegevensverwerking in kwestie te verkrijgen), aangezien dit het eigenlijke doel is van het recht van toegang: "Een natuurlijke persoon moet beschikken over het recht op inzage van de gegevens die over hem zijn verzameld, en moet dit

⁶⁶ Zie bijvoorbeeld artikel 6 van Richtlijn 2016/680 en artikel 31 van de WVG, waarin vier categorieën van betrokkenen worden genoemd (met inbegrip van slachtoffers en derden bij het betrokken misdrijf).

⁶⁷ Lid 2 heeft betrekking op De uitgaven en de afschriften van de onderzoeks- en procedurestukken van de opgeheven militaire gerechten en parketten met betrekking tot dossiers waarin definitief werd gevonnis of over dewelke de krijgsauditeur of de auditeur-generaal per 31 december 2003 hebben beslist.

⁶⁸ Blz. 183.

⁶⁹ Zie de artikelen 222 tot 227 van de WVG die niet voorzien in vrijheidsberovende straffen.

⁷⁰ Zie ook artikel 12.5 van de Richtlijn 2016/680.

recht gemakkelijk en met redelijke tussenpozen kunnen uitoefenen, *zodat hij kennis kan nemen van de verwerking en de rechtmatigheid daarvan kan nagaan*. [...] Om aan dit recht te voldoen, volstaat het dat aan de betrokkene in een begrijpelijke vorm een volledig overzicht van die gegevens wordt verstrekt, dat wil zeggen in een vorm die de betrokkene in staat stelt kennis te nemen van deze gegevens en *na te gaan of deze juist zijn en overeenkomstig deze richtlijn zijn verwerkt, zodat hij in voorkomend geval de hem uit hoofde van deze richtlijn toegekende rechten kan uitoefenen*" (italic toegevoegd door de Autoriteit)⁷¹.

63. **Uitbreiding van het onderzoek in een informaticasysteem (artikel 171, § 3).** In dit verband is het voorstel bedoeld om gevolg te geven aan het arrest nr. 174/2018 van het Grondwettelijk Hof van 6 december 2018, waarop het had geanticipeerd. In dit arrest heeft het Grondwettelijk Hof artikel 22 van de Grondwet en artikel 8 van het EVRM toegepast op de wet van 25 december 2016⁷² met name in die zin dat het de uitbreiding van zoeking in een informaticasysteem regelde. Het Hof merkt het volgende op⁷³ "De uitbreiding van de zoeking biedt de speurders de mogelijkheid toegang te hebben niet alleen tot alle gegevens die zijn opgeslagen of bewaard op het toestel dat het vertrekpunt vormt van de zoeking, *maar ook tot alle op de informaticasystemen opgeslagen documenten die door verbinding via dat toestel worden bereikt, alsook tot alle communicatie die door de gebruiker ervan met derden wordt gevoerd*, met inbegrip van de nieuwe ontvangen of onderweg zijnde berichten waarvan de gebruiker nog geen kennis heeft genomen" (italic toegevoegd door de Autoriteit). Vervolgens wordt uitgelegd dat de bestreden wetswijziging de procureur des Konings toestaat de zoeking in een informaticasysteem uit te breiden zonder toestemming van de onderzoeksrechter, terwijl een dergelijke bevoegdheid alleen door de onderzoeksrechter tijdens een onderzoek zou moeten worden toegestaan, gezien de ernst van de inmenging en het geheime en niet-tegensprekelijk karakter van de informatie⁷⁴. Het Hof merkt voorts op dat de overdracht van de bevoegdheid van de onderzoeksrechter naar de procureur des Konings niet gepaard gaat met extra waarborgen die bedoeld zijn om het privéleven en de rechten van de verdediging van de betrokken persoon daadwerkelijk te beschermen en die van dien aard zijn de afschaffing van het voorafgaand optreden van een onafhankelijke en onpartijdige rechter te compenseren⁷⁵. Het Hof concludeert "Vanwege de ernst van de erdoor teweeggebrachte inmenging in het recht op eerbiediging van het privéleven, kan de maatregel die erin bestaat een zoeking in een informaticasysteem of een deel ervan die is aangevat in een informaticasysteem dat in beslag is genomen of dat door de procureur des Konings in beslag kan worden genomen, uit te breiden naar een informaticasysteem of een deel ervan dat zich op een andere

⁷¹ Overweging (43) van Richtlijn (EU) 2016/680.

⁷² Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en de oprichting van een gegevensbank stemafdrukken.

⁷³ Onder overweging nr. B.11.2 van het arrest.

⁷⁴ Zie de overwegingen nrs. B.13.1 tot B.16.1 van het arrest.

⁷⁵ Overweging nr. B.16.2 van het arrest.

plaats bevindt dan daar waar de zoeking wordt verricht, enkel worden toegelaten onder dezelfde voorwaarden als diegene die gelden in verband met de onderzoekshandelingen bedoeld in B.14.2. [76] ».

64. Artikel 171, § 3, van het voorstel regelt nu de uitbreiding van de informaticazoekingen en is in overeenstemming met de zojuist genoemde jurisprudentie door te voorzien in de noodzaak van toestemming van de onderzoeksrechter en door een zekere bevoegdheid van het openbaar ministerie te handhaven in geval van ontdekking op heterdaad⁷⁷. Het wijkt hier echter van af door een extra mogelijkheid te bieden om de zoeking in het informaticasysteem uit te breiden tot de procureur des Konings en de officier van gerechtelijke politie op voorwaarde (naast de voorwaarden van artikel 171, § 3, eerste lid, van het voorstel) : dat hij het geschreven en duidelijk akkoord heeft van de gewoonlijke gebruiker van het informaticasysteem; dat hij deze laatste voorafgaandelijk geïnformeerd heeft over de mogelijke strekking van de uitbreiding van de zoeking en haar finaliteit; dat de uitbreiding van de zoeking een punctueel karakter vertoont en in direct verband staat met het voorwerp van het onderzoek.
65. De Autoriteit neemt hiervan akte en merkt het volgende op. Zij herinnert eraan dat een dergelijk akkoord geen basis zal vormen voor de rechtmatigheid van de verwerking van persoonsgegevens als zodanig⁷⁸, maar voor de betrokken verdachte wel een zekere garantie kan vormen, in verband met de context van de verwerking (een strafrechtelijk onderzoek). De Autoriteit merkt ook op dat een dergelijke garantie geen garantie zal zijn voor *derden* (zenders van eventuele communicaties, enz.) waarvan de persoonsgegevens in dit verband zullen worden verwerkt⁷⁹.

⁷⁶ Meer bepaald huiszoekingen, onderscheppen, kennisnemen, doorzoeken en opnemen met technische hulpmiddelen van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan (zie artikel 90ter van het Wetboek van Strafvordering).

⁷⁷ Aangaande de informaticazoeeking, zie de Toelichting bij het voorstel, blz. 157-163.

⁷⁸ Overweging nr. 35 van de richtlijn 2016/680: [...] Het uitvoeren van de bij wet aan de bevoegde autoriteiten toegewezen taken in verband met de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, stelt hen in staat van natuurlijke personen te verlangen of te eisen dat zij aan de gedane verzoeken gevolg geven. In dit geval mag de toestemming van de betrokkene als omschreven in Verordening (EU) 2016/679 geen rechtsgrond vormen voor de verwerking van persoonsgegevens door bevoegde autoriteiten. Wanneer van de betrokkene wordt verlangd dat hij aan een wettelijke verplichting voldoet, heeft hij geen echte, vrije keuze, en kan zijn reactie derhalve niet als een spontane blijk van zijn wil worden uitgelegd. Dit mag de lidstaten niet beletten om in hun wetgeving te bepalen dat de betrokkene kan instemmen met de verwerking van zijn persoonsgegevens voor de doeleinden van deze richtlijn, zoals DNA-tests in strafrechtelijke onderzoeken of het toezicht, met behulp van elektronische enkelbanden, op de locatie waar de betrokkene zich bevindt met het oog op de tenuitvoerlegging van straffen".

⁷⁹ Artikel 171, § 7 van het voorstel bepaalt: "Tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, brengt de procureur des Konings *de verantwoordelijke van het informaticasysteem* zo spoedig mogelijk op de hoogte van de zoeking in het informaticasysteem of van de uitbreiding ervan. Hij deelt hem in voorkomend geval een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd (italic toegevoegd door de Autoriteit). Ter herinnering: in het arrest van het Grondwettelijk Hof nr. 174/2018 van 6 december 2018 heeft het Hof in overweging B.22.2 van zijn arrest geoordeeld dat "Daaruit vloeit voort dat het begrip « verantwoordelijke van het informaticasysteem » in die zin moet worden begrepen dat het de persoon of de personen aanwijst die verantwoordelijk zijn voor de gegevens of de communicatie die zijn opgeslagen op het toestel dat in beslag is of kan worden genomen en voor de gegevens of de communicatie waarvan kennis kan worden genomen via de netwerken die worden beoogd door de uitbreiding van de in het voormelde toestel aangevatte zoeking, waarbij die persoon of die personen niet noodzakelijk de eigenaar of de houder van de betrokken toestellen zijn. Zoals is vermeld in B.15.2, is ook de verdachte bedoeld wiens gegevens het voorwerp uitmaken van de zoeking wanneer hij zelf niet de effectieve controle heeft over het desbetreffende informaticasysteem".

66. Ten slotte moet op bladzijde 159 van de toelichting, derde alinea, Franse versie, na de woorden "mots de passements supplémentaires" de woorden "ou l'utilisation de faux clés" worden toegevoegd om de Franse versie van de tekst in overeenstemming te brengen met de Nederlandse versie ("van valse sleutels gebruikt").

OM DIE REDENEN,

Rekening houdend met het feit dat het voorstel dat voor advies voorligt, onvolledig is wat betreft de verwerking van persoonsgegevens in het kader van strafrechtelijke procedures, is de analyse ervan, die daarom niet uitputtend en deels voorbarig is, beperkt tot beide relevante bepalingen inzake gegevensbescherming (**overwegingen nrs. 20-26**) ;

1. tekortkomingen van het positief recht De Autoriteit herinnert eraan dat zij weliswaar bevoegd is om in het kader van de vaststelling van een wet- of regelgevingsnorm advies uit te brengen over een regelgeving zoals het voorgestelde Wetboek van strafprocesrecht, maar dat in het positieve recht geen enkele autoriteit bevoegd is om in de praktijk toe te zien op de naleving van de regels inzake gegevensbescherming door de gerechtelijke autoriteiten, in dit geval de strafrechtelijke autoriteiten (**overwegingen nrs. 7-14**). Dit is een belangrijke leemte in het Belgische recht, die op dit punt tekortschiet t.a.v. artikel 8.3 3, van het Handvest van de grondrechten van de Europese Unie.

Een dergelijke tekortkoming heeft ook tot gevolg, zoals in de toelichting bij het voorstel wordt benadrukt, dat het niet mogelijk is te voorzien in de uitoefening van de rechten van de betrokkenen via de bevoegde toezichthoudende autoriteit (**overwegingen nrs. 15-17**).

De Autoriteit is van mening dat de aanvrager deze leemte moet opvullen.

2. Verwerkingsverantwoordelijken en doeleinden De Autoriteit benadrukt dat het voorstel, overeenkomstig de beginselen van transparantie en rechtmatigheid (**overweging nr. 27**), uitdrukkelijk de verwerkingsverantwoordelijken en het doel van de verwerkingen moet aangeven.

Met name in dit geval zal het voorstel in de eerste plaats bevestigen dat de procureur des Konings de persoon is die verantwoordelijk is voor de verwerking van de gegevens die nodig zijn voor **het onderzoek** en de uitoefening van de strafvordering, in de uitvoering van de bevoegdheden, competenties en verplichtingen die hij heeft en waaraan hij gebonden is door dit Wetboek (**overweging nr. 30**).

Het zal ook de mogelijke autonome verantwoordelijkheid identificeren met betrekking tot de verwerking (of gezamenlijke verantwoordelijkheid, in voorkomend geval met een andere overheidsinstantie) van de **officieren van gerechtelijke politie (overwegingen nrs. 31-32)**.

Hetzelfde geldt voor wat de context betreft van het **strafuitvoeringsonderzoek**, en de verantwoordelijkheden van de SUO-magistraat evenals in voorkomend geval van de magistraat van het Centraal Orgaan voor de Inbeslagneming (**overwegingen nrs. 33-34**).

En tot slot, gelet op de toelichting bij het voorstel betreffende het **opsluitingsregister**, moet artikel 487 in overeenstemming gebracht worden met de relevante bepalingen van de wet van 5 mei 2019 houdende diverse bepalingen inzake informatisering van Justitie, modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële aktebank, op zodanige wijze dat zowel de doeleinden, de gegevens als de verwerkingsverantwoordelijke (of de gezamenlijke verwerkingsverantwoordelijken) waarop de verwerking krachtens artikel 487 betrekking heeft, duidelijk worden omschreven (**overwegingen nrs. 35-40**).

3. Recht op gegevensbescherming Aangezien het recht op gegevensbescherming een autonoom grondrecht is en ten minste even relevant is in het kader van strafrechtelijke procedures als het recht op privacy, is de Autoriteit van mening dat het in artikel 1 van het voorstel moet worden vermeld (**overwegingen nrs. 41-43**).

4. Recht op gegevensbescherming en toelaatbaarheid van het bewijs In dezelfde zin is de Autoriteit, wat betreft de relatieve uitsluiting van bewijsmateriaal dat door het voorstel wordt ingevoerd, van mening dat, met het oog op een doeltreffende bescherming van personen in verband met de verwerking van persoonsgegevens in het kader van strafrechtelijke procedures, moet worden verwezen naar het recht op gegevensbescherming in artikel 11 van het voorstel en dat ervoor moet worden gezorgd dat gevallen waarin de gepleegde onregelmatigheid de betrouwbaarheid van het bewijsmateriaal heeft aangetast, net als in het positieve recht, tot een uitsluiting van de betrokken informatie blijven leiden (**overwegingen nrs. 44-50**).

5. Recht op toegang Zoals momenteel in het voorstel is geregeld, voldoet het recht op toegang tot het strafdossier niet aan alle vereisten die zijn vastgelegd in de artikelen 14 en 15 van Richtlijn 2016/680/EG. De Autoriteit wijst op bepaalde aandachtspunten voor de

Advies 77/2020 25/25

aanvrager indien hij overweegt het recht van toegang van de betrokkene op deze basis op te bouwen (**overwegingen nrs. 51-62**).

6. Uitbreiding van de (niet geheime) zoeking in een informaticasysteem De Autoriteit neemt nota van de wijzigingen die door het voorstel zijn aangebracht naar aanleiding van het arrest van het Grondwettelijk Hof ter zake en merkt alleen op dat de instemming van de gebruikelijke gebruiker van het systeem op zich geen garantie vormt voor de eerbiediging van de rechten van derden van wie de gegevens betrokken zijn bij de uitbreiding van de zoeking (**overwegingen nrs. 63-65**).



Alexandra Jaspar
Directeur van het Kenniscentrum

