



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 45/2026 du 13 mars 2026

Objet : Avis concernant un Avant-projet de loi relative aux points de contact de certaines entreprises qui sont chargés de répondre aux demandes de fourniture ou de gel de preuves électroniques des autorités et mettant en œuvre le règlement relatif aux preuves électroniques (CO-A-2026-016).

Mots-clés : preuves électroniques ; procédure pénale ; injonctions ; représentant légal, établissement ; EPOC ; EPOC-PR.

Version originale

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier ses 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 de Madame Vanessa Matz, ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'Etat, du Numérique et de la Politique Scientifique, recevable le 20 janvier 2025 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 13 mars 2026, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant **un avant-projet de loi relative aux points de contact de certaines entreprises qui sont chargés de répondre aux demandes de fourniture ou de gel de preuves électroniques des autorités et mettant en œuvre le règlement relatif aux preuves électroniques** (ci-après « **le Projet** »). Le Projet transpose la Directive (UE) n° 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 *établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales* (ci-après, « **la Directive** »).
2. Cette Directive « *s'applique aux décisions et aux injonctions visant à obtenir des preuves électroniques sur la base du règlement (UE) 2023/1543* [¹ (ci-après, « **le Règlement Preuves électroniques** »)], *de la directive 2014/41/UE* [²] *et de la convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne. Elle s'applique aussi aux décisions et aux injonctions visant à obtenir des preuves électroniques sur la base du droit national qui sont adressées par un État membre à une personne physique ou morale agissant en qualité de représentant légal ou d'établissement désigné d'un fournisseur de services sur le territoire de cet État membre* »³.
3. Le Projet **concerne principalement la transposition de la Directive et comporte des dispositions qui vont au-delà de son champ d'application**. Ainsi en principe, **ni le Projet, ni le présent avis ne concernent les conditions dans lesquelles les décisions et injonctions visées par ce Règlement peuvent être émises et adressées à des fournisseurs de services**.
4. L'exposé des motifs précise également que le Projet **met en œuvre (en son Chapitre 3) le Règlement Preuves Electroniques et modifie la Loi du 13 juin 2005 relative aux communications électroniques** (ci-après, « **LCE** »), « *pour apporter des corrections à certaines dispositions introduites dans cette loi par la* » Loi du 20 juillet 2022 *relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités*.

¹ Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 *relatif aux injonctions européennes de production et aux injonctions européennes de conservation de preuves électroniques, dans les procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale*.

² Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 *concernant la décision d'enquête européenne en matière pénale*.

³ Article 1er, 2., de la Directive.

II. EXAMEN DU PROJET

Le présent avis est structuré comme suit :

II.1. Portée de la Directive et du Projet	3
II.2. Commentaire général concernant l'impact du Projet sur la protection des données	6
II.3. Commentaires particuliers concernant le dispositif du Projet.....	9
II.3.1. Habilitation du Roi visée à l'article 2, al. 2, du Projet (véhicules connectés).....	9
II.3.2. Coordonnées des points de contact et modes de communication.....	10
II.3.3. Responsabilités au regard des traitements de données à caractère personnel	13
II.3.4. Habilitation du Roi et de l'IBPT visées à l'article 11, § 2, als 2 et 3, du Projet (modalités de la consultation des coordonnées de contact des cellules de coordination).....	15
II.3.5. Habilitation du Roi visée à l'article 16 du Projet (modalité de l'obligation de collaboration légale)	16
II.3.6. Le « service désigné par le Roi »	17

II.1. Portée de la Directive et du Projet

5. Conformément à son article 1^{er}, la Directive « *établit des règles relatives à la **désignation d'établissements désignés et de représentants légaux** de certains fournisseurs de services qui proposent des services dans l'Union pour la réception, le respect et l'exécution des décisions et des injonctions émises par les autorités compétentes des États membres aux fins de l'obtention de preuves dans le cadre de procédures pénales* » (mis en gras par l'Autorité). En substance, l'objectif de la Directive est de faciliter la possibilité pour les autorités d'émission d'un Etat Membre d'adresser au sein de l'Union, leurs **demandes (contraignantes – soit des injonctions de production (adressées via un EPOC)⁴ (demande de fourniture de preuves électroniques, au sens du Projet) ou de conservation (adressées via EPOC PR)⁵ (demande de gel de preuves électroniques, au sens du Projet) aux fournisseurs d'une série de services numériques**, en imposant à ces derniers l'obligation de **désigner au moins un destinataire** (un établissement⁷ ou un représentant légal⁸ ; soit un **point de contact** au sens du Projet et du présent Avis) chargé de **recevoir, respecter et exécuter** lesdites demandes. Remarque : dans le cadre du présent Avis, l'Autorité utilisera les termes **d'injonctions de production ou de conservation de preuves électroniques**.

⁴ « Certificat d'injonction européenne de production » ou « *European Production Order Certificate* ».

⁵ « Certificat d'injonction européenne de conservation » ou « *European Preservation Order Certificate* ».

⁶ L'Autorité reprend ici la terminologie du Projet qui, plutôt que de se référer aux « décisions » et « injonctions » se réfère aux « demandes », étant entendu que sont seules concernées des demandes contraignantes à l'égard de leurs destinataires.

⁷ Défini à l'article 2, 4), de la Directive.

⁸ Défini à l'article 2, 6), de la Directive.

6. Selon l'exposé des motifs, les dispositions pertinentes suivantes du droit positif nécessitent une révision en profondeur afin de transposer la Directive : l'article 127/3 de la LCE (**Cellule de coordination** à constituer auprès de chaque opérateur), l'article 2 de l'Arrêté Royal 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques (mise en place auprès de chaque opérateur d'une **Cellule de coordination de la Justice**) et l'article 2 de l'Arrêté Royal du 12 octobre 2010 *déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité permettant aux services de renseignements et de sécurité d'adresser leur demande de preuves électroniques à la Cellule de coordination de la Justice.*
7. Les **fournisseurs de services visés par la Directive** sont⁹ les fournisseurs de :
- **Services de communications électroniques** tels que définis à l'article 2, 4), de la Directive (UE) n° 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 *établissant le code des communications électroniques européen*¹⁰ ;
 - **Services d'attribution de noms de domaine sur l'internet et de numérotation IP**, tels que l'attribution d'adresses IP, les services du registre de noms de domaine, les services du bureau d'enregistrement de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire liés aux noms de domaine ;
 - **Et d'autres services de la société de l'information** visés à l'article 1^{er}, 1., b), de la Directive (UE) n° 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 *prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information*¹¹, qui permettent à leurs utilisateurs de

⁹ Conformément à l'article 2, 1), de la Directive, sont exclus d'emblée certains services financiers.

¹⁰ Soit : « le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus, comprend les types de services suivants :

a) un « **service d'accès à l'internet** » défini à l'article 2, deuxième alinéa, point 2, du règlement (UE) 2015/2120 [(soit : « un service de communications électroniques accessible au public, qui fournit un accès à l'internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés »)];

b) un **service de communications interpersonnelles**; et

c) des services consistant entièrement ou principalement en la **transmission de signaux** tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion » (mis en gras par l'Autorité).

Le **service de communications interpersonnelles** est défini par le 5) de la même disposition comme :

« un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service ».

¹¹ Soit : « tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

communiquer entre eux ou qui permettent de **stocker ou de traiter d'une autre manière des données pour le compte des utilisateurs** auxquels le service est fourni, **à condition que** le stockage des données soit une composante déterminante du service fourni à l'utilisateur.

8. Les fournisseurs de services ont en outre une **obligation de notification** du destinataire désigné. L'article 4, 1., de la Directive prévoit que « *Les États membres veillent à ce que chaque fournisseur de services établi sur leur territoire ou proposant des services sur leur territoire **notifie par écrit, à l'autorité centrale de l'État membre dans lequel son établissement désigné est établi ou dans lequel son représentant légal réside, désignée conformément à l'article 6, les coordonnées de contact** de cet établissement ou de ce représentant légal, **et toute modification de ces données*** » (mis en gras par l'Autorité). Et selon le 4. de la même disposition, « *Les États membres veillent à ce que les informations qui leur sont notifiées conformément au présent article soient **mises à la disposition du public sur une page internet spécifique du Réseau judiciaire européen en matière pénale***. Les États membres veillent à ce que ces informations soient régulièrement mises à jour. Ces informations peuvent être diffusées davantage pour en faciliter l'accès par les autorités compétentes » (mis en gras par l'Autorité). **L'autorité centrale** garantit l'application cohérente et proportionnée de la Directive et se coordonne et coopère avec les autres autorités centrales¹².
9. La Directive **s'applique** aux fournisseurs de services qui « ***proposent leurs services dans l'Union*** »¹³ **et ne s'applique pas** aux fournisseurs de services qui sont établis sur le territoire d'un seul Etat membre et proposent des services **exclusivement sur le territoire** de cet Etat membre.
10. Le Projet **va cependant au-delà du champ d'application de la Directive** en ce que :
 - Il s'applique à ces derniers services qu'il définit comme « ***fournisseurs de services nationaux*** » ;

Aux fins de la présente définition, on entend par:

i) «à distance», un service fourni sans que les parties soient simultanément présentes;

ii) «par voie électronique», un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques;

iii) «à la demande individuelle d'un destinataire de services», un service fourni par transmission de données sur demande individuelle.

Une liste indicative des services non visés par cette définition figure à l'annexe I ».

¹² Article 6 de la Directive.

¹³ Voir à ce sujet l'article 2, 2) et 3), de la Directive.

- Il s'applique **au-delà de l'hypothèse des procédures pénales** en ce que les demandes de production ou de conservation de preuves électroniques peuvent être adressées par des autorités en dehors du cadre de ces procédures (comme dans l'hypothèse des services de renseignements et de sécurité) ;
- Il vise explicitement les fournisseurs de **réseaux de communications électroniques**. L'exposé des motifs indique que « *le présent projet de loi vise aussi expressément les opérateurs qui fournissent des réseaux de communications électroniques. Il convient cependant de noter que ces opérateurs sont généralement également des opérateurs qui fournissent des services de communications électroniques* » ;
- Il vise les **fabricants et loueurs de certains véhicules connectés** ;
- Il **définit plus largement** le concept de « *preuves électroniques* ».

11. L'Institut (ci-après, « **l'Institut** » ou « **l'IBPT** ») est désigné comme **autorité centrale** au sens de l'article 6, 1., de la Directive, par l'article 8 du Projet.

II.2. Commentaire général concernant l'impact du Projet sur la protection des données

12. Avant tout, l'Autorité insiste sur le fait que le Projet ne porte pas sur les conditions dans lesquelles les décisions et injonctions concernées peuvent être émises et adressées à des fournisseurs de services. **Par conséquent, le Projet ne porte pas sur la substance des éléments essentiels des traitements de données à caractère personnel mis en œuvre dans le cadre de demandes et communications de preuves électroniques.** En ce sens, **son impact sur le plan de la protection des données est limité** à l'implication, dans ce contexte, d'un point de contact (un établissement désigné, un représentant légal, une cellule de coordination ; soit un destinataire des données constituant un responsable du traitement supplémentaire) du prestataire de service à qui une demande est adressée (également un responsable du traitement) et à certains traitements de données relatifs à celui-ci (avis de sécurité et publication de données à son sujet). Autrement dit, le présent Avis **ne porte pas sur les conditions dans lesquelles les autorités compétentes peuvent adresser des injonctions à certains prestataires de services de l'économie numérique, ni sur la question de savoir quels prestataires peuvent, conformément au droit applicable, être l'objet de telles injonctions.**
13. Cela étant précisé, **il va de soi qu'un point de contact ne pourra être tenu de traiter des données à caractère personnel en exécution du Projet que dans la mesure où l'injonction qui lui est adressée existe dans le droit applicable et y est conforme**, sauf à être illicite (article

5, 1., a), du RGPD). A cet égard, **il appartient au Demandeur de notamment s'assurer que les prestataires de services qui sont visés par le Projet en dehors et au-delà du champ d'application de la Directive puissent bien être l'objet d'injonctions** de production ou de conservation de preuves électroniques en vertu du droit belge, **à la fois dans et en dehors des procédures pénales**, selon les cas visés par le Projet. A défaut bien entendu, un Point de contact ne pourrait devoir être mis en œuvre aux fins de répondre à de telles injonctions.

14. Inversement, au regard de l'application des articles 8 CEDH, 22 de la Constitution et 6, 1., c), du RGPD, **le Projet ne peut pas être lu comme pouvant fonder juridiquement les obligations des prestataires de services concernés de produire ou conserver des preuves électroniques.** Systématiquement, une base légale doit être invoquée en combinaison avec le Projet à l'appui des injonctions adressées aux Points de contacts concernés.
15. Dans ce contexte, l'Autorité est d'avis que **l'exposé des motifs du Projet (à tout le moins) devrait rappeler les fondements légaux des injonctions qui peuvent être adressées en droit belge aux prestataires concernés et tombent dans le champ d'application du Projet.**
16. Les questionnements juste évoqués ne sont pas analysés dans le cadre du présent Avis : ils doivent l'être dans le cadre de l'analyse des autres règles du rang de loi applicables aux injonctions de production ou de conservation de preuves électroniques.
17. Cela étant précisé, l'Autorité attire l'attention du Demandeur sur le **scénario visé à l'article 14, alinéa 3, du Projet**, qui est **susceptible d'être problématique dans son principe, sur le plan des règles de protection des données.** Cette disposition est rédigée comme suit :

*« Lorsqu'une autorité belge compétente adresse une demande de fourniture ou de gel de preuves électroniques à un fabricant ou loueur de véhicules connectés et que ce dernier **ne peut répondre à cette demande sans l'aide d'un tiers, tel un sous-traitant ou un fournisseur**, ce fabricant ou ce loueur prend les mesures suivantes :*

1° soit sa cellule de coordination obtient l'aide de ce tiers de manière à pouvoir répondre à la demande de l'autorité, ou ;

2° soit il fait en sorte que ce tiers dispose d'une cellule de coordination conforme aux exigences de la présente loi » (mis en gras par l'Autorité).
18. Le Projet doit spécifier que **cette obligation ne vaut que pour les preuves électroniques dont le traitement relève de la responsabilité du fabricant ou du loueur de véhicules connectés** concerné (au sens de la responsabilité au regard du traitement, conformément au RGPD). Il est effec-

tivement nécessaire dans le cas visé par le Projet que le « tiers » (« tel un sous-traitant ou un fournisseur ») soit au regard du traitement de données à caractère personnel concernées (les preuves électroniques) un sous-traitant du fabricant ou du loueur au sens du RGPD. Dans le cas contraire, où le « tiers » est le responsable du traitement des données souhaitées (les preuves électroniques), le Projet devrait alors directement régler son éventuelle obligation de mettre en place une cellule de coordination, de la même manière qu'il y procède pour les autres prestataires de services¹⁴. Car dans ce scénario, en tant que responsable du traitement, il ne pourrait devoir, au regard des données concernées, se soumettre à des injonctions du fabricant ou loueur de véhicule connecté.

19. Ensuite, l'Autorité rappelle également que tout point de contact prévu par le Projet **dans le champ d'application de la Directive, doit en outre être prévu conformément à la Directive elle-même**. Un point de contact qui devrait être prévu d'une manière non conforme à la Directive ne pourrait en conséquence licitement traiter les données à caractère personnel concernées par les injonctions de production ou de conservation de preuves électroniques.
20. Dans la même logique, **l'acception étendue du concept de « preuves électroniques »**¹⁵ retenu dans le Projet **ne sera applicable que dans des hypothèses d'injonctions en dehors du champ d'application de la Directive et du Règlement Preuves Electroniques**. A cet égard, l'Autorité comprend qu'en pratique, le point de contact concerné pourra d'office distinguer si une demande lui est adressée en exécution du droit belge exclusivement ou du Règlement Preuves Electroniques, dès lors que ce dernier nécessite notamment l'utilisation d'un EPOC ou d'un EPOC PR via un système informatique décentralisé prévu par le Règlement Preuves Electroniques que doivent utiliser les autorités compétentes et les prestataires de services.

¹⁴ Et de nouveau, à supposer qu'il existe bien en droit positif la possibilité pour des autorités compétentes d'adresser des injonctions de production ou de conservation de preuves électroniques au type de prestataire de service alors visé.

¹⁵ L'exposé des motifs indique ce qui suit à ce propos :

« La définition de preuves électroniques pour l'application de la présente loi est plus large que la définition de ces mêmes termes dans le règlement relatif aux preuves électroniques [chapitre 3]. En effet, alors que ce règlement ne vise que les fournisseurs de services, le projet de loi vise les entreprises concernées, ce qui est plus large. **Alors que ce règlement exclut de son champ d'application les preuves électroniques collectées en temps réel, le projet de loi ne fait pas cette exclusion**, vu qu'une demande de preuves électroniques peut être adressée au point de contact de l'entreprise concernée sur base du droit belge (Code d'instruction criminelle), qui vise tout type de preuves électroniques. Par ailleurs, la définition de preuves électroniques dans ce règlement vise « un certificat d'injonction européenne de production (EPOC) » et « un certificat d'injonction européenne de conservation (EPOC-PR) », qui sont des termes spécifiques à ce règlement, alors que la directive relative aux preuves électroniques couvre d'autres instruments juridiques que ce règlement (voir exposé général, point 1). Dans le projet de loi, la définition de preuves électroniques fait référence aux **métadonnées plutôt qu'aux données de trafic** (notion reprise dans le règlement relatif aux preuves électroniques) et ce pour les raisons suivantes.

D'abord, la notion de métadonnées est une notion plus moderne que la notion de données de trafic. Ainsi, la notion de métadonnées remplace progressivement la notion de trafic dans la loi du 13 juin 2005 relative aux communications électroniques.

La notion de métadonnées permet de prendre en compte les **données de signalisation** en dehors d'une communication de contenu. Il est par exemple possible que des signaux soient échangés entre un téléphone mobile et le réseau d'un opérateur de communications électroniques sans qu'il n'y ait une communication de contenu. Ces échanges de signaux techniques permettent au réseau de l'opérateur de rendre possible un appel d'un de ses clients à tout moment (voir à cet égard l'article 123 de la loi du 13 juin 2005 relative aux communications électroniques) » (mis en gras par l'Autorité).

21. Enfin, au-delà des traitements de données liés aux injonctions elles-mêmes dont il vient d'être question et qui ne sont pas abordés dans le présent Avis, **les traitements de données à caractère personnel suivants découlent quant à eux directement du Projet lui-même (et selon, de la Directive elle-même)** : la communication et la mise à disposition des coordonnées de contact des points de contact¹⁶ et la nécessité pour chaque membre d'une cellule de coordination établie en Belgique de disposer d'un **avis de sécurité positif**, visé à l'article 36 § 1er, 1^o, de la loi 11 décembre 1998 *relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé, sans être un avis de sécurité positif avec avertissement administratif ou mise en garde individuelle* (article 10, § 2, du Projet). L'Autorité observe d'emblée que l'exigence d'un avis de sécurité et les **traitements de données rendus nécessaires par l'obtention de cet avis de sécurité positif n'appellent pas de commentaire particulier.**

II.3. Commentaires particuliers concernant le dispositif du Projet

II.3.1. Habilitation du Roi visée à l'article 2, al. 2, du Projet (véhicules connectés)

22. Les définitions des concepts de « *véhicule connecté* » et de « *fabricants et loueurs de véhicules connectés* » (propres au Projet, en dehors du champ d'application de la Directive) participent directement à la détermination des éléments essentiels des traitements de données à caractère personnel qui ont lieu dans le contexte du Projet. Notamment, l'identification de ces prestataires de service participe à la détermination de la finalité, des responsables du traitement et des destinataires des données à caractère personnel dans le contexte des traitements de données nécessaires à la mise en œuvre des injonctions de production ou de conservation de preuves électroniques. L'article 2, al. 2, du Projet, prévoit que « *Le Roi peut, après avis des autorités de protection des données compétentes au niveau fédéral et de l'Institut, préciser ce qu'il faut entendre par* » ces deux concepts. **L'exposé des motifs justifie cette habilitation comme suit :**

« *L'avant-projet de loi définit le « véhicule connecté » (article 2, 7^o) et les « fabricants et loueurs de certains véhicules connectés » (article 2, 8^o). **Comme il s'agit d'une toute nouvelle législation et que des questions pourraient se poser en pratique si certains véhicules, fabricants ou loueurs répondent à ces définitions, la possibilité est donnée de trancher ces questions par le biais d'un arrêté royal. Cet arrêté n'a pas pour objet de compléter, avec des critères complémentaires, les définitions susmentionnées, mais d'appliquer ces définitions aux cas qui posent question (trancher les questions d'interprétation de la loi).** Ainsi, l'arrêté royal pourrait déterminer des catégories de véhicules connectés, de fabricants ou de loueurs de certains véhicules connectés qui*

¹⁶ Voir le considérant n° 24.

répondent ou non aux définitions visées à l'article 2, 7° et 8° » (mis en gras et souligné par l'Autorité).

23. L'Autorité est d'avis qu'il appartient au législateur de **définir avec la clarté requise**, conformément aux articles 8 CEDH et 22 de la Constitution les concepts de véhicules connectés et de fabricants et loueurs de ces véhicules, et **qu'il reviendra le cas échéant au pouvoir judiciaire et à la Cour constitutionnelle** (voire au législateur lui-même, via une loi interprétative) **de trancher les questions d'interprétation liées à l'application du Projet**. L'Autorité est d'Avis que le Projet **doit être adapté en conséquence** (suppression de l'habilitation du Roi envisagée) et invite le Demandeur à **s'en remettre *in fine* à la position qu'exprimerait le Conseil d'Etat à ce sujet et à adapter le Projet en conséquence**.

II.3.2. Coordonnées des points de contact et modes de communication

24. Le Projet prévoit la notification à l'Institut des « **coordonnées de contact** » de l'établissement désigné ou du représentant légal (article 6, §§ 1-3, du Projet, valable dans le champ d'application de la Directive), ainsi que la notification des coordonnées de contact de la cellule de coordination (article 11, § 1^{er}, du Projet, valable en dehors du champ d'application de la Directive). Il prévoit également la **mise « à disposition du public »** sur une page internet spécifique du Réseau judiciaire européen en matière pénale (article 6, § 4, du Projet, valable **dans le champ d'application de la Directive**), des informations notifiées à l'IBPT, qui « *peuvent être diffusées davantage pour en faciliter l'accès par les autorités compétentes* ». Cette mise à disposition du public est elle-même **prévue par l'article 4, 4., de la Directive précité¹⁷**. Enfin, il prévoit encore la **mise à disposition par l'IBPT des coordonnées de contact des cellules de coordination aux « autorités belges compétentes et au service désigné par le Roi »** (article 11, § 2, al. 2, du Projet, valable en dehors du champ d'application de la Directive).
25. Cependant, le Projet **ne définit pas ce que sont les « coordonnées de contact »** (dans et en dehors du champ d'application de la Directive) de telle sorte qu'en l'état, l'Autorité ne peut pas déterminer si en pratique, les coordonnées de contact comporteront des données à caractère personnel. Or il est probable que tel soit le cas et ce par exemple, à tout le moins dans l'hypothèse des cellules de coordination établies en Belgique dès lors que les membres de celles-ci doivent faire l'objet d'un avis de sécurité positif et d'une décision de l'IBPT (remarque : ces coordonnées ne sont toutefois pas mises à disposition du public général).

¹⁷ Voir le considérant n° 8.

26. Or dans ce contexte, si la communication éventuelle de données à caractère personnel de contact à l'IBPT et le cas échéant, aux autorités compétentes, n'est pas problématique au regard des règles de protection des données, **la mise à disposition du public général** (concrètement en l'occurrence, tout utilisateur d'internet) **de telles données à caractère personnel de contact ne semblerait par contre pas proportionnée** (ce qui est sans préjudice des règles régissant la publicité passive de l'administration, le cas échéant applicables) : un tel traitement s'il ne s'avérait pas nécessaire compte-tenu de la finalité du Projet violerait l'article 5, 1., c), du RGPD. L'Autorité **ne perçoit pas le motif pour lequel d'autres entités que l'IBPT, le cas échéant les autres autorités centrales européennes et les autorités compétentes concernées (soit le public cible des coordonnées de contact) devraient accéder à ces données**¹⁸ dont la publication pour le reste impliquerait des risques pour les personnes concernées compte-tenu de la sensibilité de leur rôle dans le cadre du Projet. Et à ce sujet, **l'exposé des motifs se limite à se référer à l'article 4, 4., de la Directive**, dans lequel se trouve effectivement la source de l'obligation de publication concernée. Cela étant précisé, le considérant n° 17 de la Directive **ne permet pas de remettre en cause le fait que le public-cible concerné par les données est limité aux autorités compétentes**¹⁹. Et l'article 4, 4., de la Directive doit être interprété et appliqué conformément aux articles 7 et 8 de la Charte.

27. Ces considérations valent d'autant plus que **dans le champ d'application du Règlement Preuves Electroniques, en vertu de l'article 19** de ce Règlement²⁰, la communication écrite entre les autorités compétentes et les établissements désignés ou représentants légaux des fournisseurs de service

¹⁸ D'ailleurs l'Autorité observe que pour ce qui concerne l'obligation de droit belge (en dehors du champ d'application de la Directive) de mettre en place une cellule de coordination, le Projet ne prévoit pas une telle mise à disposition du public de coordonnées de contact.

¹⁹ « [...] Les États membres devraient veiller à ce que les informations qui leur sont notifiées conformément à la présente directive soient mises à la disposition du public sur une page internet spécifique du Réseau judiciaire européen en matière pénale afin de faciliter **la coordination entre États membres** et de rendre plus aisé le recours à l'établissement désigné ou au représentant légal **par les autorités d'un autre État membre**. Les États membres devraient veiller à ce que ces informations soient régulièrement mises à jour. Il devrait également être possible de diffuser davantage les informations afin de faciliter **l'accès des autorités compétentes à ces informations**, par exemple par la voie de sites intranet ou de forums et plateformes spécifiques » (mis en gras par l'Autorité).

²⁰ Cette disposition est rédigée comme suit :

« 1. La **communication écrite entre les autorités compétentes et les établissements désignés ou les représentants légaux** au titre du présent règlement, y compris l'échange des formulaires prévus par le présent règlement et des données demandées dans le cadre d'une injonction européenne de production ou d'une injonction européenne de conservation, **s'effectue au moyen d'un système informatique décentralisé sécurisé et fiable** (ci-après dénommé «système informatique décentralisé»).

2. Chaque État membre **veille à ce que les établissements désignés ou les représentants légaux des fournisseurs de services situés dans cet État membre aient accès au système informatique décentralisé** par l'intermédiaire de leur système informatique national respectif.

3. Les fournisseurs de services **veillent à ce que leurs établissements désignés ou leurs représentants légaux puissent utiliser le système informatique décentralisé via le système informatique national** concerné afin de recevoir les EPOC et les EPOC-PR, d'envoyer les données demandées à l'autorité d'émission et de communiquer d'une autre manière avec l'autorité d'émission et l'autorité chargée de la mise en œuvre, comme le prévoit le présent règlement.

4. La communication écrite entre les autorités compétentes au titre du présent règlement, y compris l'échange des formulaires prévus par le présent règlement et des données demandées dans le cadre de la procédure de mise en œuvre prévue à l'article 16, ainsi que la communication écrite avec les agences ou organes compétents de l'Union, s'effectuent au moyen du système informatique décentralisé.

5. **Lorsque la communication au moyen du système informatique décentralisé conformément au paragraphe 1 ou 4 n'est pas possible** en raison, par exemple, d'une panne du système informatique décentralisé, de la nature des

concernés **doit avoir lieu via le « système informatique décentralisé »** prévu par cette disposition²¹ de telle sorte qu'*a priori*, l'Autorité ne perçoit pas pourquoi les coordonnées de contact ne seraient pas uniquement disponibles via ce système, aux destinataires authentifiés pertinents.

28. **Tel qu'il est rédigé, le Projet ne pourra pas fonder une telle mise à disposition du public de données à caractère personnel.** Si le Demandeur envisageait la mise à disposition du grand public de données à caractère personnel via internet, il conviendrait à tout le moins de **définir ce que sont les « coordonnées de contact » et d'en motiver et organiser le régime de publicité active** (le cas échéant, distinction entre les données, selon qu'elles sont accessibles au grand public ou aux autorités compétentes seulement). L'Autorité invite le Demandeur à se référer aux considérations développées dans **plusieurs Avis qu'elle a déjà rendus en la matière** : Avis n° 58/2024 du 27 juin 2024 *concernant l'application de l'article 6, § 3, alinéa 1er, 2e tiret des Décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française du 16 mai 2019 relatifs à la publicité de l'administration dans les institutions bruxelloises (CO-A-2024-187)* ; Avis n° 05/2024 du 19 janvier 2024 *concernant un avant-projet de loi-programme, titre 5 Indépendants (CO-A-2023-497)*, considérants nos 44-56 ; Avis n° 154/2023 du 20 octobre 2023 *concernant un avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée (CO-A-2023-407)*, considérants nos 28-45 ; Avis n° 131/2023 du 8 septembre 2023 *concernant un amendement n° 4 du projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration et abrogeant la loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes (CO-A-2022-316)* ; Avis n° 42/2023 du 9 février 2023 *concernant un avant-projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration (CO-A-2022-311)* ; Avis n° 102/2020 du 19 octobre 2020 *concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles Capitale du 25 avril 2019 réglant la forme ainsi que les procédés d'information et de mise à disposition des décisions prises en matière de permis d'urbanisme, de permis de lotir et de certificat d'urbanisme par le collège des bourgmestre et échevins, le fonctionnaire délégué et le Gouvernement (CO-A-2020-100)*, considérants nos 18 et s.

*documents à transmettre, de contraintes techniques telles que le volume des données, de contraintes juridiques liées à la recevabilité des données demandées en tant que preuves ou aux exigences en matière de criminalistique applicables aux données demandées, ou de circonstances exceptionnelles, la transmission est effectuée à l'aide des **moyens de substitution** les plus appropriés, compte tenu de la nécessité de garantir la rapidité, la sécurité et la fiabilité de l'échange d'informations, et de permettre au destinataire d'en établir l'authenticité.*

6. *Lorsqu'une transmission est effectuée par des moyens de substitution comme le prévoit le paragraphe 5, l'autorité à l'origine de la transmission enregistre, sans retard injustifié, la transmission, y compris, s'il y a lieu, la date et l'heure de la transmission, l'expéditeur et le destinataire, le nom du fichier et sa taille, dans le système informatique décentralisé » (mis en gras par l'Autorité).*

²¹ À propos de celui-ci, voir le Règlement d'exécution (UE) 2025/1550 de la Commission du 28 juillet 2025 *établissant les spécifications et autres exigences techniques pour le système informatique décentralisé visées par le règlement (UE) 2023/1543 du Parlement européen et du Conseil et le Règlement (UE) 2022/850 du Parlement européen et du Conseil du 30 mai 2022 relatif à un système informatisé pour l'échange électronique transfrontière de données dans le domaine de la coopération judiciaire en matière civile et pénale (système e-CODEX), et modifiant le règlement (UE) 2018/1726.*

29. L'Autorité insiste également, dans le cadre du Projet, sur l'importance de **la qualité des coordonnées de contact communiquées et du mode de communication applicable aux échanges entre autorités compétentes et points de contacts** qui doivent permettre de **joindre avec certitude, exclusivement et de manière sécurisée le point de contact effectivement désigné par l'entreprise concernée**. Sur ce point néanmoins, **l'Autorité concède qu'il n'est pas exclu que les règles qui régissent les injonctions de production ou de conservation de preuves électroniques ou la coopération en la matière prévoient elles-mêmes directement des règles spécifiques en la matière**. Il en est par exemple ainsi dans le champ d'application du Règlement Preuves Electroniques (voir le considérant n° 27 ; voir également les considérants nos 36-39 concernant l'habilitation du Roi à propos des modalités de la collaboration légale).
30. S'agissant des cellules de coordination (en dehors du champ d'application de la Directive), l'Autorité est d'avis que le Projet peut prévoir que « *Les entreprises concernées suivantes ou leur cellule de coordination notifient à l'institut, conformément aux modalités pratiques qu'il fixe, les coordonnées de contact de cette cellule **que le Roi fixe*** » (mis en gras par l'Autorité) quand bien même seraient concernées des données à caractère personnel, dès lors que le Projet limite l'accessibilité de ces données (présentant pour le reste un faible niveau d'ingérence dans les droits et libertés des personnes concernées) aux autorités compétentes, dans le contexte des injonctions de production ou de conservation des preuves électroniques.

II.3.3. Responsabilités au regard des traitements de données à caractère personnel

31. Sur la base des articles 3, al. 3²², 4, § 3²³, 9, § 1^{er} 24 et § 2²⁵, 10, § 3, al. 1^{er} 26, 12²⁷, 15, § 1^{er} 28 et surtout des articles 14, als 1^{er} et 2²⁹, et 15, § 3³⁰, du Projet, qui prévoient que les points de contact doivent disposer des pouvoirs et des ressources nécessaires pour se conformer aux injonctions et sont solidairement responsables de l'éventuel non-respect d'obligations découlant du cadre légal applicable lors de la réception de demandes de production ou de conservation de preuves électroniques, **l'Autorité est d'avis que le point de contact** (qu'il soit un établissement désigné, un représentant légal ou une cellule de coordination) **et le fournisseur de service concerné sont des responsables conjoints des traitements de données impliqués par les injonctions de production ou de conservation de preuves électroniques.**
32. **L'IBPT** quant à lui sera **responsable des traitements de données à caractère personnel nécessaires à l'exécution des missions et obligations qui lui incombent en vertu du Projet**, notamment en tant qu'autorité centrale, conformément à la pratique d'Avis de l'Autorité³¹. Notamment,

²² Selon lequel : « L'établissement désigné est doté de la personnalité juridique et **est chargé** par le fournisseur de services de la réception, **du respect et de l'exécution** des demandes de fourniture ou de gel de preuves électroniques, émises par les autorités compétentes des États membres dans le cadre de procédures pénales conformément [...] » (mis en gras par l'Autorité).

²³ Selon lequel : « Le représentant légal est une personne physique ou morale qui **est chargée** par le fournisseur de services de la réception, **du respect et de l'exécution** des demandes de fourniture ou de gel des preuves électroniques, émises par les autorités compétentes des États membres dans le cadre de procédures pénales conformément [...] » (mis en gras par l'Autorité).

²⁴ Selon lequel : « La cellule de coordination comprend une ou plusieurs personnes physiques ou une personne morale et **est chargée** par l'entreprise concernée de la réception, **du respect et de l'exécution** des demandes de fourniture ou de gel de preuves électroniques, émises par les autorités belges compétentes [...] » (mis en gras par l'Autorité).

²⁵ Selon lequel : « Sans préjudice de réponses envoyées de manière automatisée, **seuls les membres de la cellule de coordination peuvent répondre** aux demandes de fourniture ou de gel de preuves électroniques des autorités belges compétentes.

Ils peuvent cependant, **sous leur surveillance et responsabilité** et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'entreprise concernée » (mis en gras par l'Autorité).

²⁶ Selon lequel : « La cellule de coordination est organisée de manière à pouvoir répondre dans le délai imparti aux demandes de fourniture ou de gel de preuves électroniques des autorités belges compétentes ».

²⁷ Les demandes doivent en principe toujours être adressées à la cellule de coordination, sauf lorsque l'autorité concernée « justifie, dans un acte interne et le cas échéant de manière succincte, que ce n'est pas opportun en raison d'un manque de fiabilité de cette cellule ou d'un de ses membres ».

²⁸ Qui vise l'obligation de coopérer (conformément au cadre légal applicable) de l'établissement désigné établi en Belgique et du représentant légal qui y réside, ainsi que de la cellule de coordination.

²⁹ Selon lesquels : « Les entreprises concernées dotent leurs établissements désignés et leurs représentants légaux **des pouvoirs et des ressources nécessaires pour se conformer** aux demandes de fourniture ou de gel de preuves électroniques que les autorités compétentes des États membres leur adressent.

Les entreprises concernées dotent leur cellule de coordination **des pouvoirs et des ressources nécessaires pour se conformer** aux demandes relatives à la fourniture ou au gel de preuves électroniques que les autorités belges compétentes leur adressent » (mis en gras par l'Autorité).

³⁰ Selon lequel : « Tant l'établissement désigné, le représentant légal que l'entreprise concernée **sont tenus solidairement responsables du non-respect** d'obligations découlant du cadre légal applicable lors de la réception de demandes de fourniture ou de gel de preuves électroniques, **de sorte que chacun d'entre eux peut être soumis à des sanctions en cas de manquement de l'un d'entre eux** » (mis en gras par l'Autorité).

³¹ Pour un rappel de cette dernière, voir l'Avis n° 36/2026 du 4 mars 2026 concernant un avant-projet de loi créant un service de signatures électroniques qualifiées (CO-A-2026-002), considérant n° 26 et les développements dans l'Avis n° 08/2026 du 20 janvier 2026 concernant un avant-projet de loi portant modification de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale et de la loi du 17 juillet 2001 relative à l'autorisation pour les services publics fédéraux de s'associer en vue de l'exécution de travaux relatifs à la gestion et à la sécurité de l'information (CO-A-2025-207), considérant n° 14 et les références citées.

l'IBPT sera responsable de la mise à disposition du public et des autorités compétentes des coordonnées de contact et de leur mise à jour, selon les obligations consacrées dans le Projet. Autrement dit, cette responsabilité au regard du traitement de données sera engagée au regard du traitement des informations **qui sont notifiées** à l'IBPT par les entreprises concernées et le cas échéant, des informations qui sont **adaptées par l'IBPT lui-même**³². Notamment, cela implique que l'IBPT doit adapter sans délai les coordonnées de contact lorsqu'il reçoit des entreprises concernées une modification de celles-ci. Il est également important qu'il agisse dans le cadre de ses compétences afin de veiller à la mise en œuvre du Projet, lorsqu'il dispose d'éléments probants justifiant de l'inexactitude de coordonnées de contact. Toutes les démarches entreprises concernant le caractère exact et à jour des données traitées sont importantes à la fois pour garantir que le Projet atteigne sa finalité (mise en œuvre des injonctions de production ou conservation de preuves électroniques) et afin d'éviter les violations de données (communication d'une injonction à un mauvais destinataire).

II.3.4. Habilitation du Roi et de l'IBPT visées à l'article 11, § 2, als 2 et 3, du Projet (modalités de la consultation des coordonnées de contact des cellules de coordination)

33. Les alinéas 2 et 3 du paragraphe 2 de l'article 11 du Projet sont rédigés comme suit : « *En respectant les **restrictions fixées par le Roi**, après avis des autorités de protection des données compétentes au niveau fédéral et de l'Institut, ce dernier permet aux autorités belges compétentes et au service désigné par le Roi de consulter les coordonnées de contact des cellules de coordination. **L'Institut détermine les modalités pratiques** de cette consultation* » (mis en gras par l'Autorité).
34. L'Autorité invite avant tout le Demandeur à se référer aux considérants nos 44 à 46 de son Avis n° 12/2026 du 3 février 2026 *sur la proposition de loi « modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel en ce qui concerne les décisions anticipées » (DOC 56, 0218/001) (CO-A-2026-011)*, où elle rappelle les conditions dans lesquelles, selon la jurisprudence de la Cour constitutionnelle et la légisprudence du Conseil d'Etat, un pouvoir réglementaire peut être attribué à une autorité non gouvernementale telle que l'IBPT³³.
35. Dans ce contexte, **elle est d'avis que le Demandeur doit vérifier si l'article 11, § 2, als 2 et 3 du Projet ne peut pas se limiter à prévoir que le Roi détermine les conditions dans lesquelles** les autorités compétentes consultent auprès de l'IBPT les coordonnées de contact des cellules

³² Voir l'article 11, § 2, al. 1er, du Projet.

³³ Voir également les considérants nos 9 à 13 de l'Avis n° 28/2026 du 23 février 2026 *concernant une proposition de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques pour permettre au consommateur de disposer systématiquement du plan tarifaire le plus avantageux (CO-A-2025-217)*.

de coordination conformément au droit applicable, plutôt que de se référer à des « *restrictions* » et à des « *modalités pratiques* » fixées respectivement par le Roi et l'IBPT. Etant entendu que **le Projet devra toujours être lu en combinaison avec les cadres législatifs applicables *in concreto*** qui justifieront et fonderont en droit la consultation des coordonnées concernées.

II.3.5. Habilitation du Roi visée à l'article 16 du Projet (modalité de l'obligation de collaboration légale)

36. L'article 16 du Projet, repris dans une section intitulée « **Modalités de l'obligation de collaboration légale** », est rédigé comme suit :

*« **Le Roi peut déterminer**, après avis des autorités fédérales compétentes pour la protection des données et de l'Institut, **les règles régissant la collaboration** entre, d'une part, les entreprises concernées ou certaines catégories d'entre elles et, d'autre part, **le service désigné par le Roi** et les autorités belges compétentes ou certaines d'entre elles, **concernant les modalités pratiques pour la fourniture** des preuves électroniques et leur gel. Le non-respect par une entreprise concernée de l'arrêté royal est puni par les sanctions prévues à l'article 655 ou à l'article 656 du nouveau Code pénal »* (mis en gras par l'Autorité).

37. L'exposé des motifs indique qu'il s'agit d'une reprise, moyennant simplification et extension compte-tenu du champ d'application élargi du Projet (qui ne vise plus seulement les cellules de coordination déjà existantes en droit positif), de **l'article 127/3, § 4, de la LCE**³⁴. Ces modalités sont **notamment** importantes afin de garantir de joindre avec certitude, exclusivement et de manière sécurisée le point de contact effectivement désigné par l'entreprise concernée³⁵.

38. **S'il appartient au Conseil d'Etat de se prononcer à ce sujet en dernier ressort, l'Autorité s'interroge néanmoins sur la portée de cette habilitation au Roi** qui concrètement, semble

³⁴ Cette disposition est rédigée comme suit :

*« Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles. **Sont déterminés, entre autres, les éléments suivants, le cas échéant et par autorité concernée:***

- a) le mode de transfert, la forme et **le contenu des demandes et des réponses**;*
- b) le **degré d'urgence** de traitement des demandes;*
- c) le **délai de réponse**;*
- d) la **disponibilité requise du service**;*
- e) les modalités de test de la collaboration;*
- f) les tarifs de rétribution de cette collaboration.*

Si nécessaire et pour l'application du présent article, le Roi peut prévoir des règles différentes pour différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et la fourniture ou non d'un réseau de communications électroniques en Belgique » (mis en gras par l'Autorité).

³⁵ Voir le considérant n° 29.

permettre l'exécution d'autres dispositions du rang de loi dès lors que ça n'est pas le Projet lui-même, qui détermine les obligations des entreprises concernées, mais bien en principe les autres dispositions du rang de Loi qui consacrent la possibilité d'adresser des injonctions de production ou de gel de preuves électroniques ou régissent la coopération en la matière (dans le domaine pénal ou au-delà). L'article 127/3, § 4, de la LCE est d'ailleurs plus clair à cet égard, en ce qu'il indique explicitement que peuvent être concernés les délais de réponse ainsi que le contenu des demandes et des réponses. **Or ces modalités sont en principe déterminées dans les dispositions de rang de loi précitées ou doivent en principe en découler de telle sorte que ce sont ces dispositions qui doivent être exécutées par le Roi plutôt que le présent Projet.** Par exemple, le **Règlement Preuves électroniques** détermine lui-même les modalités de coopération entre les autorités compétentes et les entreprises concernées selon son champ d'application, y compris et notamment les délais de réponse, le contenu des demandes et la mise en place d'un système informatique décentralisé.

39. L'Autorité souligne au passage que **ces modalités se rapportent au traitement de données à caractère personnel et sont d'ailleurs déterminantes sur le plan de la protection des données**³⁶. Elle rappelle aussi qu'en tout état de cause, conformément aux articles 22 de la Constitution et 8 CEDH, les éléments essentiels des traitements de données à caractère personnel doivent être consacrés dans une norme du rang de loi.

II.3.6. Le « service désigné par le Roi »

40. Dans ses articles 11, § 1^{er}, als 3 et 4 (dispositions visant la demande de ce service adressée à l'Institut pour que ce dernier demande à une entreprise concernée de notifier sa cellule de coordination) et § 2, al. 2 (possibilité pour les autorités compétentes de consulter les coordonnées de contact des cellules de coordination), et 16 (modalités de coopération entre les entreprises et autorités compétentes), le Projet se réfère au « **service désigné par le Roi** ».
41. **L'exposé des motifs** indique qu'il s'agit « *en pratique, le NTSU, à savoir le National Technical and Tactical Support Unit des unités spéciales de la police fédérale* » (mis en gras par l'Autorité). Il comporte à certains endroits d'autres précisions en relation avec le rôle du NTSU. A ce propos : il met ce service en relation avec les « *autorités judiciaires* » ; il indique que « *le procureur du Roi ou le juge d'instruction rédige un réquisitoire adressé aux opérateurs concernés et ce réquisitoire est exécuté par les enquêteurs au moyen de l'introduction de demandes dans la plateforme informatique* ».

³⁶ Se référer à l'Avis du CEPD n° 7/2019 du 6 novembre 2019 concernant les propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, et par exemple, aux développements relatifs aux délais (courts) dans lesquels la conformité d'un EPOC au cadre normatif applicable doit être évaluée.

d'échange des demandes et des requêtes que le NTSU (le National Technical and Tactical Support Unit des unités spéciales de la police fédérale) a mis en place » (mis en gras par l'Autorité) ; et encore que « *Lors de la consultation publique, certains opérateurs ont expliqué qu'en pratique les demandes de certaines autorités sont envoyées dans la plateforme d'échange du NTSU (la plateforme « TANK ») avant d'être transférées vers la cellule de coordination* » (mis en gras par l'Autorité).

42. Toutefois, **ni le dispositif du Projet, ni son exposé des motifs** (au-delà de ses extraits reproduits ci-avant) **ne définissent la (les) mission(s) de ce service** à désigner par le Roi, **ne fût-ce qu'en renvoyant le cas échéant aux règles qui encadreraient déjà son fonctionnement et ses missions** dans le contexte des injonctions de production ou de conservation des preuves électroniques. **Or il semble bien que celui-ci traitera des données à caractère personnel** (consultation de coordonnées de contact et plus fondamentalement, intervention dans la coopération avec les entreprises concernées). **Et les éléments essentiels des traitements de données à caractère personnel doivent être consacrés dans une norme du rang de loi conformément aux articles 8 CEDH et 22 de la Constitution.** L'Autorité n'est en l'occurrence pas en mesure de déterminer dans quelles circonstances le NTSU est amené à traiter des données à caractère personnel dans le contexte du Projet et de la mise en œuvre des injonctions de production ou de conservation de preuves électroniques.
43. Dans ces conditions, l'Autorité est d'avis que **le dispositif du Projet doit définir les missions et/ou obligations** du « service désigné par le Roi » dans le contexte des injonctions de production ou de gel de preuves électroniques visés par le Projet **ou renvoyer aux règles qui par ailleurs définissent ces missions ou obligations**. Elle ne s'exprime pas davantage à ce sujet.

PAR CES MOTIFS,

L'Autorité est d'avis que,

1. Le présent Avis ne porte pas sur les conditions dans lesquelles les autorités compétentes peuvent adresser des injonctions à certains prestataires de services de l'économie numérique, ni sur la question de savoir quels prestataires peuvent, conformément au droit applicable, être l'objet de telles injonctions. Un point de contact ne pourra être tenu de traiter des données à caractère personnel en exécution du Projet que dans la mesure où l'injonction qui lui est adressée existe dans le droit applicable et y est conforme. Il appartient au Demandeur de notamment s'assurer que les prestataires de services qui sont visés par le Projet en dehors et au-delà du champ d'application de la Directive puissent bien être l'objet d'injonctions. Celles-ci ne pourront pas être juridiquement fondées sur le Projet. L'exposé des motifs du Projet (à tout le moins) devrait rappeler les fondements légaux des injonctions qui peuvent être

adressées en droit belge aux prestataires concernés et tombent dans le champ d'application du Projet (**considérants nos 12-16 et 21**) ;

2. Le Projet doit spécifier que l'obligation prévue dans son article 14, alinéa 3, ne vaut que pour les preuves électroniques dont le traitement relève de la responsabilité du fabricant ou du loueur de véhicules connectés concerné (**considérants nos 17-18**) ;

3. Un point de contact qui devrait être prévu d'une manière non conforme à la Directive ne pourrait en conséquence licitement traiter les données à caractère personnel concernées par les injonctions de production ou de conservation de preuves électroniques. L'acception étendue du concept de « *preuves électroniques* » retenue dans le Projet ne sera applicable que dans des hypothèses d'injonctions en dehors du champ d'application de la Directive et du Règlement Preuves Electroniques (**considérants nos 19-20**) ;

4. Le Projet doit être adapté en ce qu'il habiliterait le Roi en son article 2, al. 2, à interpréter les concepts de véhicule connecté et de fabricants et loueurs de véhicules connectés (**considérants nos 22-23**) ;

5. En l'état, le Projet ne peut pas fonder une mise à disposition du public des coordonnées de contact si celles-ci contiennent des données à caractère personnel. Il convient de motiver et développer le régime de publicité active le cas échéant applicable à ces données (**considérants nos 24-30**) ;

6. Le point de contact (qu'il soit un établissement désigné, un représentant légal ou une cellule de coordination) et le fournisseur de service concerné sont des responsables conjoints du traitement des données dans le cadre de la mise en œuvre des injonctions de production ou de conservation de preuves électroniques. Et l'IBPT est responsable du traitement des données nécessaires à l'exécution des missions et obligations qui lui incombent en vertu du Projet, (**considérants nos 31-32**) ;

7. Le Demandeur doit vérifier si l'article 11, § 2, als 2 et 3 du Projet ne peut pas se limiter à prévoir que le Roi détermine les conditions dans lesquelles les autorités compétentes consultent auprès de l'IBPT les coordonnées de contact des cellules de coordination. Etant entendu que le Projet devra toujours être lu en combinaison avec les cadres législatifs applicables *in concreto* qui justifieront et fonderont en droit la consultation des coordonnées concernées (**considérants nos 33-35**) ;

8. Il convient de vérifier que l'habilitation du Roi visée à l'article 16 du Projet peut avoir la portée voulue et être maintenue en ses termes actuels (**considérants nos 36-39**) ;

9. Le dispositif du Projet doit définir les missions et/ou obligations du « *service désigné par le Roi* » dans le contexte des injonctions de production ou de conservation de preuves électroniques visés par le Projet ou renvoyer aux règles qui par ailleurs définissent ces missions ou obligations (**considérants nos 40-43**).

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice