

**Avis du Conseil de l'IBPT
du 2 octobre 2026
concernant
les avant-projets de loi relatifs
1° à l'interdiction administrative des activités des
personnes morales, des sociétés sans personnalité
juridique, des associations ou groupements de fait
constituant une menace grave et actuelle pour la
sécurité nationale et
2° aux recours devant le Conseil d'État contre les
mesures d'interdiction administrative prévues par la loi
du XXX relative à l'interdiction administrative des
activités de certaines entités constituant une menace
grave et actuelle pour la sécurité nationale**

TABLE DES MATIÈRES

1.	Objet de la demande d'avis.....	3
2.	Description des avant-projets de loi.....	4
3.	Analyse.....	6
3.1.	Compétences et domaines d'expertise de l'IBPT.....	6
3.1.1.	<i>Généralités.....</i>	6
3.1.2.	<i>Compétences dans la mise en œuvre du RTCO.....</i>	7
3.1.3.	<i>Compétences dans la mise en œuvre du DSA.....</i>	8
3.1.4.	<i>Nécessité d'une base légale complémentaire.....</i>	10
3.1.5.	<i>Choix de l'autorité la plus adéquate.....</i>	10
3.1.6.	<i>Recours contre les décisions de l'IBPT.....</i>	11
3.2.	Mécanisme envisagé.....	11
3.2.1.	<i>Quant aux fournisseurs et services susceptibles d'être concernés.....</i>	13
3.2.2.	<i>Quant aux mesures pouvant techniquement et juridiquement faire l'objet d'une injonction...16</i>	
4.	Conclusion.....	18

1. Objet de la demande d'avis

1. Le Ministre de la Sécurité et de l'Intérieur a transmis, le 20 juillet 2026, au président de l'IBPT une demande d'avis concernant les textes suivants :

1° un avant-projet de loi monocaméral *relatif à l'interdiction administrative des activités des personnes morales, des sociétés sans personnalité juridique, des associations ou groupements de fait constituant une menace grave et actuelle pour la sécurité nationale* ;

2° un avant-projet de loi bicaméral *relatif aux recours devant le Conseil d'Etat contre les mesures d'interdiction administrative prévues par la loi du XXX relative à l'interdiction administrative de certaines entités constituant une menace grave et actuelle pour la sécurité nationale*.

2. L'avis de l'IBPT est sollicité « *sur l'ensemble des deux avant-projets et, en particulier, sur la possibilité de prévoir un droit d'injonction de l'IBPT à l'égard des fournisseurs de services afin d'assurer l'exécution effective d'une interdiction d'utiliser les moyens de communications électroniques visés par l'avant-projet* ».

3. Plus précisément, l'avis de l'IBPT est sollicité quant aux points suivants :

1° « *les compétences dont l'IBPT dispose actuellement* » ;

2° « *la nécessité éventuelle d'une base légale complémentaire* » ;

3° « *les fournisseurs et services susceptibles d'être concernés* » ;

4° « *les mesures pouvant techniquement et juridiquement faire l'objet d'une injonction* » ;

5° « *les garanties et modalités procédurales qui devraient encadrer un tel mécanisme* ».

4. Enfin, il est demandé à l'IBPT « *Si les dispositions nécessaires à l'instauration d'un tel pouvoir d'injonction peuvent, selon lui, être intégrées dans l'avant-projet de loi qui lui est soumis ou si elles nécessitent une modification spécifique de la législation relative à l'IBPT.* ».

5. Dans le cadre de l'élaboration de la présente note, l'IBPT a pu prendre connaissance des avis publiquement disponibles, à savoir [l'avis n° 2025/9 de l'Institut Fédéral pour la protection et la promotion des Droits Humains du 18 septembre 2025](#), [l'avis du Collège des Procureurs généraux du 25 septembre 2025](#), [l'avis 003/CPR/2025 du Comité permanent R du 9 octobre 2025](#) et [l'avis 78.110/AG du Conseil d'Etat du 31 décembre 2025](#).

6. L'IBPT n'a, en revanche, pas pu prendre connaissance de l'avis du CCRS du 8 octobre 2025, dont l'exposé des motifs résume cependant succinctement la teneur.

7. Compte tenu de l'existence de ces avis antérieurs, et dans le cadre de ses compétences et de ses domaines d'expertise, l'IBPT consacre le présent avis à l'examen des questions plus spécifiquement liées à la mesure visée à l'article 5, § 1^{er}, 1°, d), qui semble pouvoir être qualifiée de mesure de type « bannissement numérique » ou de mesure de restriction d'accès numérique.

2. Description des avant-projets de loi

8. L'avant-projet de loi « *relatif à l'interdiction administrative des activités des personnes morales, des sociétés, sans personnalité juridique, des associations ou groupements de fait constituant une menace grave et actuelle pour la sécurité nationale* » fixe des mesures administratives visant à mettre un terme aux activités de certaines entités.
9. Le mécanisme d'interdiction établi par cet avant-projet de loi prévoit la possibilité pour le Conseil des ministres, sur proposition du Ministre de la Sécurité et de l'Intérieur, de prendre une mesure administrative à l'encontre de l'une des entités visées, à savoir :
 - les personnes morales, à l'exception des personnes morales de droit public, visées aux articles 1:5, §§ 2 et 3, 1:6, § 2, et 1:7 du Code des sociétés et des associations ;
 - les sociétés sans personnalité juridique, visées à l'article 1:5, § 1^{er}, du même code ;
 - les associations de fait, visées à l'article 1:6, § 1^{er}, (du même code) ;
 - les groupements de fait, entendus comme des ensembles de personnes physiques, dépourvus de personnalité juridique, qui s'organisent de manière informelle, en vue de poursuivre collectivement un objectif commun.
10. Une telle entité peut faire l'objet d'une ou plusieurs des mesures d'interdiction prévues par l'avant-projet de loi « *lorsqu'il ressort d'éléments concrets qu'elle constitue une menace grave et actuelle pour la sécurité nationale, cette menace devant constituer une caractéristique essentielle et structurelle de l'entité concernée* ». Pour l'application de cet avant-projet de loi, il est précisé que « *la sécurité nationale comprend la protection de la pérennité de l'ordre démocratique et constitutionnel, des institutions démocratiques, ainsi que la protection contre les atteintes graves, organisées et systématiques à l'exercice des droits et libertés fondamentaux* » (article 3, § 3 de l'avant-projet).
11. Sont cependant exclues du champ d'application de l'avant-projet de loi, les organisations représentatives des travailleurs, les partis politiques qui présentent des candidats à une élection, pendant la période comprise entre la publication de l'acte convoquant les électeurs et le jour du scrutin concerné (article 3, § 1^{er}, alinéas 2 et 3 de l'avant-projet). Il est également précisé que la loi « *ne peut être appliquée au seul motif que l'entité concernée professe une opinion politique, syndicale, religieuse, philosophique ou autre, aussi critique, contestataire ou radicale soit-elle* » (article 3, § 2 de l'avant-projet) et que « *La mesure ne peut être fondée ni sur des faits isolés, occasionnels ou accessoires, ni sur des comportements imputables à certains membres agissant à titre purement individuel.* » (article 3, § 4 de l'avant-projet). L'exposé des motifs précise encore, à cet égard, que « *l'interdiction administrative n'est pas une condamnation, mais une mesure de police spéciale, visant la structure et non les individus qui la composent.* ».
12. A la suite de l'avis du Conseil d'Etat, l'article 4 énonce les trois conditions cumulatives qui doivent être réunies pour qu'une mesure d'interdiction administrative puisse être adoptée, à savoir : 1° la constatation de faits susceptibles de caractériser la menace grave et actuelle visée à l'article 3 (listés à l'article 4, alinéa 1^{er}, 1°) ; 2° l'existence d'un lien concret avec le territoire belge ; 3° le respect du principe de nécessité et de proportionnalité.

13. Parmi les mesures administratives pouvant être adoptées, figure l'interdiction d'utiliser les outils numériques pour organiser, promouvoir, coordonner, soutenir ou poursuivre l'action de l'entité concernée.
14. L'article 5, § 1^{er}, 1^o, d), de l'avant-projet de loi prévoit en effet que :
*« § 1^{er}. En fonction de la nature juridique de l'entité concernée, de la gravité de la menace constatée, et du principe de proportionnalité, l'interdiction peut consister en :
1^o une ou plusieurs mesures administratives consistant en tout ou partie des mesures suivantes : (...)
d) l'interdiction d'utiliser, des plateformes numériques, sites internet, comptes de réseaux sociaux, canaux de messagerie ou autres moyens de communication numérique principalement ou de manière déterminante utilisés pour organiser, promouvoir, coordonner ou poursuivre l'action de l'entité concernée ; (...) »*
15. L'article 8, § 1^{er}, alinéa 1^{er}, précise que : *« § 1^{er}. Les mesures visées à l'article 5, § 1^{er}, 1^o, sont adoptées par arrêté royal délibéré en Conseil des ministres, sur proposition du ministre. »*.
16. L'article 5, § 3, alinéa 1^{er}, indique, par catégorie de mesures administratives, quelle autorité est responsable de leur exécution. Contrairement aux autres types de mesures, aucune responsabilité d'exécution n'est mentionnée pour la catégorie d) précitée (c.-à-d. interdiction d'utiliser certains moyens de communication numérique).
17. L'avant-projet de loi *« relatif aux recours devant le Conseil d'État contre les mesures d'interdiction administrative prévues par la loi du XXX relative à l'interdiction administrative des activités de certaines entités constituant une menace grave et actuelle pour la sécurité nationale »* organise un recours spécifique contre les mesures administratives adoptées en exécution du projet.

3. Analyse

18. Conformément à la demande formulée par le Monsieur le Ministre de la Sécurité et de l'Intérieur, il est répondu ci-après en deux temps :
 - 18.1. *Premièrement*, quant aux compétences et domaines d'expertise de l'IBPT (point 3.1, ci-après) ;
 - 18.2. *Deuxièmement*, quant au mécanisme envisagé, et en particulier, quant à la mesure administrative de restriction d'accès numérique, visée à l'article 5, § 1^{er}, 1^o, d), du premier avant-projet de loi (point 3.2, ci-après).

3.1. Compétences et domaines d'expertise de l'IBPT

3.1.1. Généralités

19. L'IBPT est un organisme d'intérêt public doté de la personnalité juridique dont les missions sont essentiellement énumérées à l'article 14 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, ci-après « loi relative au statut de l'IBPT ». Cette loi a été complétée ces dernières années afin de confier à l'IBPT notamment des missions particulières concernant certains fournisseurs de services de l'écosystème numérique.
20. Il s'agit, en particulier, de compétences de contrôle et de sanction dans le cadre de la lutte contre la diffusion de contenus à caractère terroriste en ligne au sens du Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, ci-après « RTCO » (voir point 3.1.2. ci-dessous), lequel s'applique aux fournisseurs de « services d'hébergement »¹. On ajoutera à cette extension la mise en œuvre au niveau fédéral, le contrôle et les sanctions en cas de non respect du Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), ci-après « DSA » pour « Digital Services Act » (voir point 3.1.2 ci-dessous), lequel s'applique aux fournisseurs de « services intermédiaires »².
21. L'IBPT est également l'organisme fédéral qui intervient comme régulateur dans le secteur des médias sur le territoire de la région bilingue de Bruxelles-Capitale en ce qui concerne les services de médias audiovisuels et les services de plateformes de partage de vidéos qui ne relèvent ni de la Communauté flamande, ni de la Communauté française (loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale).

¹ Au sens de l'article 2, § 1^{er}, 1) du RTCO.

² Au sens de l'article 3, § 1^{er}, g) du DSA.

22. Ses compétences sectorielles spécifiques sont précisées par d'autres lois spécifiques³, essentiellement la loi du 13 juin 2005 relative aux communications électroniques, ci-après « LCE », en matière de gestion du spectre radio, de régulation des communications électroniques, de numérotation, de protection des intérêts de la société et des utilisateurs, de sécurité des communications électroniques, de protection des utilisateurs finaux, etc.

3.1.2. Compétences dans la mise en œuvre du RTCO

23. Le RTCO a pour objectif d'établir des règles communes pour garantir que les fournisseurs de services d'hébergement luttent contre l'utilisation abusive de leurs services pour diffuser des contenus à caractère terroriste et de protéger la sécurité publique tout en garantissant le respect des droits fondamentaux, notamment la liberté d'expression et d'information.
24. Dans le cadre du RTCO, l'IBPT est l'autorité compétente en charge des missions spécifiques énumérées à l'article 12, § 1^{er}, c) et d), du RTCO, sans préjudice de tâches confiées au procureur fédéral en vertu de l'article 12, § 1^{er}, a) et b), du RTCO.⁴ Les missions de l'IBPT portent dès lors sur la supervision de la mise en œuvre des mesures spécifiques en vertu de l'article 5 du RTCO⁵ ainsi que sur l'imposition de sanctions en vertu de l'article 18 du RTCO⁶. Cette dernière mission comprend notamment la possibilité de sanctionner le non-respect des injonctions de retrait des contenus à caractère terroriste ou d'en bloquer l'accès dans l'ensemble des États membres, émises par les autorités compétentes des États membres. L'IBPT n'est toutefois pas compétent pour émettre lui-même de telles injonctions de retrait ou de blocage de contenus. En Belgique, cette compétence relève du procureur fédéral⁷ et est exercée, en pratique, par la police fédérale.
25. Les fournisseurs auxquels s'applique le RTCO sont les « fournisseurs de services d'hébergement », comme définis à l'article 2, § 1^{er}, point 1, du RTCO,⁸ dans la mesure où ils diffusent des informations au public.⁹
26. Le RTCO repose sur le principe du contrôle par l'État membre d'établissement du fournisseur. Conformément à l'article 16 du RTCO, l'État membre dans lequel est situé l'établissement principal du fournisseur de services d'hébergement, ou dans lequel son représentant légal réside ou est établi, est compétent pour assurer la surveillance de la mise en œuvre des mesures spécifiques prévues à l'article 5 du RTCO, ainsi que pour imposer des sanctions conformément à l'article 18 du RTCO. Par conséquent, l'IBPT n'est compétent pour exercer ses missions qu'à l'égard des fournisseurs de services d'hébergement dont l'établissement

³ On notera bien entendu la loi du 26 janvier 2018 relative aux services postaux, mais également la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique : l'IBPT exerce la fonction d'autorité sectorielle et de service d'inspection pour les infrastructures numériques (à l'exception des prestataires de confiance) et pour le secteur des services postaux et d'expédition en matière postale. Enfin, on notera qu'en vertu de la loi du 19 décembre 2025 relative à la résilience des entités critiques, l'IBPT est l'autorité sectorielle en charge de contrôler les infrastructures critiques relevant du secteur des infrastructures numériques (à l'exception des prestataires de confiance).

⁴ L'article 14, §1^{er}, 3^o, l), de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, *M.B.*, 24 janvier 2003.

⁵ L'article 12, § 1^{er}, c), du RTCO.

⁶ L'article 12, § 1^{er}, d), du RTCO.

⁷ L'article 144bis. § 2, al. 1^{er}, 4^o, du Code Judiciaire conformément aux lignes directrices énoncées dans une circulaire du Collège des procureurs généraux et l'article 12, § 1^{er}, a), du RTCO.

⁸ Voir point 3.2.1 infra.

⁹ L'article 1er, § 2, du RTCO.

principal se situe en Belgique ou qui ont désigné en Belgique leur représentant légal au sens du RTCO.

3.1.3. Compétences dans la mise en œuvre du DSA

27. Le DSA vise à rendre l'environnement en ligne plus sûr et plus équitable pour les utilisateurs, en imposant aux fournisseurs de services intermédiaires en ligne certaines obligations de diligence, comme de la transparence en cas de suppression de contenus, la possibilité de signaler facilement des contenus illicites, etc.
28. Dans le cadre de la mise en œuvre du DSA, l'IBPT a été désigné d'une part coordinateur national pour les services numériques (ci-après « DSC ») dans le cadre de l'accord de coopération du 3 mai 2024,¹⁰ et d'autre part autorité compétente pour le niveau fédéral¹¹. Par ailleurs, le Conseil supérieur de l'audiovisuel (CSA), le Medienrat et le Vlaamse Regulator voor de Media (VRM) ont également été désignés comme autorités compétentes pour la mise en œuvre du DSA en Belgique, dans le champ des compétences attribuées aux communautés.
29. L'accord de coopération du 3 mai 2024 organise l'exécution coordonnée du DSA en Belgique. Il prévoit que, par principe, les autorités compétentes et le DSC mettent en œuvre le DSA dans le respect de leur compétences respectives.¹² En sa qualité de DSC, l'IBPT est responsable de la coordination au niveau national de toutes les questions en lien avec la surveillance et l'exécution du DSA et contribue à une surveillance et une exécution efficaces et cohérentes du DSA dans toute l'UE.¹³ Les missions du DSC sont énumérées de manière exhaustive à l'article 2, § 2, alinéa 2 de l'accord de coopération. Elles comprennent notamment la centralisation des injonctions émanant des autorités sectorielles belges, telles que visées aux articles 9 et 10 du DSA.
30. S'agissant des obligations prévues à l'article 9 et 10 du DSA, l'autorité compétente¹⁴ assignée n'est pas chargée de contrôler ou d'exécuter l'injonction adressée au fournisseur de services intermédiaires de retirer un contenu ou de fournir des informations concernant un ou plusieurs utilisateurs du service. Cette compétence appartient à l'autorité sectorielle, administrative ou judiciaire, qui a adopté l'injonction sur le fondement du droit applicable.
31. Cependant, l'autorité compétente au sens du DSA est chargée de vérifier si le fournisseur de services intermédiaires concerné a respecté les obligations procédurales que l'article 9 du DSA lui imposées en réponse à cette injonction, telles que les obligations d'information et de suivi. En Belgique, l'identité de l'autorité compétente pour faire respecter ces obligations dans un cas particulier, dépendra en définitive du niveau de pouvoir compétent pour la matière concernée.

¹⁰ L'article 4, § 1^{er}, de l'accord de coopération du 3 mai 2024 entre l'Etat fédéral, la Communauté flamande, la Communauté française et la Communauté germanophone relatif à l'exécution coordonnée partielle du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *M.B.*, 30 décembre 2024.

¹¹ L'article 14, § 1^{er}/1, loi du 17 janvier 2003 (statut) précitée : « *En ce qui concerne les compétences fédérales, l'Institut est une autorité compétente au sens de l'article 49 du règlement sur les services numériques.* »

¹² L'article 3 et 4, § 2, alinéa 3, de l'accord de coopération du 3 mai 2024.

¹³ L'article 4, § 2, alinéa 1^{er}, de l'accord de coopération du 3 mai 2024.

¹⁴ C'est-à-dire : l'autorité compétente pour mettre en œuvre le DSA.

32. De manière générale, il convient de rappeler que le DSA définit la notion de contenu illicite par référence au droit matériel applicable, sans fixer lui-même les règles déterminant quels contenus sont illicites.¹⁵ Il n'appartient pas aux autorités compétentes chargées de la surveillance et de l'exécution du DSA, dans l'exercice des compétences qui leur sont conférées dans le cadre de celui-ci, d'assurer une surveillance générale des contenus diffusés en ligne en vue de détecter ou de qualifier des contenus individuels comme étant illicites. Leur mission consiste avant tout à contrôler le respect, par les fournisseurs de services intermédiaires, des obligations que le DSA met à leur charge et qui constituent principalement des obligations de diligence. Par ailleurs, l'article 28 du DSA (« Protection des mineurs en ligne ») prévoit par exemple des obligations liées à la gestion des risques et s'apparentent donc davantage à des obligations de moyens visant à atténuer les risques identifiés.¹⁶
33. Afin de contrôler le respect de ces obligations, l'autorité compétente examinera essentiellement les mesures, processus et mécanismes mis en place par le fournisseur, tels que, notamment dans le cadre de l'article 28 DSA, les éventuelles restrictions d'accès au service, les paramètres par défaut, la conception d'interfaces en ligne, les systèmes de recommandation et les fonctions de recherche ou encore les systèmes de modération de contenu, afin de garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service. Le contenu lui-même ne constitue donc pas l'objet principal du contrôle. Le contrôle porte sur la réponse apportée par le fournisseur au risque concerné, et non sur la qualification juridique de contenus individuels pris isolément.¹⁷
34. Les fournisseurs auxquels s'applique le DSA sont les fournisseurs de « services intermédiaires », définis à l'article 3, § 1^{er}, point g), du DSA.¹⁸ Conformément à l'article 56 du DSA, la compétence à l'égard d'un fournisseur de services intermédiaires est déterminée par l'État membre dans lequel celui-ci a son établissement principal¹⁹ ou dans lequel son représentant légal réside ou est établi. Cet État membre dispose d'une compétence exclusive pour surveiller et faire appliquer le DSA, sans préjudice des pouvoirs conférés à la Commission européenne à l'égard des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne.
35. Il en résulte que seuls les fournisseurs de services intermédiaires dont l'établissement principal est situé en Belgique, ainsi que ceux qui ont désigné un représentant légal en Belgique, relèvent de la compétence des autorités belges compétentes pour l'application du DSA, dont l'IBPT. Le contrôle des obligations que le DSA prévoit à l'égard des fournisseurs de services intermédiaires qui ne relèvent pas de la compétence belge est assuré par le DSC compétent et, le cas échéant, la Commission européenne.

¹⁵ L'article 3, § 1^{er}, h), du DSA.

¹⁶ L'article 28 du DSA prévoit que les fournisseurs de plateformes en ligne accessibles aux mineurs mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service. Les lignes directrices de la Commission européenne adoptées conformément à l'article 28, § 4 formulent à cet égard des recommandations destinées aux fournisseurs de plateformes en concernés.

¹⁷ Le nombre de contenus signalés et qualifiés de préjudiciables vis-à-vis de la vie privée, la sûreté et la sécurité des mineurs peut néanmoins être pris en considération à titre incident, dans la mesure nécessaire pour apprécier l'adéquation, la proportionnalité et l'effectivité des mesures mises en place par le fournisseur.

¹⁸ Voir point 3.3 infra.

¹⁹ C'est-à-dire, conformément au considérant 123 du DSA : l'Etat membre « dans lequel le fournisseur a son administration centrale ou son siège statutaire au sein duquel sont exercés les principales fonctions financières ainsi que le contrôle opérationnel. »

3.1.4. Nécessité d'une base légale complémentaire

36. L'IBPT ne dispose, à ce jour, pas des bases légales nécessaires qui lui permettraient d'intervenir dans le cadre de la mise en œuvre de mesures de restriction d'accès numérique, telles que celles envisagées par le premier avant-projet de loi soumis pour avis.
37. Dans l'hypothèse où une extension des compétences de l'IBPT devrait être envisagée, il importe de noter que ses missions légales sont énumérées, à tout le moins dans leur principe, à l'article 14 de la loi relative au statut de l'IBPT précitée.
38. Or, contrairement à ce qui est prévu quant aux autres mesures visées par le premier avant-projet de loi, pour la catégorie visée à l'article 5, § 1^{er}, 1^o, d) du projet (c.-à-d l'interdiction d'utiliser certains moyens de communication numérique), aucune responsabilité d'exécution n'est mentionnée. Cette absence de précision a pour conséquence qu'en l'état actuel des textes, il reviendrait au Roi de désigner l'autorité responsable de l'exécution de la mesure visée au d). Ceci rend toute participation de l'IBPT problématique au niveau juridique puisque seul le législateur peut attribuer de nouvelles missions à une autorité administrative indépendante telle que l'IBPT.

3.1.5. Choix de l'autorité la plus adéquate

39. Avant d'envisager une éventuelle base légale complémentaire visant à confier à l'IBPT une nouvelle compétence dans le cadre du mécanisme envisagé, se pose la question de savoir si l'IBPT est l'autorité la plus adéquate pour prendre en charge la mission de contrôle de la bonne exécution des mesures de restriction d'accès numérique envisagées. Or, tel ne semble pas être le cas, et ce pour les raisons développées ci-dessous.
40. En exécution du RTCO, l'IBPT est chargé de sanctionner administrativement le non-respect des injonctions de retrait ou de blocage de contenu à caractère terroriste émises par le procureur fédéral ou par les autorités compétentes des autres Etats membres, une fois celles-ci devenues définitives. Ce faisant, en cas d'infraction, l'IBPT peut, en vertu de l'article 21 de la loi relative au statut de l'IBPT, condamner un fournisseur de services d'hébergement à cesser une infraction, le cas échéant sous astreinte, et/ou à une amende administrative.
41. Néanmoins, dans l'exercice de cette mission, l'IBPT ne dispose d'aucun pouvoir d'appréciation quant au contenu de l'injonction en tant que telle et n'est pas amené à évaluer la nécessité ou la proportionnalité de cette injonction ; ces missions étant réservées à l'autorité d'émission dans un premier temps, et éventuellement aux instances de recours et autorités chargées d'un examen approfondi de l'injonction de retrait transfrontalière prévu à l'article 4, § 3, du RTCO dans un second temps. En Belgique, cette dernière procédure, qui a pour objectif de déterminer si l'injonction de retrait viole gravement ou manifestement le RTCO ou les libertés et droits fondamentaux garantis par la Charte, relève de la compétence du procureur fédéral.²⁰
42. De même, dans le cadre du DSA, la compétence de l'IBPT est en principe limitée à la vérification des obligations procédurales mises à charge des fournisseurs de service dans le cadre des injonctions d'agir contre des contenus illicites.

²⁰ L'article 144bis, § 2, al. 1^{er}, 4^o du Code Judiciaire conformément aux lignes directrices énoncées dans une circulaire du Collège des procureurs généraux et l'article 12, § 1^{er}, b), du RTCO.

43. La procédure de sanction administrative, dont est chargé l'IBPT, présente naturellement des avantages appréciables en termes d'efficacité. Cependant, cette mission de sanction administrative est d'une nature bien différente de la compétence d'émettre des injonctions. L'exercice d'une compétence de cette nature suppose en effet une expertise en matière de détection de contenus illicites et de qualification de ce contenu, ce dont l'IBPT ne dispose pas.
44. En effet, comment contrôler l'effectivité d'une mesure de restriction d'accès numérique d'une entité déterminée, si ce n'est en vérifiant que cette dernière ne réapparaît pas au moyen d'un nouveau compte d'utilisateur, et donc en effectuant un travail de détection de contenu lié à l'activité de cette entité ?
45. Dans le contexte du contenu à caractère terroriste, cette mission de détection est réalisée en pratique par le Federal Computer Crime Unit (FCCU) – Internet Referral Unit (IRU) de la Police fédérale. Dans de nombreux autres domaines, ce sont des services publics fédéraux qui assurent cette détection de contenus illicites en ligne. Tel est le cas, par exemple, du Service de lutte contre les atteintes au droit d'auteur et aux droits voisins commises en ligne et contre l'exploitation illégale de jeux de hasard en ligne, créé au sein de la DG Inspection économique du SPF Economie par l'arrêté royal du 18 avril 2024.²¹ Le cas échéant, il pourrait être envisagé de créer un service d'inspection spécialisé au sein du SPF Intérieur, du SPF Justice ou du SPF Chancellerie du Premier Ministre²².

3.1.6. Recours contre les décisions de l'IBPT

46. Pour terminer, en termes de voies de recours, il est utile de préciser que la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges, ci-après « loi recours », confie à la Cour des marchés statuant comme en référé la mission de statuer sur un recours en pleine juridiction contre les décisions de l'IBPT concernant les fournisseurs relevant de la compétence de l'IBPT. Lorsqu'un recours est dirigé contre une décision à caractère réglementaire, la Cour des marchés dispose uniquement d'un pouvoir d'annulation.
47. Dès lors, tenant compte de l'organisation des recours contre les décisions de l'IBPT auprès de la Cour des marchés, l'organisation d'une voie de recours spécifique devant le Conseil d'Etat nécessiterait d'envisager une adaptation de la loi « recours » du 17 janvier 2003 précitée et risquerait d'aboutir à un système peu compréhensible pour les acteurs relevant du secteur numérique.

3.2. Mécanisme envisagé

48. Les questions posées par Monsieur le Ministre de la Sécurité et de l'Intérieur font inévitablement émerger la question sous-jacente de la faisabilité juridique et pratique de la mesure administrative envisagée.

²¹ Voir la page Internet du Service : <https://economie.fgov.be/fr/themes/propriete-intellectuelle/droits-de-propriete/droits-dauteur-et-droits/sanctions-et-actions/piraterie-en-ligne>.

²² Voir notamment l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B.*, 21/11/2014.

49. A cet égard, il convient tout d'abord de relever que l'article 5, § 1^{er}, 1^o, d), de l'avant-projet²³ entend instaurer une mesure administrative à portée très générale, consistant en « *l'interdiction d'utiliser, des plateformes numériques, sites internet, comptes de réseaux sociaux, canaux de messagerie ou autres moyens de communication numérique principalement ou de manière déterminante utilisés pour organiser, promouvoir, coordonner, soutenir ou poursuivre l'action de l'entité concernée* ».
50. L'article 5, § 3, alinéa 1^{er}, du projet de loi précise, par catégorie de mesures administratives, l'autorité responsable de leur exécution. Or, l'IBPT rappelle que pour la catégorie d) (c.-à-d. interdiction d'utiliser certains moyens de communication numérique), aucune responsabilité d'exécution n'est mentionnée.
51. Certes, l'alinéa 2 du même paragraphe prévoit que « l'arrêté royal visé à l'article 8 » désigne, pour chaque mesure adoptée, les autorités et services chargés de son exécution et de son suivi. L'alinéa 3 ajoute, à cet égard, que « *Les autorités et services ainsi désignés prennent les actes matériels, administratifs ou techniques strictement nécessaires à l'exécution effective des mesures qui les concernent.* » (nous soulignons). Selon l'alinéa 4, les autorités et services ainsi désignés « *peuvent, à cette fin, adresser aux personnes, organismes ou prestataires directement concernés les injonctions strictement nécessaires à cette exécution, pour autant que ces injonctions soient directement liées aux mesures adoptées par l'arrêté royal, limitées à leur exécution effective et proportionnées à la menace constatée.* » (nous soulignons). L'alinéa 5 précise enfin que : « *Ces injonctions ne peuvent modifier la portée des mesures adoptées par l'arrêté royal ni créer de nouvelles interdictions.* ».
52. La mise en œuvre du mécanisme envisagé repose donc sur **plusieurs niveaux décisionnels**.

52.1. Un arrêté royal délibéré en Conseil des Ministres détermine :

- i. l'entité faisant l'objet de la mesure d'interdiction ;
- ii. le type de mesure (en l'occurrence, la restriction d'accès numérique visée à l'article 5, § 1^{er}, 1^o, d)), et ;
- iii. l'autorité / le service d'exécution ;

52.2. Une injonction émise par une autorité administrative détermine :

52.3. Les mesures concrètes à adopter, pour autant qu'elles soient limitées « *à l'exécution effective* » de l'interdiction et « *proportionnées à la menace constatée* » ;

²³ « Art. 5. § 1^{er}. En fonction de la nature juridique de l'entité concernée, de la gravité de la menace constatée, et du principe de proportionnalité, l'interdiction peut consister en :
1^o une ou plusieurs mesures administratives consistant en tout ou partie des mesures suivantes : [...]
d) l'interdiction d'utiliser, des plateformes numériques, sites internet, comptes de réseaux sociaux, canaux de messagerie ou autres moyens de communication numérique principalement ou de manière déterminante utilisés pour organiser, promouvoir, coordonner ou poursuivre l'action de l'entité concernée ; [...] ».

- i. Les « *personnes, organismes ou prestataires directement concernés* » destinataires enjoint de prendre ces mesures ;

52.4. Un contrôle de l'exécution de ces mesures par (la même ?) autorité administrative ;

52.5. Une voie de recours effective contre chacune de ces décisions administratives.

3.2.1. Quant aux fournisseurs et services susceptibles d'être concernés

- 53. Quant à la détermination des fournisseurs et services susceptibles d'être concernés, une ***première difficulté juridique*** concerne les **types de services visés** ; les notions ne sont pas définies par l'avant-projet et ne correspondent pas à des notions définies en droit belge ou en droit européen. Or, il importe de définir clairement les services concernés à des fins de sécurité juridique, mais également de proportionnalité. En l'état actuel du texte, ces objectifs ne semblent pas rencontrés.
- 54. En effet, il n'apparaît pas clairement, par exemple, si les services concernés visent uniquement les canaux de communication « publics » ou également les canaux « privés »²⁴, ni s'ils comprennent ou non les services de communications interpersonnelles fondées ou non sur la numérotation. Une lecture extensive de « *canaux de messagerie ou autres moyens de communication numérique* » pourrait *a priori* conduire à inclure notamment les communications privées, en ce compris par exemple les appels vocaux et SMS, dans le champ d'application de ladite disposition.
- 55. Afin de mieux circonscrire les services visés et d'assurer la cohérence globale entre les normes, il conviendrait d'utiliser autant que possible des concepts définis au niveau européen, que ce soit par le Code des communications électroniques européen (ci-après « le Code »), le DSA, le RTCO ou encore le Règlement 2022/1925 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) ou « DMA » pour « Digital Markets Act »).
- 56. Ainsi, l'examen des concepts européens suivants, repris ci-après de façon non exhaustive, permettrait déjà d'affiner la portée de la mesure en fonction de l'objectif poursuivi :

²⁴ Notons, à cet égard, que tant le DSA que le RTCO tiennent compte de la manière dont l'accès à une information est obtenu, notamment dans un groupe ou à un canal, à savoir s'il existe des restrictions d'accès et si l'autorisation est accordée automatiquement ou à la suite d'une intervention humaine. Le considérant 14 du DSA indique que : « La notion de « diffusion au public », [...] devrait impliquer la mise à disposition de l'information à un nombre potentiellement illimité de personnes, c'est-à-dire le fait de rendre l'information facilement accessible aux destinataires du service en général sans que le destinataire du service ayant fourni l'information ait à intervenir, que ces personnes aient ou non effectivement accès à l'information en question. En conséquence, lorsque l'accès à une information nécessite un enregistrement ou l'admission au sein d'un groupe de destinataires du service, cette information ne devrait être considérée comme étant diffusée au public que lorsque les destinataires du service qui cherchent à accéder à cette information sont enregistrés ou admis automatiquement sans intervention humaine pour en décider ou pour sélectionner les personnes auxquelles l'accès est accordé. » et voir également le considérant 14 du RTCO.

1° « **service de communication interpersonnelle** », définie 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;* » (art. 2, § 1^{er}, point 5 du Code). A priori, il ne ressort pas de l'exposé des motifs que l'intention serait de viser de telles communications de nature privée, protégées par le secret des communications électroniques (article 5 de la directive 2002/58/CE²⁵). Ce point devrait être éclairci.

2° « **service intermédiaire** » : dans le cadre du DSA, ils reposent sur la notion de « service de la société de l'information », « *un service tel qu'il est défini à l'article 1^{er}, paragraphe 1, point b), de la directive (UE) 2015/1535;* » et qui est un service de « simple transport », de « mise en cache » ou d'« hébergement » (article 3, § 1^{er}, point a) et g), du DSA).

3° « **service d'hébergement** » : dans le cadre du DSA, il est défini comme un service intermédiaire, à savoir un service de la société de l'information « *consistant à stocker des informations fournies par un destinataire du service à sa demande;* » (article 3, § 1^{er}, point g), iii), du DSA). Dans le cadre du RTCO, un « fournisseur de services d'hébergement » est défini comme « *un fournisseur de services tels qu'ils sont définis à l'article 1^{er}, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil, qui consistent à stocker des informations fournies par un fournisseur de contenus à la demande de celui-ci;* » (article 2, § 1^{er}, point 1, du RTCO). Les définitions du service d'hébergement figurant dans le DSA et dans le RTCO renvoient ainsi toutes deux à la notion de « service de la société de l'information » ainsi qu'à la caractéristique technique consistant à stocker des informations fournies par un utilisateur²⁶ à la demande de celui-ci. Le RTCO limite toutefois son champ d'application aux fournisseurs de services d'hébergement « *dans la mesure où ils diffusent des informations au public* »²⁷, de sorte que son champ d'application se rapproche, en pratique, davantage de la notion de « plateforme en ligne » au sens du DSA, telle que décrite ci-dessous.

4° « **plateforme en ligne** », est une sous-catégorie de services d'hébergement, définie comme « *un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse au public des informations, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d'un autre service ou une fonctionnalité mineure du service principal qui, pour des raisons objectives et techniques, ne peut être utilisée sans cet autre service, et pour autant que l'intégration de cette caractéristique ou de cette fonctionnalité à l'autre service ne soit pas un moyen de contourner l'applicabilité du présent règlement;* » (article 3, § 1^{er}, point i), du DSA).²⁸

²⁵ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31/07/2002 p. 0037 – 0047.

²⁶ Dans le cadre du DSA appelé « destinataire » et dans le cadre du RTCO « fournisseur de contenus ».

²⁷ Article 1^{er}, § 2, du RTCO.

²⁸ Notons que le considérant 14 du DSA précise que : « **Les services de communication interpersonnelle**, tels qu'ils sont définis dans la directive (UE) 2018/1972 du Parlement européen et du Conseil, comme les courriels ou les services de messagerie privée, **ne relèvent pas du champ d'application de la définition des plateformes en ligne** car ils sont utilisés pour la communication interpersonnelle entre un nombre fini de personnes, déterminé par l'émetteur de la communication. Cependant, les obligations prévues dans le présent règlement pour les fournisseurs de plateformes en ligne peuvent s'appliquer à des services qui permettent de mettre des informations à la disposition d'un nombre potentiellement illimité de destinataires, non déterminé par l'émetteur de la communication, notamment par l'intermédiaire de groupes publics ou de canaux ouverts. Des informations ne

5° « **réseaux sociaux** » : Le DSA ne prévoit pas de définition autonome des services de réseaux sociaux. Ces services sont néanmoins susceptibles de relever de la catégorie des plateformes en ligne au sens de l'article 3, § 1^{er}, point i), du DSA, dans la mesure où ils satisfont aux éléments constitutifs de cette définition. A titre indicatif, il peut être relevé que l'article 2, § 1^{er}, point 7, du DMA définit un « **service de réseau social en ligne** » comme « *une plateforme permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations* ». Cette définition ne précise toutefois pas la portée de la notion des termes « découvrir d'autres utilisateurs et d'autres contenus ». La définition est mentionnée à titre de référence uniquement, l'IBPT ne disposant d'aucune compétence particulière en matière d'application ou de contrôle du DMA.

57. Dans la mesure où les frontières entre les services de réseaux sociaux et les autres catégories de services numériques tendent à s'estomper, une définition trop étroite ou trop spécifique risquerait de ne plus refléter adéquatement l'évolution rapide des services numériques et de devenir rapidement dépassée. À l'inverse, le DSA repose sur des catégories définies de manière générale, dont celle de « **plateforme en ligne** », qui couvre en pratique de nombreux services généralement considérés comme des réseaux sociaux, tout en englobant également d'autres services permettant aux utilisateurs de diffuser des informations auprès du public.
58. Enfin, il convient de noter que les **sites web classiques**, qui ne stockent pas d'informations fournies par des tiers, ne relèvent ni de la définition des services intermédiaires ni de celle des services d'hébergement. Ceux-ci sont eux-mêmes responsables de leur propre contenu.
59. Une **seconde difficulté juridique** réside dans la limitation de l'interdiction à l'utilisation des services « *principalement ou de manière déterminante utilisés pour organiser, promouvoir, coordonner, soutenir ou poursuivre l'action de l'entité concernée* ».
60. Selon notre compréhension, l'objectif de la mesure est d'interdire l'utilisation d'un service déterminé pour lequel il a été constaté une utilisation aux fins précitées. Une interdiction de l'utilisation de l'ensemble des services au moyen d'une surveillance constante de l'activité en ligne de l'entité concernée, serait plus difficilement justifiable au regard de la proportionnalité et des droits fondamentaux. Se pose aussi la question de la finalité de l'utilisation : la restriction d'accès à certains moyens de communication a-t-elle vocation à s'appliquer de manière absolue ou, au contraire, ne vise-t-elle que les activités répréhensibles de l'entité frappée par la mesure ? Dans cette dernière hypothèse, le contrôle de l'exécution de la mesure s'en verrait évidemment rendu plus complexe et plus "subjectif" dans le chef de l'autorité qui en serait chargée. Afin d'éviter toute difficulté d'interprétation quant à la portée de la mesure, le texte devrait également être clarifié sur ces points.

devraient être considérées comme étant diffusées au public au sens du présent règlement que lorsque cette diffusion se produit à la demande directe du destinataire du service qui a fourni les informations. ».

3.2.2. Quant aux mesures pouvant techniquement et juridiquement faire l'objet d'une injonction

3.2.2.1. Le caractère effectif des mesures de mise en œuvre

61. Une restriction d'accès numérique qui se bornerait à la suppression du compte d'un utilisateur créé au nom de l'entité concernée (personne morale ou simple association ou groupement de fait), sans autre mesure visant à empêcher cette même entité de recréer immédiatement un nouveau compte, le cas échéant au moyen d'une autre dénomination, nom d'utilisateur ou pseudonyme, présenterait une efficacité (quasi-)nulle.
62. Afin de prévenir efficacement toute tentative de réapparition de l'entité concernée, des moyens techniques fiables devraient permettre d'identifier les personnes physiques agissant pour cette entité concernée au-delà des activités liées à son compte utilisateur initial, et au travers de ses activités ultérieures. Dans ce cadre, la mise en œuvre d'une mesure de restriction d'accès numérique est directement liée à celle de l'identification fiable des utilisateurs de services et à son pendant inverse, l'anonymat en ligne.
63. Dès lors, et bien que l'avant-projet précise que la mesure ne vise pas les individus, mais seulement les groupements (a fortiori si ceux-ci ne disposent pas de la personnalité juridique) dont ils font partie, force est de constater que la surveillance de l'activité des individus paraît un élément pertinent à la mise en œuvre effective de la mesure²⁹. À défaut de suivre l'activité des individus, la mise en œuvre semble devoir s'envisager alors exclusivement sous l'angle du monitoring de contenu, afin de détecter la réapparition de contenu issu de cette même entité.
64. En outre, il convient de noter que l'effectivité d'une mesure de restriction d'accès numérique visant un fournisseur de services établi dans un autre État dépend largement de l'existence de mécanismes de coopération européens ou même internationaux adéquats. C'est la raison pour laquelle le DSA encadre les injonctions ordonnant le retrait de contenus spécifiques ou la communication des informations spécifiques concernant des utilisateurs, émises par les autorités nationales, en prévoyant certaines exigences de forme et des obligations procédurales relatives à leur traitement. L'objectif est de garantir l'exécution effective et efficiente de ces injonctions, en particulier lorsqu'elles présentent une dimension transfrontière, dans un contexte où les législations nationales sur lesquelles elles reposent peuvent différer sensiblement d'un État membre à l'autre. En l'absence d'un mécanisme coordonné entre fournisseurs, la mesure de restriction d'accès numérique pourrait simplement conduire l'utilisateur concerné à migrer vers d'autres services, limitant ainsi son efficacité pratique. Ceci est d'autant plus vrai que la plupart des fournisseurs de service qui semblent visés par le présent avant-projet ne sont pas établis en Belgique, parfois ni même en Europe. Conformément au DSA et au RTCO, ceux-ci doivent, en revanche, dans un tel cas, désigner un représentant légal dans l'un des États membres, lequel est alors compétent pour la mise en œuvre du DSA et/ou du RTCO.

²⁹ Voir notamment [l'avis n° 52.522 du Conseil d'Etat du 19 février 2013](#), à propos des associations de fait que sont les milices privées, indique que « *il n'est en soi pas possible de dissoudre quelque chose qui juridiquement n'a pas d'existence en tant que sujet de droit* » (pt. 25, p. 55). L'avis se poursuit comme suit : « (...) bien que les lois pénales précitées visent - explicitement ou implicitement - des associations telles que des milices privées (...), elles ne tendent essentiellement qu'à désigner des personnes qui, en raison de leur implication dans cette association, peuvent être poursuivies pénalement (...) » (pt. 27, p. 56). Un raisonnement par analogie peut être suivi en l'espèce quant à la mise en œuvre d'une mesure de restriction d'accès numérique.

65. Le présent projet viserait donc à prévoir un mécanisme national parallèle à celui mis en place par le DSA et le RTCO, sans les moyens d'en assurer une mise en œuvre transfrontalière effective.

3.2.2.2. Le caractère nécessaire et proportionné des mesures de mise en œuvre

66. Sur la base des alinéas 3 et 4 de l'article 5, § 3, les autorités et services chargées de l'exécution et du suivi des mesures de restriction d'accès numérique disposeront d'une très grande flexibilité quant à la nature des injonctions à adresser et quant à leurs destinataires, pour autant que celles-ci soient « strictement nécessaires » à l'exécution effective de cette mesure.
67. En l'état, le projet de texte n'apporte pas davantage de précisions quant aux types de mesures (autres que le simple blocage du compte initial de l'entité visée auprès du fournisseur de service concerné) qui pourraient faire l'objet d'une injonction³⁰, ni quant aux destinataires de celles-ci, qui pourraient dès lors vraisemblablement s'étendre à un périmètre plus large que celui des seuls fournisseurs des services visés par l'interdiction.
68. Dans ce contexte, une lecture maximaliste du projet de texte permettrait de considérer que, dans l'hypothèse où le fournisseur d'un service, par exemple une plateforme en ligne, dont l'utilisation aurait été interdite à certains utilisateurs ne se conformerait pas aux injonctions de restriction d'accès numérique, l'autorité compétente pourrait, par exemple, à imposer aux fournisseurs de services d'accès à Internet (ISP's)³¹ de bloquer l'accès à ce service sur le territoire belge. Une telle mesure reviendrait cependant à priver dudit service non pas uniquement le ou les utilisateurs visés par la mesure de restriction d'accès numérique, mais l'ensemble des utilisateurs de ce service sur le territoire belge. Or, une telle mesure paraît difficilement conciliable avec l'exigence de proportionnalité.
69. En outre, réserver une telle marge d'appréciation quant à la nécessité et la proportionnalité de mesures potentiellement aussi intrusives à l'égard des droits fondamentaux concernés pose également fondamentalement question sous l'angle du respect du principe de légalité³².

³⁰ Il n'apparaît, par exemple, pas clairement quels seraient les actes « matériels » ou « techniques » strictement nécessaires pour les besoins de l'exécution de la mesure de restriction d'accès numérique.

³¹ Qui relèvent à la fois de la notion de « **fournisseurs de services intermédiaires** » au sens de l'article 3, § 1^{er}, point g), i), du DSA et de la notion de « **fournisseur de service de communications électroniques** » au sens de l'article 2, 4), du Code des communications électroniques européen.

³² Nous renvoyons, à cet égard, notamment aux considérations émises dans le cadre de [l'Avis n° 2025/9 du 18 septembre 2025 de l'Institut Fédéral pour la protection et la promotion des Droits Humains](#).

4. Conclusion

70. En ce qui concerne l'avant-projet de loi relative à l'interdiction administrative des activités des personnes morales, des sociétés sans personnalité juridique, des associations ou groupements de fait constituant une menace grave et actuelle pour la sécurité nationale, il ressort de ce qui précède que l'IBPT ne dispose pas des compétences nécessaires à la mise en œuvre dudit projet.
71. Dans son rôle d'autorité de régulation du numérique, notamment dans le cadre du DSA et du RTCO, l'IBPT est compétent pour faire respecter certaines obligations de diligence imposées aux services intermédiaires numériques, sans toutefois être habilité à apprécier l'illégalité des contenus circulant via ces services. La création d'une « base légale complémentaire » ne constituerait pas un simple élargissement des missions existantes de l'IBPT, mais serait de nature à confier à l'IBPT un rôle qui sort manifestement de ses missions actuelles, y compris dans son rôle de régulateur numérique. Elle l'amènerait en effet à intervenir dans le domaine de la sécurité nationale, lequel relève d'autres autorités disposant de l'expertise requise à cet effet.
72. Les réserves principales suivantes sont émises quant au mécanisme envisagé, et en particulier, quant à la mesure de restriction d'accès numérique visée à l'article 5, § 1^{er}, 1^o, d) du premier avant-projet de loi.
73. *Premièrement*, les fournisseurs et services concernés devraient être davantage précisés afin d'éviter toute ambiguïté quant à la portée de la mesure envisagée.
74. *Deuxièmement*, les mesures de mise en œuvre et leurs destinataires devraient être déterminés par la loi, tenant compte des exigences de nécessité et de proportionnalité, mais également des contraintes en termes d'effectivité de ces mesures. À cet égard, le contexte légal européen (DSA, RTCO et autres initiatives en cours) devrait être pris en compte, de même que les difficultés pratiques liées à l'absence de présence des fournisseurs de service concernés sur le territoire belge.
75. En ce qui concerne l'avant-projet de loi *relatif aux recours devant le Conseil d'État contre les mesures d'interdiction administrative prévues par la loi du XXX relative à l'interdiction administrative des activités de certaines entités constituant une menace grave et actuelle pour la sécurité nationale*, si ce dernier devait effectivement être couplé à une base légale complémentaire mandatant l'IBPT pour un rôle d'autorité administrative, aurait pour conséquence une différence entre le type de voie de recours utilisé par un même acteur, c'est-à-dire les fournisseurs de services soumis à plusieurs réglementations relevant de la compétence de l'IBPT, selon le type de litige concerné.

Bernardo Herman
Membre du Conseil

Peggy Valcke
Membre du Conseil

Stefaan Vyverman
Membre du Conseil

Michel Van Bellinghen
Président du Conseil