



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. COMPETENCE DE L'AUTORITE

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).

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 inexactes¹⁶, 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.

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.

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-HOLSTEIN c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN 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-HOLSTEIN c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN 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 bénéficiaire, 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

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**).

(sé) Alexandra Jaspar
Directrice du Centre de Connaissances