



CONSEIL D'ÉTAT
section de législation

RAAD VAN STATE
afdeling Wetgeving

avis 74.861/4
du 10 janvier 2024

advies 74.861/4
van 10 januari 2024

sur

over

un avant-projet de loi
‘établissant un cadre pour la
cybersécurité des réseaux et
des systèmes d’information
d’intérêt général pour la
sécurité publique’

een voorontwerp van wet ‘tot
vaststelling van een kader voor
de cyberbeveiliging van
netwerk- en
informatiesystemen van
algemeen belang voor de
openbare veiligheid’

Le 13 novembre 2023, le Conseil d'État, section de législation, a été invité par le Premier Ministre à communiquer un avis dans un délai de trente jours, sur un avant-projet de loi 'établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique'.

L'avant-projet a été examiné par la quatrième chambre le 10 janvier 2024. La chambre était composée de Bernard BLERO, président de chambre, Luc CAMBIER et Dimitri YERNAULT, conseillers d'État, Christian BEHRENDT et Jacques ENGLEBERT, assesseurs, et Charles-Henri VAN HOVE, greffier.

Le rapport a été présenté par Roger WIMMER, premier auditeur, et Xavier MINY, auditeur adjoint.

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

L'avis, dont le texte suit, a été donné le 10 janvier 2024.

*

Op 13 november 2023 is de Raad van State, afdeling Wetgeving, door de Eerste Minister verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid'.

Het voorontwerp is door de vierde kamer onderzocht op 10 januari 2024. De kamer was samengesteld uit Bernard BLERO, kamervoorzitter, Luc CAMBIER en Dimitri YERNAULT, staatsraden, Christian BEHRENDT en Jacques ENGLEBERT, assessoren, en Charles-Henri VAN HOVE, griffier.

Het verslag is uitgebracht door Roger WIMMER, eerste auditeur, en Xavier MINY, adjunct-auditeur.

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

Het advies, waarvan de tekst hierna volgt, is gegeven op 10 januari 2024.

*

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

Sur ces trois points, l'avant-projet appelle les observations suivantes.

FORMALITÉ PRÉALABLE

L'avant-projet de loi à l'examen comporte diverses dispositions portant sur un traitement de données à caractère personnel, en particulier son titre 6.

L'article 36, paragraphe 4, du 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 (règlement général sur la protection des données)', combiné avec son article 57, paragraphe 1, c), le considérant 96 de son préambule et, le cas échéant, l'article 2, alinéa 2, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', prévoit une obligation de consulter l'autorité de contrôle, en l'occurrence l'Autorité de protection des données visée dans la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement de données à caractère personnel.

Il ressort du dossier transmis et des informations communiquées à la section de législation que l'avant-projet a été envoyé pour avis à l'Autorité de protection des données simultanément à la saisine de la section de législation.

Si l'accomplissement de cette formalité devait encore donner lieu à des modifications du texte soumis au Conseil d'État sur des points autres que de pure forme et ne résultant pas des suites réservées au présent avis, les dispositions modifiées ou ajoutées devraient être soumises à nouveau à l'avis de la section de législation conformément à l'article 3, § 1^{er}, alinéa 1^{er}, des lois coordonnées 'sur le Conseil d'État'.

[‡] S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

OBSERVATIONS GÉNÉRALES

1. Concernant la compétence de l'autorité fédérale dans le cadre de la transposition de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 'concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)' (ci-après, « la directive NIS2 »), le délégué du Premier Ministre a fourni les explications suivantes :

« Le champ d'application de la directive NIS2 porte sur les règles de cybersécurité applicables à certaines entités (fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques), dont la protection relève en droit interne des compétences résiduelles fédérales en matière de sécurité publique. La directive NIS2 détermine, en effet, des mesures destinées à assurer un niveau commun de cybersécurité dans l'ensemble de l'Union européenne pour certaines entités qualifiées comme 'essentielles' ou 'importantes', en raison des services qu'elles fournissent et de leur taille (voir ci-après). Les entités concernées sont celles fournissant des services essentiels énumérés dans les 'secteurs hautement critiques' de l'annexe I ou dans les 'autres secteurs critiques' de l'annexe II.

En application de la directive NIS2 et de la recommandation 2003/361/CE, les 'entités essentielles' sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de 'grande entreprise', c'est-à-dire qui occupe min. 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros (ou le total du bilan annuel excède 43 millions d'euros).

Les 'entités importantes' sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de 'moyenne entreprise', c'est-à-dire qui occupe min. 50 personnes ou réalise un chiffre d'affaires annuel (ou le total du bilan annuel) qui excède 10 millions d'euros. Sont également des 'entités importantes' les organisations qui fournissent un service repris dans l'annexe II et qui répondent aux notions de moyenne ou de grande entreprise.

Outre les considérants, le contenu des dispositions de la directive NIS2 démontre à suffisance que la matière concrète traitée par celle-ci est bien la sécurité des citoyens (utilisateurs des services concernés), des entreprises, des biens et des autorités publiques contre les cybermenaces et les cyberincidents. En effet, la défaillance ou la compromission des réseaux et systèmes d'information de certaines entités jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation (car elles fournissent des services essentiels au maintien d'activités sociétales ou économiques critiques) peut avoir des conséquences importantes pour la société et l'économie. La cybersécurité des 'entités essentielles' ou 'entités importantes' NIS2 relève dès lors clairement de la protection exercée dans le domaine général de la sécurité publique (la protection des personnes physiques, des personnes morales et des biens).

Par ailleurs, la directive NIS2 ne détermine pas des règles de cybersécurité applicables à toutes les organisations actives dans un domaine particulier. Elle fixe des mesures minimales communes de gestion des risques en matière de cybersécurité et de notification des incidents importants (ou des cybermenaces importantes) à toutes les entités essentielles et importantes, sans distinction entre leur secteur d'activités.

La nature générale (transsectorielle) et commune des mesures envisagées par la directive (visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne) démontre l'absence de lien entre la matière concrète traitée par la directive et les différents secteurs repris dans ses annexes (les actes juridiques sectoriels de l'Union sont d'ailleurs explicitement exclus du champ d'application de la directive par l'article 4).

Cette analyse juridique a été confirmée par la section législation du Conseil d'État dans son avis sur le projet qui allait devenir la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après la 'loi NIS1') qui a transposé la Directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la 'directive NIS1').

Dans son avis sur la loi NIS1 (n° 62.296/4 du 2 mai 2018), le Conseil d'État a souligné que la transposition de la directive NIS1 pouvait 'soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédéral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles qu'il exerce dans le domaine de la sécurité publique' mais que le projet ne soulevait aucun problème de compétence.

À cet égard, le Conseil d'État a rappelé l'analyse formulée à propos de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques (avis n° 48.989/VR 1 du 9 décembre 2010) :

'[...] L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme le point [...] qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif [...] du fait de la défaillance de ces fonctions [...].

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral.

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local' ».

Dans l'avis 63.296/4 donné le 2 mai 2018 sur un avant-projet devenu la loi du 7 avril 2019 'établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique', la section de législation a en effet observé ce qui suit :

« Ce n'est pas la première fois que la section de législation est saisie d'un avant-projet de loi visant, en exécution d'une directive européenne à transposer, à recenser des opérateurs de services essentiels en vue d'assurer de manière préventive la protection de certaines de leurs infrastructures jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation.

Cette opération peut soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédéral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles qu'il exerce dans le domaine de la sécurité publique.

Cette question de compétence a été analysée dans les termes suivants à l'occasion de l'avis n° 48.989/VR¹ donné le 9 décembre 2010 sur un avant-projet devenu la loi du 1^{er} juillet 2011 'relative à la sécurité et la protection des infrastructures critiques' :

'1. Ainsi que l'exprime son article 2, alinéa 1^{er}, l'avant-projet à l'examen a notamment pour objet de transposer la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (ci-après, la directive).

Comme l'énonce l'article 1^{er} de la directive, il s'agit d'établir une procédure de recensement et de désignation des infrastructures critiques européennes en vue d'éventuellement améliorer leur protection afin de contribuer à la protection des personnes. L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme 'le point (...) qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif (...) du fait de la défaillance de ces fonctions'. L'article 3, paragraphe 3, de la directive mentionne qu'elle s'applique pour l'instant uniquement dans les secteurs de l'énergie et des transports. Selon le premier considérant de la directive, ses auteurs ont d'abord eu en vue l'adoption de 'mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques'. Par la suite, tout en maintenant 'une priorité donnée à la lutte contre la menace terroriste', le programme européen de protection des infrastructures critiques, dont la directive est un instrument, s'est fondé sur 'une approche tous risques (qui) tient compte des risques d'origine humaine, des menaces technologiques et des catastrophes naturelles dans le processus de protection des infrastructures critiques' (troisième considérant).

¹ Note de bas de page n° 1 de l'avis cité : Doc. parl., Chambre, 2010-2011, n° 1357/001, pp. 53-64, <http://www.raadvst-consetat.be/dbx/avis/48989.pdf>.

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral ².

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local.

2. Toutefois, les mesures qui seront prises sur la base de l'avant-projet seront susceptibles de concerner des opérateurs exploitant des infrastructures qui, envisagées d'un autre point de vue, pourraient relever de la compétence matérielle des régions, s'agissant spécialement des secteurs de l'énergie et du transport, auxquels la directive s'applique (article 6, § 1^{er}, VII et X, de la loi spéciale du 8 août 1980 de réformes institutionnelles).

L'auteur de l'avant-projet est d'ailleurs sensible à cet aspect des choses puisqu'il a le souci d'associer les régions à la réglementation applicable et à sa mise en œuvre, comme en témoignent les dispositions suivantes de l'avant-projet :

– l'article 5, § 1^{er}, alinéa 2, selon lequel l'autorité sectorielle ³ procède à l'identification des infrastructures critiques européennes 'après avis conforme des régions pour les infrastructures critiques potentielles relevant de leurs compétences' ;

– l'article 6, § 2, selon lequel l'autorité sectorielle 'établit des critères sectoriels auxquels doivent répondre les infrastructures critiques européennes eu égard aux caractéristiques particulières du secteur concerné, (...), le cas échéant, après avis conforme des régions concernées' ;

– l'article 6, § 5, selon lequel 'l'autorité sectorielle établit au cas par cas les seuils applicables aux critères intersectoriels auxquels doivent répondre les infrastructures critiques européennes, (...), le cas échéant après avis conforme des régions concernées' ;

– l'article 7, § 2, alinéa 2, selon lequel la Direction générale Centre de Crise du service public fédéral Intérieur (ci-après, DGCC) 'est chargée en collaboration (...), le cas échéant, avec les régions concernées (...) de mener des discussions bilatérales ou multilatérales avec les États membres de l'Union européenne concernés (...) en ce qui concerne les infrastructures critiques européennes potentielles identifiées sur le territoire belge (...)'

– l'article 13, § 6, alinéa 2, selon lequel 'le Roi, le cas échéant, en accord avec les régions concernées, détermine pour un secteur ou un sous-secteur déterminé la fréquence des exercices et des mises à jour' du plan de sécurité de l'exploitant d'une infrastructure critique européenne ;

– l'article 24, § 2, alinéa 2, selon lequel le Roi 'peut fixer les modalités du contrôle, le cas échéant en accord avec les régions concernées', du respect des dispositions de la loi en projet par les exploitants d'infrastructures concernées par celle-ci.

² Note de bas de page n° 2 de l'avis cité : Note de bas de page n° 1 de l'avis cité : C.E., État belge, n° 175.462, 8 octobre 2007. Pour d'autres exemples de lois adoptées par l'État fédéral en vue d'assurer la protection préventive des « fonctions vitales de la société », voir la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité qui vise notamment à protéger « le potentiel économique du pays » ou la loi du 10 juillet 2006 relative à l'analyse de la menace qui a notamment en vue les « intérêts fondamentaux » du pays.

³ Note de bas de page n° 3 de l'avis cité : Note de bas de page n° 2 de l'avis cité : Pour les infrastructures critiques européennes, l'autorité sectorielle est le ministre fédéral ayant les Transports dans ses attributions ou son délégué (article 3, 3°, a, de l'avant-projet) ou le ministre fédéral ayant l'Énergie dans ses attributions ou son délégué (article 3, 3°, b), de l'avant-projet.

3. Comme les régions détiennent des compétences dans les domaines de l'énergie et du transport, qu'il pourrait en être de même pour d'autres secteurs auxquels la loi en projet s'appliquerait et que, selon l'auteur de l'avant-projet lui-même, dans l'exécution de la loi, l'incidence de certaines des mesures envisagées pourrait affecter la gestion d'infrastructures relevant des compétences régionales, il est admissible d'associer les régions à l'adoption des mesures d'exécution du texte en projet.

Toutefois, ce faisant, il doit le faire d'une manière qui respecte l'autonomie des différents niveaux de pouvoir. Le législateur fédéral ne peut imposer unilatéralement – par le biais d'une loi ordinaire – une collaboration forcée des régions au système mis en place par l'avant-projet. L'intervention des régions ne peut être prévue, si nécessaire, que de façon facultative et en manière telle que leur éventuelle abstention n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale compétente.

4. Si, dans l'avenir, il devait s'avérer que l'adoption des mesures d'exécution de la loi devait impliquer l'exercice conjoint de compétences propres à l'autorité fédérale et aux régions, et non plus uniquement la mise en œuvre de la seule compétence fédérale en matière de sécurité publique, il conviendrait de conclure un accord de coopération avec les régions sur ces questions' »⁴.

Cette observation vaut *mutatis mutandis* pour l'avant-projet à l'examen, dans le cadre duquel les régions et/ou les communautés sont associées au processus opératoire par l'effet des articles 3, § 3, 3°, 11, §§ 3 et 4, 15, § 2, alinéa 3, et 44, § 1^{er}, alinéa 2, de l'avant-projet, chaque fois d'une manière compatible avec les principes dégagés ci-dessus.

Il ne peut par ailleurs pas être exclu que les communautés et les régions, agissant dans le cadre de leurs compétences matérielles, puissent également elles-mêmes protéger certaines catégories d'intérêts de sécurité qui coïncident avec des éléments sur lesquels se fonde l'appréciation de la sécurité publique⁵.

L'avant-projet ne soulève dès lors aucun problème de compétence au regard de ces principes.

2. De manière complémentaire aux règles générales d'identification, l'article 11 de l'avant-projet charge l'autorité nationale de cybersécurité d'identifier dans certaines circonstances une entité comme entité essentielle ou importante.

⁴ *Doc. parl.*, Chambre, 2018-2019, n° 54-3340/001, pp. 75-87.

⁵ Voir en ce sens l'avis 67.887/1 donné le 28 septembre 2020 sur un avant-projet de loi « visant à instaurer un mécanisme de filtrage des investissements directs étrangers », observation n° 3.1.

Interrogé quant aux motifs pour lesquels cette mission est confiée à l'autorité nationale de cybersécurité, le délégué du Premier Ministre a répondu ce qui suit :

« Les entités essentielles et importantes visées par la directive 2022/2555 ('directive NIS2') sont principalement celles répondant aux définitions reprises aux annexes I ou II de la directive NIS2 et, sauf exception, à la taille (équivalente à une entreprise moyenne ou large au sens de l'annexe de la recommandation 2003/361/CE). Il n'y a pas d'identification nécessaire pour ces entités (celles-ci auront au contraire l'obligation de s'enregistrer voir l'art. 13 de l'APL).

Toutefois, les articles 2 (2) b)-e) et 3 (1) e) & (2) de la directive imposent le maintien d'un processus d'identification au niveau national pour certaines entités essentielles ou importantes complémentaires.

Conformément à l'article 11 de l'APL, le choix a été fait de confier à l'autorité nationale de cybersécurité (le projet d'arrêté royal approuvé par le Conseil des Ministres prévoit la désignation du Centre pour la Cybersécurité Belgique – 'CCB' pour assurer ce rôle) le soin de coordonner le processus d'identification complémentaire et de prendre la décision formelle d'identification, après différentes consultations préalables (l'entité concernée, les éventuelles entités fédérées concernées, les autorités sectorielles concernées ou encore le Comité stratégique du renseignement et de la sécurité).

Il s'agit d'assurer une cohérence avec les autres missions légales confiées à l'autorité nationale de cybersécurité par l'APL (voir l'art. 16 et s. de l'APL) : mission de coordination de la loi, mission de supervision (service d'inspection et de sanction), mission de CSIRT national (gestion des incidents), mission de représentation au niveau européen, etc.

S'agissant d'un acte administratif motivé d'une autorité administrative (CCB), l'identification formelle pourra être contestée devant la section du contentieux administratif du Conseil d'État. Ce faisant, les garanties prévues par les lois coordonnées sur le Conseil d'État et la loi sur la motivation formelle des actes administratifs s'appliqueront ».

Néanmoins, en désignant directement des services du pouvoir exécutif pour exercer des missions liées à l'exécution de l'avant-projet et pour prendre des décisions formelles d'identification, le pouvoir législatif s'immisce dans l'organisation interne du pouvoir exécutif. C'est en principe au Roi qu'il revient de désigner ceux de ses services qui seront chargés d'intervenir dans le processus d'identification qui résulte de la mise en œuvre de la loi.

C'est ainsi au Roi qu'il appartient de compléter la liste des entités essentielles et importantes soumises à la loi en application de la directive NIS2 ou de déléguer ce pouvoir à un service relevant de son autorité.

3. Le dispositif en projet fait référence à des textes législatifs en cours d'élaboration.

Ainsi, à l'article 8, les définitions prévues aux 43°, 45° et 49° comportent une double référence, d'une part, à des textes qui existent et, d'autre part, à des projets de textes législatifs, à savoir respectivement la loi CER et la loi NCCN. La définition prévue au 44° renvoie également à un projet de texte législatif, la loi NPU. L'avant-projet contient en outre, dans diverses dispositions, des références faites aux lois CER, NCCN et NPU.

À ce propos, le délégué du Premier Ministre a communiqué les informations suivantes :

« Sur base des dernières informations reçues de nos collègues du Centre de crise national (NCCN), il s'avère l'avant-projet de loi relatif à la planification d'urgence et à la gestion de crise (loi NPU) devrait être soumise prochainement au Conseil des Ministres. Pour les autres avant-projets de lois, il semble toutefois que ceux-ci ne seront, en définitive, pas adoptés avant la présente loi.

Ces références ont été volontairement accompagnées ou mentionnées entre crochets dans le dispositif du présent avant-projet de loi pour être adaptées en fonction des derniers développements de ces autres avant-projets.

Il faudra dès lors vraisemblablement remplacer les mentions 'loi CER' par la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques et les mentions 'loi NCCN' par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise ».

Une telle manière de faire ne permet pas à la section de législation de déterminer avec suffisamment de précision la portée et le contenu de certaines dispositions. Tel est le cas, par exemple, de l'article 29 de l'avant-projet portant sur le plan national de réaction aux crises et incidents de cybersécurité majeurs qui renvoie à la loi NPU dont l'avant-projet n'a pas encore été soumis au Conseil des ministres, ainsi que de l'article 68, 5°, de l'avant-projet qui énonce que pour la finalité mentionnée à l'article 67, 5°, de l'avant-projet, sont traitées « les données d'identification des personnes concernées par la coopération dans le cadre de la loi CER ».

Le dispositif sera revu afin de renvoyer aux dispositions pertinentes, à savoir celles qui seront en vigueur au moment où la loi en projet sera publiée et entrera elle-même en vigueur. L'auteur de l'avant-projet s'assurera par ailleurs de la cohérence de l'avant-projet avec les dispositifs légaux auxquels celui-ci renvoie.

Compte tenu de ces incertitudes, il va de soi que l'absence d'observation sur tel ou tel aspect de l'avant-projet dans le présent avis ne saurait être interprétée en ce sens que ces aspects ne soulèvent aucune difficulté juridique en ce qui concerne la correcte transposition de la directive NIS2 et la conformité du dispositif à l'examen aux normes de droit supérieures pertinentes.

OBSERVATIONS PARTICULIÈRES

Article 11

1. Au paragraphe 3, alinéa 2, au lieu de prévoir que lorsqu'aucun avis d'une entité visée à l'alinéa 1^{er} n'est rendu dans le délai prévu par ce même alinéa, « l'avis est réputé être favorable », il sera prévu qu'en l'absence d'un avis rendu dans le délai visé à l'alinéa 1^{er}, il peut être passé outre à l'absence d'avis.

2. Au paragraphe 5, il est prévu ce qui suit :

« Dans les cas visés au paragraphe 1^{er}, le Roi peut, par arrêté délibéré en Conseil des ministres désigner comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe ».

Selon le commentaire de l'article,

« [L]e paragraphe 5 prévoit la possibilité pour le Roi, par arrêté délibéré en Conseil des ministres, de désigner individuellement comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe de la loi. En effet, une entité ou un sous-traitant particulier d'une entité NIS pourrait fournir un service critique justifiant d'être soumis aux dispositions de la loi alors que par ailleurs ses activités ne relèvent pas de l'un des secteurs repris dans les annexes de la loi. L'application de cet article est limitée à des cas particuliers et implique au préalable de la décision du Comité stratégique du renseignement et de la sécurité, une concertation entre l'entité concernée, l'autorité nationale de cybersécurité, les entités fédérées et l'éventuelle autorité sectorielle ».

Il en résulte que préalablement à la décision du Comité stratégique du renseignement et de la sécurité, « une concertation entre l'entité concernée, l'autorité nationale de cybersécurité, les entités fédérées et l'éventuelle autorité sectorielle » doit avoir lieu.

La disposition sera revue et complétée pour y faire figurer l'encadrement procédural de l'habilitation faite au Roi.

Article 21

Au paragraphe 2, alinéa 2, il est prévu ce qui suit :

« Les finalités poursuivies par les tâches précitées sont :

1° sans préjudice des compétences des personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction, la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave ;

2° la prévention de menaces graves contre la sécurité publique ;

3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information ».

La section de législation n'aperçoit cependant pas pourquoi le rappel des compétences des personnes exerçant la police judiciaire se limite à l'hypothèse envisagée au 1°.

Interrogé à ce sujet, le délégué du Premier Ministre a répondu ce qui suit :

« L'ajout à l'article 21, § 2, alinéa 1^{er} ('sans préjudice des compétences des personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction') a été inséré au cours des discussions des textes afin de confirmer ce qui était une évidence : les missions de l'autorité nationale de cybersécurité (CCB) s'exercent sans préjudice des missions légales dévolues personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction.

Le cas échéant, cette mention pourrait accompagner l'ensemble de l'article 21 (lequel a pour vocation initiale d'habiliter l'autorité nationale de cybersécurité à accomplir certaines tâches ».

La précision relative aux compétences des personnes exerçant la police judiciaire figurera dès lors dans la phrase introductive de l'article à l'examen.

Article 23

Le commentaire de la disposition précise que

« [...] toutes les données collectées par le hacker éthique devraient être supprimées dans un délai raisonnable après le signalement. Si cela s'avère nécessaire de conserver ces données encore pendant un certain temps ou si une procédure judiciaire est en cours, le hacker éthique doit veiller à ce que ces données sont conservées en toute sécurité durant cette période ».

Le dispositif sera complété afin d'énoncer le régime relatif à la suppression des données collectées qui est évoqué dans le commentaire de l'article.

Article 26

Au paragraphe 1^{er}, il est prévu que la disposition ne porte pas préjudice à l'application de la loi du 11 décembre 1998 'relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé'.

Or, il résulte déjà de l'article 5, § 2, que l'avant-projet est sans préjudice de la loi du 11 décembre 1998.

Le dispositif sera réexaminé et, le cas échéant, revu, afin de veiller à l'articulation des articles 5 et 26 et d'éviter les dispositifs redondants.

Article 29

Compte tenu de l'article 9, paragraphe 4, de la directive NIS2 que l'article 29 tend à transposer et à l'instar de ce que mentionne l'intitulé du chapitre 5 du titre 2 en projet, au paragraphe 1^{er}, première phrase, et dans la phrase introductive du paragraphe 2, les mots « plan national de réaction aux crises et incidents de cybersécurité » seront complétés par le mot « majeurs ».

Article 30

Le paragraphe 1^{er} tend à transposer l'article 21, paragraphe 1, alinéa 1^{er}, de la directive NIS2.

Ce dernier prévoit que les États membres veillent à ce que « [l]es entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services ». Or, le paragraphe 1^{er} ne fait mention que de « mesures appropriées et proportionnées » sans préciser qu'il s'agit de mesures « techniques, opérationnelles et organisationnelles » comme le prévoit la directive.

La disposition sera réexaminée et, le cas échéant, revue, afin d'assurer la transposition complète de la directive NIS2.

Article 44

Au paragraphe 1^{er}, le contenu de l'alinéa 2 figure déjà à l'article 39, alinéa 2, de l'avant-projet.

Le dispositif sera réexaminé et, le cas échéant, revu, afin de veiller à l'articulation des articles 39 et 44 et d'éviter les dispositifs redondants.

Article 59

1. À l'alinéa 1^{er}, 1^o, de l'accord du délégué du Premier Ministre, les mots « à l'article 11, § 5 » seront remplacés par les mots « à l'article 12 ».

2. Selon l'alinéa 1^{er}, 3^o, « [e]st puni d'une amende de 500 à 200 000 euros quiconque ne se conforme pas aux obligations de contrôle visées au présent titre ». Le titre 4 auquel se réfère le dispositif englobe un grand nombre d'obligations.

Comme la section de législation l'a rappelé à diverses reprises, « [l]e droit de ne pas s'auto-incriminer, garanti par l'article 6 de la Convention européenne des droits de l'homme, fait toutefois obstacle à ce qu'une personne, 'pénalement accusée' au sens de cette disposition, puisse être sanctionnée pour avoir refusé de prêter son concours à l'établissement de sa propre culpabilité »⁶.

L'article 48, § 4, alinéa 1^{er}, 3^o, de l'avant-projet prévoit que la personne auditionnée par le service de l'inspection a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Il faut donc considérer que l'alinéa 1^{er}, 3^o, est applicable sans préjudice de l'article 48, § 4, alinéa 1^{er}, 3^o, de l'avant-projet.

Partant, et pour éviter toute méprise à ce sujet, mieux vaut ajouter au début de la disposition les mots « Sans préjudice de l'article 48, § 4, alinéa 1^{er}, 3^o, ».

Article 65

De l'accord du délégué du Premier Ministre, les mots « visé à l'alinéa 1^{er} » seront remplacés par les mots « visé à l'article 64 ».

Article 79

Au 1^o, les mots « l'autorité nationale de cybersécurité visée à l'article 8, 47^o, » seront remplacés par les mots « l'autorité nationale de cybersécurité visée à l'article 8, 46^o, ».

La même observation vaut pour le 2^o.

Article 83

1. Aux 2^o et 3^o, les mots « au sens de l'article 8, 24^o, de cette même loi » seront insérés après les mots « prestataires de services de confiance ».

⁶ Avis 60.619/2 donné le 25 janvier 2017 sur un avant-projet devenu la loi du 2 octobre 2017 'réglementant la sécurité privée et particulière', *Doc. parl.*, Chambre, 2016-2017, n° 54-2388/001, p. 194. Voir aussi l'avis 63.296/4 ; l'avis 64.879/4 donné le 4 février 2019 sur un avant-projet devenu le décret du 2 mai 2019 'modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé', *Doc. parl.*, Parl. w., 2018-2019, n° 1332/1, pp. 25-35 ; et l'avis 70.306/2 donné le 23 novembre 2021 sur un avant-projet devenu la loi du 23 février 2022 'visant à mettre en œuvre le règlement (UE) 2020/1503 du parlement européen et du conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937 et à transposer la directive (UE) 2021/338 du parlement européen et du conseil du 16 février 2021 modifiant la directive 2014/65/UE en ce qui concerne les obligations d'information, la gouvernance des produits et les limites de position, et les directives 2013/36/UE et (UE) 2019/878 en ce qui concerne leur application aux entreprises d'investissement, afin de soutenir la reprise à la suite de la crise liée à la COVID-19', *Doc. parl.*, Chambre, 2021-2022, n° 55-2400/001, pp. 84-98.

2. Au 3°, les mots « comme autorité sectorielle et service d'inspection sectoriel pour » seront remplacés par les mots « comme autorité sectorielle au sens de l'article 8, 55°, de cette même loi et service d'inspection sectoriel au sens de l'article 44, § 1^{er}, alinéa 2, de cette même loi pour ».

Article 85

Dans l'article 2, 94°, en projet (article 85, 5°, de l'avant-projet), les mots « comme prévu dans la loi » seront remplacés par les mots « au sens de l'article 8, 24°, de la loi ».

Article 87

Dans l'article 107/4, § 6, en projet, les mots « dans le chapitre 2 de la loi NIS 2 » seront remplacés par les mots « dans le titre 4, chapitre 2, de la loi du [XX XXXX XXXX] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ».

Annexes

Conformément aux annexes I et II de la directive NIS2, l'intitulé complet des directives et règlements qui y figurent sera inséré dans les tableaux.

OBSERVATIONS FINALES

1. Les tableaux de correspondance, le cas échéant, lus en combinaison avec l'exposé des motifs et le commentaire des articles, doivent notamment permettre d'appréhender la mesure dans laquelle la directive NIS2 est correctement transposée.

Or, il apparaît que les tableaux qui ont été transmis à la section de législation sont, pour plusieurs dispositions de l'avant-projet, en défaut de satisfaire aux exigences de précision auxquelles pareils tableaux doivent se conformer.

2. Ainsi, dans les tableaux, les articles 84 et 87 de l'avant-projet ne constituent pas des dispositions nationales étrangères à la transposition de la directive NIS2, mais constituent au contraire des dispositions transposant cette directive.

3. En outre, il y a lieu, dans le premier tableau, d'indiquer :

– que l'article 3, § 1^{er}, alinéa 2, de l'avant-projet transpose l'article 2, paragraphe 1, alinéa 2, de la directive ;

– que l'article 4, § 4, de l'avant-projet transpose l'article 26, paragraphe 2, de la directive ;

- que l'article 5, § 5, de l'avant-projet transpose l'article 2, paragraphe 8, de la directive ;
- que l'article 20, 1°, de l'avant-projet transpose l'article 10, paragraphe 3, de la directive ;
- que l'article 37, § 2, de l'avant-projet transpose l'article 23, paragraphe 7, de la directive ;
- que l'article 37, § 3, de l'avant-projet transpose l'article 23, paragraphe 8, de la directive ;
- que l'article 37, § 4, de l'avant-projet transpose l'article 23, paragraphe 9, de la directive ;
- que l'article 37, § 5, de l'avant-projet transpose l'article 23, paragraphe 10, de la directive ;
- que l'article 46, §§ 2 et 3, de l'avant-projet transpose l'article 37, paragraphe 1, de la directive ;
- que l'article 48, § 7, alinéa 2, de l'avant-projet transpose l'article 35, paragraphe 3, de la directive.

4. Les principes de technique législative établis par la section de législation invitent les auteurs d'avant-projets, lors d'une transposition de directive, à établir des tableaux de transposition :

« 191. Établissez deux tableaux de transposition.

191.1. Pour contrôler qu'une directive est transposée correctement et complètement, établissez un tableau de correspondance entre les (subdivisions des) articles de la directive et les (subdivisions des) articles de l'acte de transposition que vous rédigez. Mentionnez également dans ce tableau :

a) les (subdivisions des) articles de la directive qui ont éventuellement déjà été transposés, en correspondance avec les actes de droit interne et les (subdivisions des) articles qui ont procédé à cette transposition ;

b) les (subdivisions des) articles de la directive qui doivent encore être transposés par une autre autorité.

191.2. Pour pouvoir lire chaque article de l'acte de transposition à la lumière des exigences de la directive, établissez aussi un tableau de correspondance entre les (subdivisions des) articles de l'acte de transposition et les (subdivisions des) articles de la directive »⁷.

⁷ *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet « Technique législative », recommandations n^{os} 191 à 191.2.

Il convient dès lors de prévoir un tableau reprenant les (subdivisions des) articles de la directive qui doivent encore être transposés par une autre autorité.

*

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

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

VOORAFGAAND VORMVEREISTE

Het voorliggende voorontwerp van wet bevat verschillende bepalingen, met name in titel 6, die betrekking hebben op de verwerking van persoonsgegevens.

Artikel 36, lid 4, van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 ‘betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)’, gelezen in samenhang met artikel 57, lid 1, c), en overweging 96 van de preambule van die verordening en in voorkomend geval met artikel 2, tweede lid, van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, schrijft voor dat de toezichthoudende autoriteit, *in casu* de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 ‘tot oprichting van de Gegevensbeschermingsautoriteit’, wordt geraadpleegd bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel, in verband met de verwerking van persoonsgegevens.

Uit het dossier en de informatie die aan de afdeling Wetgeving zijn bezorgd, blijkt dat de Gegevensbeschermingsautoriteit tegelijk met de afdeling Wetgeving om advies over het voorontwerp is verzocht.

Indien de aan de Raad van State voorgelegde tekst naar aanleiding van het vervullen van dat vormvereiste nog wijzigingen zou ondergaan die niet louter vormelijk zijn en niet voortvloeien uit het gevolg dat aan dit advies wordt gegeven, moeten de gewijzigde of toegevoegde bepalingen op hun beurt om advies aan de afdeling Wetgeving worden voorgelegd, overeenkomstig artikel 3, § 1, eerste lid, van de gecoördineerde wetten ‘op de Raad van State’.

[‡] Aangezien het om een voorontwerp van wet gaat, wordt onder “rechtsgrond” de overeenstemming met de hogere rechtsnormen verstaan.

ALGEMENE OPMERKINGEN

1. Met betrekking tot de bevoegdheid van de federale overheid in het kader van de omzetting van richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 ‘betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)’ (hierna: “de NIS 2-richtlijn”), heeft de gemachtigde van de eerste minister de volgende toelichting gegeven:

“Le champ d’application de la directive NIS2 porte sur les règles de cybersécurité applicables à certaines entités (fournissant des services essentiels au maintien d’activités sociétales ou économiques critiques), dont la protection relève en droit interne des compétences résiduelles fédérales en matière de sécurité publique. La directive NIS2 détermine, en effet, des mesures destinées à assurer un niveau commun de cybersécurité dans l’ensemble de l’Union européenne pour certaines entités qualifiées comme ‘essentiels’ ou ‘importantes’, en raison des services qu’elles fournissent et de leur taille (voir ci-après). Les entités concernées sont celles fournissant des services essentiels énumérés dans les ‘secteurs hautement critiques’ de l’annexe I ou dans les ‘autres secteurs critiques’ de l’annexe II.

En application de la directive NIS2 et de la recommandation 2003/361/CE, les ‘entités essentielles’ sont les organisations qui fournissent un service repris dans l’annexe I et qui répondent à la notion de ‘grande entreprise’, c’est-à-dire qui occupe min. 250 personnes ou dont le chiffre d’affaires annuel excède 50 millions d’euros (ou le total du bilan annuel excède 43 millions d’euros).

Les ‘entités importantes’ sont les organisations qui fournissent un service repris dans l’annexe I et qui répondent à la notion de ‘moyenne entreprise’, c’est-à-dire qui occupe min. 50 personnes ou réalise un chiffre d’affaires annuel (ou le total du bilan annuel) qui excède 10 millions d’euros. Sont également des ‘entités importantes’ les organisations qui fournissent un service repris dans l’annexe II et qui répondent aux notions de moyenne ou de grande entreprise.

Outre les considérants, le contenu des dispositions de la directive NIS2 démontre à suffisance que la matière concrète traitée par celle-ci est bien la sécurité des citoyens (utilisateurs des services concernés), des entreprises, des biens et des autorités publiques contre les cybermenaces et les cyberincidents. En effet, la défaillance ou la compromission des réseaux et systèmes d’information de certaines entités jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation (car elles fournissent des services essentiels au maintien d’activités sociétales ou économiques critiques) peut avoir des conséquences importantes pour la société et l’économie. La cybersécurité des ‘entités essentielles’ ou ‘entités importantes’ NIS2 relève dès lors clairement de la protection exercée dans le domaine général de la sécurité publique (la protection des personnes physiques, des personnes morales et des biens).

Par ailleurs, la directive NIS2 ne détermine pas des règles de cybersécurité applicables à toutes les organisations actives dans un domaine particulier. Elle fixe des mesures minimales communes de gestion des risques en matière de cybersécurité et de notification des incidents importants (ou des cybermenaces importantes) à toutes les entités essentielles et importantes, sans distinction entre leur secteur d’activités.

La nature générale (transsectorielle) et commune des mesures envisagées par la directive (visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne) démontre l'absence de lien entre la matière concrète traitée par la directive et les différents secteurs repris dans ses annexes (les actes juridiques sectoriels de l'Union sont d'ailleurs explicitement exclus du champ d'application de la directive par l'article 4).

Cette analyse juridique a été confirmée par la section législation du Conseil d'État dans son avis sur le projet qui allait devenir la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après la 'loi NIS1') qui a transposé la Directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la 'directive NIS1').

Dans son avis sur la loi NIS1 (n° 62.296/4 du 2 mai 2018), le Conseil d'État a souligné que la transposition de la directive NIS1 pouvait 'soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédéral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles qu'il exerce dans le domaine de la sécurité publique' mais que le projet ne soulevait aucun problème de compétence.

À cet égard, le Conseil d'État a rappelé l'analyse formulée à propos de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (avis n° 48.989/VR 1 du 9 décembre 2010):

'(...) L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme le point (...) qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif (...) du fait de la défaillance de ces fonctions (...).

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral.

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local.'"

In advies 63.296/4, op 2 mei 2018 gegeven over een voorontwerp dat heeft geleid tot de wet van 7 april 2019 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid', heeft de afdeling Wetgeving immers het volgende opgemerkt:

"Het is niet voor het eerst dat de afdeling Wetgeving advies moet uitbrengen over een voorontwerp van wet dat, met toepassing van een om te zetten Europese richtlijn, aanbieders van essentiële diensten beoogt te inventariseren teneinde sommige van hun infrastructuur die noodzakelijk worden geacht voor het behoud van verschillende centrale functies voor het bestaan van de Natie, preventief te beschermen.

Die onderneming kan op zichzelf bevoegdheidsproblemen doen rijzen, wanneer de te beschermen infrastructuur afhangen van operatoren die hun activiteiten uitoefenen op gebieden waarvoor de deelstaten of sommige deelstaten bevoegd zijn gemaakt, en wanneer de federale wet die deelstaten eenzijdig wil betrekken bij de identificatie van de te beschermen infrastructuur, een identificatie die de federale Staat, wat hem betreft, doet krachtens de restbevoegdheden die hij op het gebied van de openbare veiligheid uitoefent.

Die bevoegdheidskwestie is als volgt geanalyseerd in advies 48.989/VR,¹ op 9 december 2010 gegeven over een voorontwerp dat heeft geleid tot de wet van 1 juli 2001 'betreffende de beveiliging en de bescherming van de kritieke infrastructuur':

'1. Het voorliggende voorontwerp voorziet, zoals te lezen staat in artikel 2, eerste lid, ervan, inzonderheid in de omzetting van richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren (hierna 'de richtlijn' genoemd).

Artikel 1 van de richtlijn geeft aan dat bij deze richtlijn een procedure wordt ingesteld voor de identificatie en de aanmerking van Europese kritieke infrastructuur, om de bescherming van de mensen te bevorderen. De kritieke infrastructuur wordt in artikel 2, a), van de richtlijn in wezen gedefinieerd als 'een voorziening (...), die van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de verstoring of vernietiging (...) aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken'. Artikel 3, lid 3, van de richtlijn bepaalt dat deze op dit ogenblik uitsluitend van toepassing is in de sectoren energie en vervoer. Volgens de eerste overweging van de richtlijn hebben de stellers ervan in de eerste plaats het aannemen van 'voorstellen (beoogd) over de wijze waarop de preventie van, de paraatheid bij en de reactie op terreuraanslagen op kritieke infrastructuur in Europa kunnen worden verbeterd'. In dat verband is besloten dat het Europese programma voor de bescherming van kritieke infrastructuur, waarvan de richtlijn een beleidsmiddel is, 'gebaseerd moet zijn op een alle risico's omvattende aanpak, waarbij de bestrijding van terroristische dreigingen als prioriteit zou gelden', een aanpak waarbij 'in het proces ter bescherming van kritieke infrastructuur rekening (dient) te worden gehouden met door mensen veroorzaakte dreigingen, technologische dreigingen en natuurrampen' (derde overweging).

Gelet op hetgeen voorafgaat, moet worden beschouwd dat de omzetting van deze richtlijn hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort.²

Hetzelfde geldt voor de overige bepalingen van het voorontwerp die weliswaar niet voorzien in de omzetting van de richtlijn, maar strekken tot het aannemen van analoge maatregelen met betrekking tot de nationale kritieke infrastructuur, de andere punten van federaal belang en de punten van lokaal belang.

¹ Voetnoot 1 van het geciteerde advies: Parl.St. Kamer 2010-11, nr. 1357/001, 53-64, <http://www.raadvst-consetat.be/dbx/adviezen/48989.pdf>.

² Voetnoot 2 van het geciteerde advies: Voetnoot 1 van het geciteerde advies: Raad van State, Belgische Staat, nr. 175.462, 8 oktober 2007. Andere voorbeelden van wetten die de federale Staat heeft aangenomen met het oog op de preventieve bescherming van de "vitale maatschappelijke functies": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, die onder meer de bescherming van het "economisch potentieel van het land" beoogt, of de wet van 10 juli 2006 betreffende de analyse van de dreiging, die onder meer 's lands "fundamentele belangen" beoogt.

2. De maatregelen die op basis van het voorontwerp zullen worden getroffen, kunnen evenwel een weerslag hebben op operatoren die een infrastructuur exploiteren welke, uit een ander oogpunt beschouwd, tot de bevoegdheid ratione materiae van de gewesten kan behoren, meer in het bijzonder wat betreft de sectoren energie en vervoer, waarop de richtlijn toepassing vindt (artikel 6, § 1, VII en X, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen).

De steller van het voorontwerp heeft overigens oog gehad voor dit aspect, daar hij de gewesten wenst te 'betrekken' bij het uitwerken van de toepasselijke regelgeving en bij de uitvoering ervan, zoals blijkt uit de volgende bepalingen van het voorontwerp:

– artikel 5, § 1, tweede lid, naar luid waarvan de sectorale overheid³ de Europese kritieke infrastructuren identificeert 'na eensluitend advies van de gewesten voor de potentiële kritieke infrastructuren die onder hun bevoegdheden vallen';

– artikel 6, § 2, naar luid waarvan de sectorale overheid 'de sectorale criteria (bepaalt) waaraan de Europese kritieke infrastructuren moeten beantwoorden, rekening houdend met de bijzondere karakteristieken van de betrokken sector, (...), in voorkomend geval, na eensluitend advies van de betrokken gewesten';

– artikel 6, § 5, naar luid waarvan de sectorale overheid 'geval per geval de drempelwaarden (bepaalt) die van toepassing zijn op de intersectorale criteria waaraan de Europese kritieke infrastructuren dienen te beantwoorden, (...), in voorkomend geval, na eensluitend advies van de betrokken gewesten';

– artikel 7, § 2, tweede lid, naar luid waarvan de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (hierna 'ADCC' genoemd) 'in samenwerking met (...), in voorkomend geval (...) de betrokken gewesten, belast (is) met het voeren van bilaterale of multilaterale besprekingen met de betrokken lidstaten van de Europese Unie, (...) inzake de potentiële Europese kritieke infrastructuren geïdentificeerd op Belgisch grondgebied (...)';

– artikel 13, § 6, tweede lid, naar luid waarvan 'de Koning bepaalt, in voorkomend geval, met instemming van de betrokken gewesten, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de bijwerkingen' van het beveiligingsplan van de exploitant van een Europese kritieke infrastructuur;

– artikel 24, § 2, tweede lid, naar luid waarvan de Koning 'de nadere regels van [de controle van de inachtneming van de bepalingen van de ontworpen wet door de exploitanten van de bij deze wet bedoelde infrastructuren] kan vastleggen, in voorkomend geval met instemming van de betrokken gewesten'.

3. Aangezien de gewesten bevoegdheden bezitten op het gebied van energie en vervoer, aangezien dit eveneens zou kunnen gelden voor andere sectoren waarop de ontworpen wet toepassing zou vinden en volgens de steller zelf van het voorontwerp bij de uitvoering van de wet de weerslag van sommige van de voorgenomen maatregelen voelbaar zou kunnen zijn in het beheer van infrastructuren die tot de bevoegdheid van de gewesten behoren, kan worden aanvaard dat de gewesten worden betrokken bij het aannemen van de uitvoeringsmaatregelen omschreven in de ontworpen tekst.

³ Voetnoot 3 van het geciteerde advies: Voetnoot 2 van het geciteerde advies: Voor de Europese kritieke infrastructuren is de federale minister bevoegd voor het Vervoer of diens gemachtigde (artikel 3, 3°, a), van het voorontwerp), dan wel de federale minister bevoegd voor de Energie of diens gemachtigde (artikel 3, 3°, b), van het voorontwerp) de sectorale overheid.

De steller van het voorontwerp moet evenwel aldus te werk gaan dat de autonomie van de verschillende beleidsniveaus in acht wordt genomen. De federale wetgever kan niet eenzijdig – bij wege van een gewone wet – een gedwongen medewerking van de gewesten aan het bij het voorontwerp uitgestippelde systeem opleggen. De medewerking van de gewesten kan dus indien nodig alleen facultatief zijn, en op een zodanige wijze dat, indien ze dat verzuimen, zulks niet verhindert dat de bevoegde federale overheid de voorgenomen maatregelen kan nemen.

4. Indien in de toekomst mocht blijken dat het aannemen van maatregelen ter uitvoering van de wet inhoudt dat bevoegdheden eigen aan de federale overheid en aan de gewesten gezamenlijk worden uitgeoefend, en niet meer dat uitsluitend de enkele federale bevoegdheid op het gebied van de openbare veiligheid wordt uitgeoefend, moet daaromtrent met de gewesten een samenwerkingsakkoord worden gesloten.”⁴

Deze opmerking geldt *mutatis mutandis* voor het voorliggende voorontwerp, in het kader waarvan de gewesten en/of de gemeenschappen bij de gang van zaken worden betrokken ingevolge de artikelen 3, § 3, 3°, 11, §§ 3 en 4, 15, § 2, derde lid, en 44, § 1, tweede lid, van het voorontwerp, telkens op een wijze die verenigbaar is met de hierboven naar voren gebrachte principes.

Voorts valt niet uit te sluiten dat de gemeenschappen en de gewesten, handelend binnen hun materiële bevoegdheden, zelf ook bepaalde categorieën veiligheidsbelangen kunnen beschermen die samenvallen met elementen die de basis vormen voor de beoordeling van de nationale veiligheid.⁵

Ten aanzien van die principes doet het voorontwerp dan ook geen enkel bevoegdheidsprobleem rijzen.

2. In aanvulling op de algemene regels inzake identificatie belast artikel 11 van het voorontwerp de nationale cyberbeveiligingsautoriteit ermee om in bepaalde omstandigheden een entiteit als een essentiële of belangrijke entiteit te identificeren.

Op de vraag waarom die opdracht aan de nationale cyberbeveiligingsautoriteit wordt toevertrouwd, heeft de gemachtigde van de eerste minister het volgende geantwoord:

“Les entités essentielles et importantes visées par la directive 2022/2555 (‘directive NIS2’) sont principalement celles répondant aux définitions reprises aux annexes I ou II de la directive NIS2 et, sauf exception, à la taille (équivalente à une entreprise moyenne ou large au sens de l’annexe de la recommandation 2003/361/CE). Il n’y a pas d’identification nécessaire pour ces entités (celles-ci auront au contraire l’obligation de s’enregistrer voir l’art. 13 de l’APL).

Toutefois, les articles 2 (2) b)-e) et 3 (1) e) & (2) de la directive imposent le maintien d’un processus d’identification au niveau national pour certaines entités essentielles ou importantes complémentaires.

⁴ Parl.St. Kamer 2018-19, nr. 54-3340/001, 75-87.

⁵ Zie in die zin advies 67.887/1 van 28 september 2020 over een voorontwerp van wet ‘tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen’, opmerking 3.1.

Conformément à l'article 11 de l'APL, le choix a été fait de confier à l'autorité nationale de cybersécurité (le projet d'arrêté royal approuvé par le Conseil des Ministres prévoit la désignation du Centre pour la Cybersécurité Belgique – 'CCB' pour assurer ce rôle) le soin de coordonner le processus d'identification complémentaire et de prendre la décision formelle d'identification, après différentes consultations préalables (l'entité concernée, les éventuelles entités fédérées concernées, les autorités sectorielles concernées ou encore le Comité stratégique du renseignement et de la sécurité).

Il s'agit d'assurer une cohérence avec les autres missions légales confiées à l'autorité nationale de cybersécurité par l'APL (voir l'art. 16 et s. de l'APL): mission de coordination de la loi, mission de supervision (service d'inspection et de sanction), mission de CSIRT national (gestion des incidents), mission de représentation au niveau européen, etc.

S'agissant d'un acte administratif motivé d'une autorité administrative (CCB), l'identification formelle pourra être contestée devant la section du contentieux administratif du Conseil d'État. Ce faisant, les garanties prévues par les lois coordonnées sur le Conseil d'État et la loi sur la motivation formelle des actes administratifs s'appliqueront."

Niettemin, doordat de wetgevende macht rechtstreeks diensten van de uitvoerende macht aanwijst om opdrachten in verband met de uitvoering van het voorontwerp uit te voeren en om formele beslissingen inzake identificatie te nemen, mengt ze zich in de interne organisatie van de uitvoerende macht. In principe staat het aan de Koning te bepalen welke van zijn diensten een rol dienen te spelen bij de identificatieprocedure die voortvloeit uit de tenuitvoerlegging van de wet.

Zo staat het aan de Koning de lijst van de essentiële en belangrijke entiteiten waarop de wet met toepassing van de NIS 2-richtlijn van toepassing is, aan te vullen, of die bevoegdheid te delegeren aan een dienst die onder zijn gezag ressorteert.

3. In het ontworpen dispositief wordt verwezen naar wetteksten die zich nog in de ontwerpfase bevinden.

Zo bevatten de definities in de punten 43°, 45° en 49° van artikel 8 een dubbele verwijzing, enerzijds naar bestaande teksten en anderzijds naar ontwerpen van wetteksten, namelijk respectievelijk de CER-wet en de NCCN-wet. De definitie in punt 44° verwijst eveneens naar een ontwerp van wettekst, namelijk de NPU-wet. Voorts bevatten verschillende bepalingen van het voorontwerp verwijzingen naar de CER-wet, de NCCN-wet en de NPU-wet.

In dat verband heeft de gemachtigde van de eerste minister de volgende informatie verstrekt:

"Sur base des dernières informations reçues de nos collègues du Centre de crise national (NCCN), il s'avère l'avant-projet de loi relatif à la planification d'urgence et à la gestion de crise (loi NPU) devrait être soumise prochainement au Conseil des Ministres. Pour les autres avant-projets de lois, il semble toutefois que ceux-ci ne seront, en définitive, pas adoptés avant la présente loi.

Ces références ont été volontairement accompagnées ou mentionnées entre crochets dans le dispositif du présent avant-projet de loi pour être adaptées en fonction des derniers développements de ces autres avant-projets.

Il faudra dès lors vraisemblablement remplacer les mentions ‘loi CER’ par la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques et les mentions ‘loi NCCN’ par l’arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise.”

Met zo’n werkwijze is het voor de afdeling Wetgeving niet mogelijk de draagwijdte en de inhoud van sommige bepalingen nauwkeurig genoeg te bepalen. Dat is bijvoorbeeld het geval met artikel 29 van het voorontwerp, dat betrekking heeft op het nationale plan voor crisisrespons en grootschalige cyberbeveiligingsincidenten en dat verwijst naar de NPU-wet waarvan het voorontwerp nog niet aan de Ministerraad is voorgelegd, alsook met artikel 68, 5°, van het voorontwerp, waarin wordt bepaald dat voor het doeleinde bedoeld in artikel 67, 5°, van het voorontwerp “de identificatiegegevens [worden verwerkt] van de personen die betrokken zijn bij de samenwerking in het kader van de CER-wet”.

Het dispositief moet worden herzien zodat het verwijst naar de relevante bepalingen, namelijk die welke van kracht zullen zijn op het ogenblik dat de ontworpen wet wordt bekendgemaakt en zelf in werking treedt. Voorts moet de steller van het voorontwerp voor samenhang zorgen tussen het voorontwerp en de wetteksten waarnaar het verwijst.

Gezien die onduidelijkheden kan het feit dat in dit advies geen opmerking wordt gemaakt over een of ander aspect van het voorontwerp, vanzelfsprekend niet zo worden geïnterpreteerd dat die aspecten geen enkel juridisch probleem zouden doen rijzen wat betreft de correcte omzetting van de NIS 2-richtlijn en de overeenstemming van het voorliggende dispositief met de relevante hogere rechtsnormen.

BIJZONDERE OPMERKINGEN

Artikel 11

1. In plaats van in paragraaf 3, tweede lid, te bepalen dat “het advies geacht [wordt] gunstig te zijn” indien de in het eerste lid bedoelde entiteit geen advies heeft uitgebracht binnen de daar bedoelde termijn, dient men te schrijven dat wanneer binnen de in het eerste lid bedoelde termijn geen advies is uitgebracht, kan worden voorbijgegaan aan het feit dat geen advies is gegeven.

2. Paragraaf 5 luidt als volgt:

“In de gevallen bedoeld in paragraaf 1 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die geen deel uitmaakt van de in de bijlage bedoelde sectoren, aanwijzen als een essentiële of belangrijke entiteit.”

In de toelichting bij het artikel staat het volgende te lezen:

“Op grond van paragraaf 5 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die niet tot de in de bijlage bij de wet bedoelde sectoren behoort, individueel aanwijzen als een essentiële of belangrijke entiteit. Een entiteit of een bepaalde onderaannemer van een NIS-entiteit kan immers een kritieke dienst verlenen die rechtvaardigt dat zij of hij onderworpen is aan de bepalingen van de wet, ook al behoren haar of zijn activiteiten niet tot een van de sectoren opgenomen in de bijlagen bij de wet. De toepassing van dit artikel is beperkt tot bijzondere gevallen en houdt in dat, vóór de beslissing van het Strategisch Comité voor Inlichtingen en Veiligheid, overleg wordt gepleegd tussen de betrokken entiteit, de nationale cyberbeveiligingsautoriteit, de deelgebieden en de eventuele sectorale overheid.”

Daaruit vloeit voort dat voorafgaand aan de beslissing van het Strategisch Comité voor Inlichtingen en Veiligheid “overleg [moet worden] gepleegd tussen de betrokken entiteit, de nationale cyberbeveiligingsautoriteit, de deelgebieden en de eventuele sectorale overheid”.

De bepaling moet worden herzien zodat ze de aan de Koning verleende machtiging procedureel omkadert.

Artikel 21

Paragraaf 2, tweede lid, luidt als volgt:

“De doeleinden van voornoemde taken zijn:

1° onverminderd de bevoegdheden van de personen die de gerechtelijke politie uitoefenen, met name de procureurs des Konings, de federale procureur of de procureurs-generaal, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronisch communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;

2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

3° het onderzoeken van beveiligingsproblemen bij elektronische communicatienetwerken of -diensten of informatiesystemen.”

Het is de afdeling Wetgeving evenwel niet duidelijk waarom de “bevoegdheden van de personen die de gerechtelijke politie uitoefenen” enkel worden gememoreerd in het geval dat in punt 1° wordt bedoeld.

Op die vraag heeft de gemachtigde van de eerste minister het volgende geantwoord:

“L'ajout à l'article 21, § 2, alinéa 1er ('sans préjudice des compétences des personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction') a été inséré au cours des discussions des textes afin de confirmer ce qui était une évidence : les missions de l'autorité nationale de cybersécurité (CCB) s'exercent sans préjudice des missions légales dévolues personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction.

Le cas échéant, cette mention pourrait accompagner l'ensemble de l'article 21 (lequel a pour vocation initiale d'habiliter l'autorité nationale de cybersécurité à accomplir certaines tâches.”

De precisering in verband met de bevoegdheden van de personen die de gerechtelijke politie uitoefenen, dient dan ook te worden opgenomen in de inleidende zin van het voorliggende artikel.

Artikel 23

In de toelichting bij de bepaling wordt het volgende gesteld:

“Ook moeten alle door ethische hackers verzamelde gegevens binnen een redelijke termijn na de melding worden verwijderd. Indien het noodzakelijk is om deze gegevens nog enige tijd te bewaren of indien er een gerechtelijke procedure loopt, moeten ethische hackers ervoor zorgen dat deze gegevens in deze periode veilig worden bewaard.”

Het dispositief moet worden aangevuld zodat het melding maakt van de regeling inzake het verwijderen van de verzamelde gegevens, die ter sprake komt in de toelichting bij het artikel.

Artikel 26

In paragraaf 1 wordt gesteld dat de bepaling niet raakt aan de toepassing van de wet van 11 december 1998 ‘betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst’.

Dat het voorontwerp geen afbreuk doet aan de wet van 11 december 1998, blijkt echter al uit artikel 5, § 2.

Men dient het dispositief opnieuw te onderzoeken en in voorkomend geval te herzien, om te zorgen voor samenhang tussen de artikelen 5 en 26 en om overbodige bepalingen te vermijden.

Artikel 29

Gelet op artikel 9, lid 4, van de NIS 2-richtlijn dat bij artikel 29 wordt omgezet, en naar het voorbeeld van hetgeen wordt vermeld in het opschrift van het ontworpen hoofdstuk 5 van titel 2, dient men in paragraaf 1, eerste zin, en in de inleidende zin van paragraaf 2 het woord “grootschalige” in te voegen tussen de woorden “plan voor” en “cyberbeveiligingsincidenten”.

Artikel 30

Paragraaf 1 strekt ertoe artikel 21, lid 1, eerste alinea, van de NIS 2-richtlijn om te zetten.

Die laatstgenoemde bepaling stelt het volgende: “De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico’s voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken”. Paragraaf 1 maakt evenwel alleen melding van “passende en evenredige maatregelen”, zonder nader te stellen dat het gaat om “technische, operationele en organisatorische maatregelen” zoals bedoeld in de richtlijn.

Men dient de bepaling opnieuw te onderzoeken en in voorkomend geval te herzien, om te zorgen voor de volledige omzetting van de NIS 2-richtlijn.

Artikel 44

De inhoud van het tweede lid van paragraaf 1 staat reeds in artikel 39, tweede lid, van het voorontwerp.

Men dient het dispositief opnieuw te onderzoeken en in voorkomend geval te herzien, om te zorgen voor samenhang tussen de artikelen 39 en 44 en om overbodige bepalingen te vermijden.

Artikel 59

1. De gemachtigde van de eerste minister is het ermee eens dat de woorden “in artikel 11, § 5,” in het eerste lid, 1°, moeten worden vervangen door de woorden “in artikel 12”.

2. Volgens het eerste lid, 3°, wordt “eenieder die niet voldoet aan de in deze titel bedoelde toezichtverplichtingen (...) bestraft met een geldboete van 500 tot 200 000 euro”. Titel 4, waarnaar het dispositief verwijst, omvat een groot aantal verplichtingen.

De afdeling Wetgeving heeft er al herhaaldelijk aan herinnerd dat “[h]et recht om zichzelf niet te beschuldigen, dat gewaarborgd is door artikel 6 van het Europees Verdrag voor de rechten van de mens, (...) er evenwel aan in de weg [staat] dat een persoon, ‘tegen wie een vervolging is ingesteld’, in de zin van deze bepaling, kan worden bestraft omdat hij geweigerd heeft zijn medewerking te verlenen bij het bewijzen van zijn eigen schuld”.⁶

⁶ Advies 60.619/2 van 25 januari 2017 over een voorontwerp dat heeft geleid tot de wet van 2 oktober 2017 ‘tot regeling van de private en bijzondere veiligheid’, *Parl.St.* Kamer 2016-17, nr. 54-2388/001, 194. Zie ook advies 63.296/4; advies 64.879/4 van 4 februari 2019 over een voorontwerp dat heeft geleid tot het decreet van 2 mei 2019 ‘tot wijziging van het Waalse Wetboek van Sociale Actie en Gezondheid wat betreft de preventie en de bevordering van de gezondheid’, *Parl.St.* W.Parl 2018-19, nr. 1332/1, 25-35; en advies 70.306/2 van 23 november 2021 over een voorontwerp dat heeft geleid tot de wet van 23 februari 2022 ‘tot tenuitvoerlegging van verordening (EU) 2020/1503 van het europees parlement en de raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van verordening (EU) 2017/1129 en richtlijn (EU) 2019/1937, en tot omzetting van richtlijn (EU) 2021/338 van het europees parlement en de raad van 16 februari 2021 tot wijziging van richtlijn 2014/65/EU wat betreft informatievereisten, productgovernance en positielimieten, en richtlijnen 2013/36/EU en (EU) 2019/878 wat betreft de toepassing daarvan op

Artikel 48, § 4, eerste lid, 3°, van het voorontwerp bepaalt dat de persoon die door de inspectiedienst wordt verhoord, het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Het eerste lid, 3°, moet dus geacht worden van toepassing te zijn onverminderd artikel 48, § 4, eerste lid, 3°, van het voorontwerp.

Om elke misvatting in dat verband te vermijden, verdient het derhalve aanbeveling aan het begin van de bepaling de woorden “Onverminderd artikel 48, § 4, eerste lid, 3°,” toe te voegen.

Artikel 65

De gemachtigde van de eerste minister is het ermee eens dat de woorden “bedoeld in het eerste lid” dienen te worden vervangen door de woorden “bedoeld in artikel 64”.

Artikel 79

In de bepaling onder 1° dienen de woorden “de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 47°,” te worden vervangen door de woorden “de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 46°,”.

Dezelfde opmerking geldt voor de bepaling onder 2°.

Artikel 83

1. In de bepalingen onder 2° en 3° dienen de woorden “in de zin van artikel 8, 24°, van diezelfde wet” te worden ingevoegd na de woorden “verleners van vertrouwensdiensten”.

2. In de bepaling onder 3° dienen de woorden “als sectorale overheid en sectorale inspectiedienst voor” te worden vervangen door de woorden “als sectorale overheid in de zin van artikel 8, 55°, van diezelfde wet en sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van diezelfde wet, voor”.

Artikel 85

In het ontworpen artikel 2, 94° (artikel 85, 5°, van het voorontwerp) dienen de woorden “zoals bedoeld in de wet” te worden vervangen door de woorden “in de zin van artikel 8, 24°, van de wet”.

Artikel 87

In het ontworpen artikel 107/4, § 6, dienen de woorden “in hoofdstuk 2 van de NIS 2-wet” te worden vervangen door de woorden “in titel 4, hoofdstuk 2, van de wet van [XX XX XXXX] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.

Bijlagen

Overeenkomstig de bijlagen I en II van de NIS 2-richtlijn dient het volledige opschrift van de richtlijnen en verordeningen die daarin worden vermeld, in de tabellen te worden ingevoegd.

SLOTOPMERKINGEN

1. De concordantietabellen, in voorkomend geval gelezen in samenhang met de memorie van toelichting en de artikelsgewijze toelichting, moeten het onder meer mogelijk maken na te gaan in welke mate de NIS 2-richtlijn correct is omgezet.

Voor verschillende bepalingen van het voorontwerp blijken de tabellen die aan de afdeling Wetgeving zijn overgezonden, echter niet te beantwoorden aan de nauwkeurigheidsvereisten waaraan ze moeten voldoen.

2. In de tabellen vormen de artikelen 84 en 87 van het voorontwerp aldus geen nationale bepalingen die geen uitstaans hebben met de omzetting van de NIS 2-richtlijn, maar zijn ze integendeel wetsbepalingen tot omzetting van die richtlijn.

3. Voorts dient in de eerste tabel te worden aangegeven:

– dat artikel 3, § 1, tweede lid, van het voorontwerp artikel 2, lid 1, tweede alinea, van de richtlijn omzet;

– dat artikel 4, § 4, van het voorontwerp artikel 26, lid 2, van de richtlijn omzet;

– dat artikel 5, § 5, van het voorontwerp artikel 2, lid 8, van de richtlijn omzet;

– dat artikel 20, 1°, van het voorontwerp artikel 10, lid 3, van de richtlijn omzet;

– dat artikel 37, § 2, van het voorontwerp artikel 23, lid 7, van de richtlijn omzet;

– dat artikel 37, § 3, van het voorontwerp artikel 23, lid 8, van de richtlijn omzet;

– dat artikel 37, § 4, van het voorontwerp artikel 23, lid 9, van de richtlijn omzet;

– dat artikel 37, § 5, van het voorontwerp artikel 23, lid 10, van de richtlijn omzet;

– dat artikel 46, §§ 2 en 3, van het voorontwerp artikel 37, lid 1, van de richtlijn omzet;

– dat artikel 48, § 7, tweede lid, van het voorontwerp artikel 35, lid 3, van de richtlijn omzet.

4. Volgens de beginselen van de wetgevingstechniek die de afdeling Wetgeving heeft opgesteld, wordt de stellers van voorontwerpen verzocht om bij de omzetting van richtlijnen omzettingstabellen op te maken:

“191. Maak twee omzettingstabellen op.

191.1. Om te controleren of een richtlijn correct en volledig wordt omgezet, maak een concordantietabel op met de (onderdelen van de) artikelen van de richtlijn en van de er mee overeenstemmende (onderdelen van de) artikelen van de door u opgestelde tekst die in de omzetting voorziet. Vermeld eveneens in deze tabel:

a) de artikelen van de richtlijn die eventueel reeds zijn omgezet, alsmede de overeenstemmende teksten van intern recht en de artikelen waarbij de richtlijn is omgezet;

b) de artikelen van de richtlijn die door een andere instantie nog moeten worden omgezet.

191.2. Om ieder artikel van de tekst die in de omzetting voorziet te kunnen lezen in het licht van de vereisten van de richtlijn, maak eveneens een concordantietabel op met de (onderdelen van de) artikelen van de tekst die in de omzetting voorziet en de (onderdelen van de) artikelen van de richtlijn.”⁷

Er dient derhalve in een tabel te worden voorzien die opgeeft welke (onderdelen van de) artikelen van de richtlijn nog moeten worden omgezet door een andere instantie.

LE GREFFIER – DE GRIFFIER

LE PRÉSIDENT – DE VOORZITTER

Charles-Henri VAN HOVE

Bernard BLERO

⁷ *Beginnelsen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbevelingen 191 tot 191.2.