DOC 55 **3862/004**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

18 avril 2024

PROJET DE LOI

établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Amendement

déposé en séance plénière

Voir:

Doc 55 **3862/ (2023/2024)**:
001: Projet de loi.
002: Rapport.
003: Texte adopté par la commission.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

18 april 2024

WETSONTWERP

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

Amendement

ingediend in de plenaire vergadering

Zie:

Doc 55 **3862/ (2023/2024)**:
001: Wetsontwerp.
002: Verslag.
003: Tekst aangenomen door de commissie.

N° 1 de M. **Freilich**

Art. 98

Compléter cet article par un alinéa rédigé comme suit:

"Par dérogation à l'alinéa 1er, la présente loi entre en vigueur à l'égard des entités de l'administration publique qui dépendent des entités fédérées à la date d'entrée en vigueur de l'accord de coopération réglant la coopération entre les différentes administrations publiques.".

JUSTIFICATION

L'avis n° 74.861/4 rendu par le Conseil d'État à propos de ce projet de loi renvoie au raisonnement suivi par la section de législation du Conseil d'État dans son avis sur l'avant-projet de loi visant à transposer la directive NIS1 (n° 62.296/4 du 2 mai 2018). Dans cet avis du 2 mai 2018, la section de législation reconnaît que la transposition de cette directive pourrait "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 reconnaît aussi la compétence de principe du législateur fédéral pour transposer la directive concernée dans le droit national. À l'époque, la section de législation du Conseil d'État avait principalement fondé son analyse des règles répartitrices de compétence sur l'avis n° 48.989/VR du 9 décembre 2010 rendu précédemment au sujet de la loi transposant la directive ICE (qui a précédé la directive CER), à savoir la loi relative aux infrastructures critiques, qui, selon la section de législation précitée, "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.".

En ce qui concerne la transposition de la directive NIS1, la section de législation a constaté de manière similaire que la loi de transposition associe de la même manière les Régions et/ou les Communautés "au processus opératoire", "l'avant-projet ne [soulevant] dès lors aucun problème de compétence […]". Dans le même temps, le Conseil d'État a souligné que "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

Nr. 1 van de heer **Freilich**

Art. 98

Dit artikel aanvullen met een lid, luidende:

"In afwijking van het eerste lid, treedt deze wet ten aanzien van de overheidsinstanties die van de deelgebieden afhangen, in werking op de datum van inwerkingtreding van het samenwerkingsakkoord dat de samenwerking tussen de overheden regelt."

VERANTWOORDING

Het advies van de Raad van State 74.861/4 over dit wetsontwerp verwijst naar de analyse die werd gehanteerd door de afdeling Wetgeving van de Raad van State in het advies over het voorontwerp van de omzettingswet van de NIS1-richtlijn (nr. 62.296/4 van 2 mei 2018). De afdeling Wetgeving erkent in dat advies van 2 mei 2018 dat de omzetting van deze richtlijn "bevoegdheidsproblemen [kan] doen rijzen, wanneer de te beschermen infrastructuren afhangen van operatoren die hun activiteiten uitoefenen op gebieden waarvoor de deelstaten of sommige deelstaten bevoegd zijn gemaakt", en erkent de principiële bevoegdheid van de federale wetgever om de betrokken richtlijn om te zetten in het nationale recht. De afdeling Wetgeving van de Raad van State steunde destijds haar bevoegdheidsrechtelijke analyse hoofdzakelijk op een eerder advies nr. 48.989/VR van 9 december 2010) over de omzettingswet van de ECI-richtlijn (i.e. de voorloper van de CER-richtlijn), namelijk de zogenaamde "Wet Kritieke Infrastructuren" die, volgens de afdeling Wetgeving van de Raad van State, "hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort".

Wat de omzetting van de NIS1-richtlijn betreft, stelde de afdeling Wetgeving in gelijkaardige zin vast dat de omzettingswet op gelijkaardige wijze de gewesten en/of de gemeenschappen "bij de gang van zaken betrok", waardoor "het voorontwerp dan ook geen enkel bevoegdheidsprobleem (doet) rijzen". Tegelijkertijd stelde de Raad van State dat "indien in de toekomst zou blijken dat het nemen van maatregelen ter uitvoering van de wet de gezamenlijke uitoefening van specifieke bevoegdheden van de federale overheid en de gewesten zou impliceren, en niet langer uitsluitend de uitvoering van

seule compétence fédérale en matière de sécurité publique, il conviendrait de conclure un accord de coopération avec les régions sur ces questions.". Le Conseil d'État indique dans l'avis qu'il a rendu récemment que cette observation vaut *mutatis mutandis* pour le projet de loi à l'examen.

Le récent avis du Conseil d'État 74.861/4 n'évoque pas le fait que la NIS2 vise désormais également les entités de l'administration publique au niveau régional (et pas seulement certains secteurs tels que ceux de l'énergie et des transports).

Conformément à l'article 87 de la LSRI, les Communautés et les Régions sont compétentes pour instaurer et réglementer leurs propres administrations et services. Lue en combinaison avec l'article 9 de la LSRI, qui prévoit que, dans les matières qui relèvent de leurs compétences, les Communautés et les Régions peuvent créer des services et des institutions décentralisés, cette disposition les habilite à prendre des mesures relatives à l'organisation de l'autorité flamande.

En outre, conformément aux principes d'autonomie et de verticalité, toute autorité est compétente pour régler le fonctionnement (interne) de ses propres services publics. Cette compétence pourrait inclure l'adoption de mesures visant à améliorer la cybersécurité des autorités publiques au niveau régional.

L'on peut donc conclure de manière convaincante que les Communautés et les Régions sont compétentes en matière de cybersécurité pour les services et les institutions qui dépendent des entités fédérées respectives.

Dans cette optique, il est permis de conclure que le principe d'autonomie semble s'opposer à ce qu'une administration publique régionale (telle que l'autorité flamande) se voie imposer des mesures de (cyber)sécurité par une autorité de contrôle du niveau fédéral, sur la base d'une loi fédérale transposant la directive NIS2. Le contraire signifierait en effet que l'autorité fédérale de contrôle aurait été chargée par le législateur fédéral de tâches de contrôle concernant des matières qui ne relèvent pas de la compétence de l'autorité fédérale. Or, il n'appartient pas au législateur fédéral de s'immiscer dans les matières relevant de la compétence exclusive des Communautés ou des Régions, et encore moins de contrôler les administrations publiques régionales. La coopération des Communautés et des Régions peut tout au plus être facultative sur ce point.

de federale bevoegdheid inzake openbare veiligheid, zou het aangewezen zijn om met de gewesten een samenwerkingsakkoord over deze aangelegenheden te sluiten". De Raad van State stelt in het recente advies dat deze opmerking geldt *mutatis mutandis* voor het voorliggende voorontwerp van wet.

In het recente advies van de Raad van State 74.861/4 wordt niet dieper ingegaan op het feit dat NIS2 nu ook de overheidsinstanties op regionaal niveau viseert (en niet alleen sectoren zoals energie en vervoer).

Overeenkomstig artikel 87 BWHI zijn de gemeenschappen en de gewesten bevoegd om een eigen administratie en eigen diensten op te richten en te regelen. In samenhang gelezen met artikel 9 BWHI, dat bepaalt dat de gemeenschappen en gewesten gedecentraliseerde diensten en instellingen kunnen oprichten in de aangelegenheden die tot hun bevoegdheid behoren, omvat dat de bevoegdheid om maatregelen te nemen die verband houden met de organisatie van de Vlaamse overheid.

Bovendien is overeenkomstig het autonomiebeginsel en het verticaliteitsbeginsel elke overheid bevoegd om de (interne) werking van haar eigen overheidsdiensten te regelen. De bevoegdheid om maatregelen te nemen die de cyberveiligheid van de overheidsinstanties op regionaal niveau verbeteren, kan daaronder worden gebracht.

Er kan daarom op overtuigende wijze geconcludeerd worden dat de gemeenschappen en de gewesten bevoegd zijn om cyberveiligheidsmaatregelen te nemen ten aanzien van de diensten en instellingen die afhangen van de respectievelijke deelstatelijke overheid.

In dat opzicht kan worden besloten dat het autonomiebeginsel eraan in de weg staat dat aan de overheidsinstanties op regionaal niveau (zoals de Vlaamse overheid) op grond van een federale omzettingswet van de NIS2-richtlijn (cyber) veiligheidsmaatregelen worden opgelegd door een federale toezichthoudende autoriteit. Hier anders over oordelen, zou immers betekenen dat de federale toezichthoudende autoriteit door de federale wetgever zou zijn belast met toezichtstaken buiten het kader van de aangelegenheden die tot de bevoegdheid van de federale overheid behoren. Het komt echter niet aan de federale wetgever toe om zich in te mengen in aangelegenheden waarvoor de gemeenschappen of gewesten exclusief bevoegd zijn, laat staan om toezicht uit te oefenen op overheidsinstanties op regionaal niveau. De medewerking van de gemeenschappen en de gewesten kan op dit punt hoogstens facultatief zijn.

Cet élément est donc certainement l'un des aspects les plus importants qu'il convient de règlementer dans le cadre d'un accord de coopération.

Outre l'article 13.1 de la directive NIS2 prévoyant qu'une coopération est nécessaire, la complexité de la directive exige également que la transposition de la directive NIS2 soit effectuée de manière coordonnée. Cette transposition nécessitera donc une concertation afin de parvenir à une harmonisation réciproque des politiques.

La conclusion d'un accord de coopération, en application de l'article 92*bis*, § 1er, de la LSRI, est préférable dans ce contexte, afin d'assurer la cohérence de la transposition de la directive en droit interne.

Dans certains cas, la conclusion d'un tel accord de coopération sera même obligatoire.

Compte tenu de ce qui précède, il convient de conclure un accord de coopération sur les dimensions de la directive NIS2 qui portent sur:

1° l'éventuel élargissement du champ d'application aux entités de l'administration publique au niveau local et aux établissements d'enseignement (article 2.5);

2° l'établissement d'une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine (articles 3.3 et 3.4);

3° les obligations d'information à la Commission et au groupe de coopération (article 3.5);

4° l'adoption d'une stratégie nationale en vue de sécuriser les réseaux et systèmes d'information (article 7);

5° la désignation des autorités compétentes chargées de la cybersécurité et des tâches de supervision et d'un point de contact unique (article 8);

6° la désignation des autorités de gestion des crises et du coordinateur (article 9);

7° la désignation des CSIRT (Centres de réponse aux incidents de sécurité informatique) et du coordinateur (article 10);

8° la désignation du coordinateur chargé de la divulgation coordonnée des vulnérabilités (article 12);

Vandaar dat dit zeker een van de belangrijkste aspecten is die een regeling in een samenwerkingsakkoord vergt.

Nog los van artikel 13.1 van de NIS2-richtlijn dat bepaalt dat er moet worden samengewerkt, vereist ook de complexiteit van de richtlijn dat de omzetting van de NIS2-richtlijn op een gecoördineerde wijze verloopt. De omzetting van de NIS2-richtlijn zal dus alleszins vereisen dat onderling overleg wordt gepleegd om tot een wederzijdse beleidsafstemming te komen.

Het sluiten van een samenwerkingsakkoord, met toepassing van artikel 92*bis*, § 1, BWHI, is in dat verband verkieslijk, met het oog op de coherentie van de omzetting van de richtlijn in het interne recht.

In bepaalde gevallen zal het sluiten van zo een samenwerkingsakkoord zelfs vereist zijn.

Rekening houdend met wat voorafgaat, moet een samenwerkingsakkoord worden gesloten over de aspecten van de NIS2-richtlijn die verband houden met:

1° de eventuele uitbreiding van het toepassingsgebied naar overheidsinstanties op lokaal niveau en onderwijsinstellingen (artikel 2.5);

2° het vaststellen van een lijst van essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen (artikel 3.3 en 3.4);

3° rapporteringsverplichtingen aan de Commissie en de samenwerkingsgroep (artikel 3.5);

4° het vaststellen van een nationale strategie voor de beveiliging van netwerk- en informatiesystemen (artikel 7);

5° het aanwijzen van de bevoegde autoriteiten voor cyberbeveiliging en voor toezichthoudende taken en een centraal contactpunt (artikel 8);

6° het aanwijzen van crisisbeheerautoriteiten en een coordinator (artikel 9);

7° het aanwijzen van CSIRT's (Computer Security Incident Response Teams) en een coördinator (artikel 10);

8° het aanwijzen van een coördinator voor de gecoördineerde bekendmaking van kwetsbaarheden (artikel 12);

9° la mise en place d'une coopération au niveau national (article 13);

10° la représentation au sein du groupe de coopération (article 14), le réseau des CSIRT (article 15), le EU-CyCLONE (article 16) et la participation aux évaluations par les pairs (article 19);

11° la supervision et l'exécution (article 31 et suivants).

De par leur nature, les mesures précitées ne peuvent être prises que conjointement par toutes les autorités visées.

Ce principe est d'autant plus vrai que, dans son avis exposé ci-avant, la section de législation du Conseil d'État a répété que "si (…) il devait s'avérer que l'adoption des mesures (…) 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".

Or, comme il ressort de ce qui précède, les Communautés et les Régions détiennent des compétences pertinentes en ce qui concerne la transposition de la directive NIS2, si bien que la directive NIS2 ne règle pas uniquement "la seule compétence fédérale en matière de sécurité publique". Dans cette hypothèse, la section de législation du Conseil d'État reconnaît que seul un accord de coopération pourra apporter une solution.

Les dispositions relatives aux mesures de gestion des risques en matière de cybersécurité et des obligations d'information pour les entités essentielles et importantes (chapitre IV) peuvent en revanche, en fonction du secteur dont l'entité relève, être transposées en toute autonomie par l'autorité fédérale, les Communautés ou les Régions au travers de l'adoption d'une législation parallèle. En vue d'assurer la clarté et la cohérence de la réglementation en droit interne, il serait toutefois indiqué que les parties concernées concluent également un accord de coopération à ce sujet. Cet accord permettrait également, par exemple, d'établir certaines exigences communes en matière de sécurité et de notification pour tous les fournisseurs de services essentiels, quel que soit le secteur dont ils relèvent.

En résumé, dès lors que le contrôle fédéral du fonctionnement des autorités publiques des entités fédérées viole le principe de l'autonomie des entités fédérées, la loi ne pourra produire ses effets à l'égard de ces autorités publiques

9° het regelen van de samenwerking op nationaal niveau (artikel 13);

10° de vertegenwoordiging in de samenwerkingsgroep (artikel 14), het CSIRT-netwerk (artikel 15), het EU-CyCLONE (artikel 16) en de deelname aan collegiale toetsingen (artikel 19);

11° toezicht en handhaving (artikel 31 e.v.).

De bovenstaande maatregelen kunnen uit hun aard slechts door alle betrokken overheden gezamenlijk worden genomen.

Dat geldt des te meer omdat de afdeling Wetgeving van de Raad van State in haar advies zoals hierboven reeds uiteengezet, heeft herhaald dat "indien (…) mocht blijken dat het aannemen van maatregelen (…) inhoudt dat de 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".

Welnu, zoals hierboven aangetoond, beschikken de gemeenschappen en de gewesten over relevante bevoegdheden voor de omzetting van de NIS2-richtlijn en kan worden geconcludeerd dat de NIS2-richtlijn méér regelt dan "uitsluitend de enkele federale bevoegdheid op het gebied van de openbare veiligheid". In deze hypothese erkent de afdeling Wetgeving van de Raad van State dat enkel een samenwerkingsakkoord soelaas zal kunnen bieden.

De bepalingen die verband houden met de risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging voor essentiële en belangrijke entiteiten (hoofdstuk IV) kunnen daarentegen, afhankelijk van de sector waartoe de entiteit behoort, autonoom worden omgezet door de federale overheid, c.q. de gemeenschappen of de gewesten. Zij kunnen dit doen door het aannemen van parallelle wetgeving. Met het oog op de duidelijkheid en de coherentie van de regeling in het interne recht zou het niettemin aangewezen zijn om ook hierover een samenwerkingsakkoord tussen de betrokken partijen te sluiten. Dit zou bijvoorbeeld ook toelaten om bepaalde gemeenschappelijke beveiligings- en meldingseisen vast te stellen voor alle aanbieders van essentiële diensten, ongeacht de sector waartoe zij behoren.

Kort samengevat, omdat federaal toezicht op de werking van de overheidsinstanties van de deelgebieden het principe van de autonomie van de deelgebieden schendt, kan de wet ten aanzien van die overheidsinstanties pas uitwerking

qu'après que les parties se sont entendues à ce sujet par le biais d'un accord de coopération législatif.

hebben nadat daarover afspraken via een wetgevend samenwerkingsakkoord zijn gemaakt.

Michael Freilich (N-VA)

Imprimerie centrale – Centrale drukkerij