DOC 55 **2693/002**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

17 juin 2022

PROJET DE LOI

relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité

RAPPORT DE LA PREMIÈRE LECTURE

FAIT AU NOM DE LA COMMISSION
DE L'ÉCONOMIE,
DE LA PROTECTION DES CONSOMMATEURS
ET DE L'AGENDA NUMÉRIQUE
PAR
MME **Leslie LEONI**

SOMMAIRE Pages

Voir:

Doc 55 **2693/ (2021/2022)**:
001: Projet de loi.
Voir aussi:
003: Articles adoptés en première lecture.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

17 juni 2022

WETSONTWERP

inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

VERSLAG VAN DE EERSTE LEZING

NAMENS DE COMMISSIE
VOOR ECONOMIE,
CONSUMENTENBESCHERMING
EN DIGITALE AGENDA
UITGEBRACHT DOOR
MEVROUW **Leslie LEONI**

INHOUD Blz.

Zie:

Doc 55 **2693/ (2021/2022)**:
001: Wetsontwerp.
Zie ook:
003: Artikelen aangenomen in eerste lezing.

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de sa réunion du 1er juin 2022.

I. — **EXPOSE INTRODUCTIF**

M. Pierre-Yves Dermagne, vice-premier ministre et ministre de l'Économie et du Travail, explique que le projet de loi vise à mettre en œuvre le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013, ci-après le "Règlement sur la cybersécurité" (ou en anglais *Cybersecurity Act* – "CSA"). La mise en œuvre de ce règlement exige l'adoption de dispositions en droit national, notamment pour les inspections, les réclamations, les recours et les sanctions, ainsi que pour la collaboration entre autorités.

Le Règlement sur la cybersécurité crée un cadre pour la délivrance et la reconnaissance mutuelle de certificats européens liés à la cybersécurité. En établissant un système européen harmonisé de certifications en matière de cybersécurité, le Règlement sur la cybersécurité vise à accroître la transparence de l'assurance en matière de cybersécurité des produits, services et processus des technologies de l'information et des communications (ci-après "TIC") et, partant, à renforcer la confiance dans le marché intérieur numérique ainsi que sa compétitivité.

Le recours aux certifications prévues par le Règlement sur la cybersécurité demeure en principe volontaire. Ces certifications de cybersécurité reposent sur des schémas de certification de cybersécurité qui contiennent un ou plusieurs niveaux d'assurance ("élémentaire", "substantiel" ou "élevé") ainsi que leur objet, leur champ d'application, leur finalité, les critères et méthodes d'évaluation spécifiques et les informations à fournir.

Afin d'obtenir un certificat de cybersécurité, il faut respecter les exigences du schéma de certification de cybersécurité et, soit délivrer une déclaration de conformité de l'Union européenne, soit obtenir la certification auprès d'une entité compétente. Les organismes d'évaluation de la conformité accrédités délivrent (en principe) les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel" et l'autorité nationale de certification de cybersécurité délivre (en principe) les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élevé".

DAMES EN HEREN,

Uw commissie heeft dit wetsontwerp besproken tijdens haar vergadering van 1 juni 2022.

I. — **INLEIDENDE UITEENZETTING**

De heer Pierre-Yves Dermagne, vice-eersteminister en minister van Economie en Werk, geeft aan dat dit wetsontwerp uitvoering beoogt te geven aan Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013, hierna de "Cyberbeveiligingsverordening" (of in het Engels *Cybersecurity Act* – "CSA"). Om deze verordening uit te voeren, moeten in het nationaal recht bepalingen worden ingevoerd, met name met betrekking tot inspecties, klachten, beroepen, sancties en de samenwerking tussen overheden.

De Cyberbeveiligingsverordening biedt een kader voor de afgifte en wederzijdse erkenning van Europese cyberbeveiligingscertificaten. Ze voert een geharmoniseerd Europees cyberbeveiligingscertificeringssysteem in om de transparantie van de cyberbeveiligingszekerheid van producten, diensten en processen op het gebied van informatie- en communicatietechnologie (hierna "ICT"), en daarmee het vertrouwen in en het concurrentievermogen van de digitale interne markt, te vergroten.

Het gebruik van de certificeringen waarin de Cyberbeveiligingsverordening voorziet, blijft in principe vrijwillig. Deze cyberbeveiligingscertificeringen zijn gebaseerd op cyberbeveiligingscertificeringsregelingen die een of meer zekerheidsniveaus ("basis", "substantieel" of "hoog") bevatten, alsook het onderwerp, het toepassingsgebied en het doel ervan, de specifieke evaluatiecriteria en -methoden, en de te verstrekken informatie.

Om een cyberbeveiligingscertificaat te verkrijgen, moet worden voldaan aan de voorschriften van de cyberbeveiligingscertificeringsregeling en moet ofwel een EU-conformiteitsverklaring worden afgegeven, ofwel de certificering worden verkregen bij een bevoegde entiteit. Geaccrediteerde conformiteitsbeoordelingsinstanties geven (in principe) Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" af en de nationale cyberbeveiligingscertificeringsautoriteit geeft (in principe) Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog" af.

Le Règlement sur la cybersécurité prévoit la désignation, au niveau national, d'une entité en tant qu'Autorité nationale de certification de cybersécurité (ANCC). Il dispose également que l'ANCC doit être munie de certains pouvoirs et respecter certaines obligations afin d'accomplir ses missions de représentation au niveau européen, de délivrance, de contrôle, de sanction et de recours. Ce règlement requiert également qu'un recours juridictionnel effectif soit mis en place au niveau national. Enfin, il permet que le droit national rende certaines certifications de cybersécurité obligatoires au sein de l'État membre concerné.

Ce projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité contient les dispositions nécessaires à la mise en œuvre effective du Règlement sur la cybersécurité.

Le projet établit la procédure de désignation de l'ANCC, les possibilités d'échange d'informations au niveau national, les obligations en matière d'indépendance et de respect des droits des tiers (encadrement des traitements de données à caractère personnel, respect du principe *audi alteram partem*, usage proportionné des pouvoirs, etc.) et détaille les pouvoirs de délivrance, de contrôle, de sanction et de réclamation ainsi que les garanties venant encadrer ces pouvoirs (contrôle par le juge d'instruction, recours spécifique devant la Cour des Marchés, devoir d'information des personnes concernées, etc.). Afin de réaliser les missions de contrôle et de sanction, un service d'inspection sera créé au sein de l'ANCC.

Le Roi pourra confier certaines missions de contrôle et de sanction à d'autres autorités, à leur demande et après avis de l'ANCC, pour certains schémas de certification de cybersécurité.

Le projet de loi encadre également les certifications éventuellement rendues obligatoires en Belgique. L'utilisation de certificats de cybersécurité pourra aussi faciliter les contrôles des autorités sectorielles ou de surveillance du marché.

Selon le Règlement sur la cybersécurité et le projet de loi qui le met en œuvre, les organismes d'évaluation de la conformité accrédités par l'autorité nationale d'accréditation délivreront, en principe, les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel". L'ANCC sera, elle, chargée de délivrer les certifications au niveau d'assurance élevé dans notre pays.

De Cyberbeveiligingsverordening voorziet in de aanwijzing, op nationaal niveau, van een entiteit als nationale cyberbeveiligingscertificeringsautoriteit (hierna "NCCA"). Ze bepaalt ook dat de NCCA over bepaalde bevoegdheden moet beschikken en bepaalde verplichtingen moet nakomen om haar opdrachten op het gebied van vertegenwoordiging op Europees niveau, afgifte, toezicht, sancties en beroepen uit te voeren. Verder moet, volgens deze verordening, een doeltreffende voorziening in rechte worden geboden op nationaal niveau. Tot slot zorgt ze ervoor dat het nationaal recht bepaalde cyberbeveiligingscertificeringen kan opleggen binnen de betrokken lidstaat.

Dit wetsontwerp inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit bevat de nodige bepalingen om de Cyberbeveiligingsverordening effectief ten uitvoer te leggen.

Het wetsontwerp bepaalt de aanwijzingsprocedure van de NCCA, de mogelijkheden van informatie-uitwisseling op nationaal niveau, de verplichtingen met betrekking tot onafhankelijkheid en naleving van de rechten van derden (regeling voor de verwerking van persoonsgegevens, naleving van het principe *audi alteram partem*, evenredig gebruik van bevoegdheden enzovoort) en beschrijft de bevoegdheden inzake afgifte, toezicht, sancties en klachten, alsook de waarborgen voor deze bevoegdheden (toezicht van de onderzoeksrechter, specifieke beroepsprocedure voor het Marktenhof, informatieplicht van de betrokkenen enzovoort). Met het oog op de uitvoering van de opdrachten inzake toezicht en sancties zal binnen de NCCA een inspectiedienst worden opgericht.

Voor sommige cyberbeveiligingscertificeringsregelingen kan de Koning bepaalde opdrachten inzake toezicht en sancties toevertrouwen aan andere overheden, zulks op verzoek van laatstgenoemden en na advies van de NCCA.

Het wetsontwerp regelt ook de certificeringen die eventueel zijn opgelegd in België. Het gebruik van cyberbeveiligingscertificaten kan ook controles door sectorale overheden of inzake markttoezicht vergemakkelijken.

Volgens de Cyberbeveiligingsverordening en het wetsontwerp dat voorziet in de uitvoering ervan, zullen de conformiteitsbeoordelingsinstanties die door de nationale accreditatieautoriteit zijn geaccrediteerd, in principe Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" afgeven. De NCCA zal belast zijn met de afgifte van certificeringen voor zekerheidsniveau "hoog" in België.

L'ANCC devra également s'assurer que toutes les règles liées à ce règlement seront correctement appliquées en Belgique. Enfin, cette autorité sera le représentant national au sein du Groupe européen de certification de cybersécurité (GECC).

De NCCA zal er ook op moeten toezien dat alle regels in verband met deze verordening correct worden toegepast in België. Tot slot zal deze autoriteit de nationale vertegenwoordiger zijn in de Europese Groep voor cyberbeveiligingscertificering (EGC).

II. — **DISCUSSION**

A. **Questions et observations des membres**

M. Michael Freilich (N-VA) souscrit aux objectifs du projet de loi à l'examen.

En effet, les organisations, les fabricants ou les fournisseurs impliqués dans la conception et le développement de produits TIC, services TIC ou processus TIC doivent être encouragés à mettre en œuvre, aux stades les plus précoces de la conception et du développement, des mesures permettant de protéger au mieux la sécurité de ces produits, services et processus, de manière à ce que la survenance de cyberattaques soit présumée et que leur incidence soit anticipée et réduite le plus possible.

Le membre estime qu'il est positif que les pratiques soient harmonisées en matière de cybersécurité au sein de l'Union, tout comme la prise en compte des innovations en matière de cybersécurité.

Le membre émet pourtant des réserves à propos du texte à l'examen. Ce texte prévoit en effet une série de délégations au Roi qui empêchent de savoir précisément qui fera quoi. Comment la collaboration entre les autorités publiques, les services d'inspection et les acteurs privés sera-t-elle, par exemple, réglée? Pourquoi cela ne peut-il pas être prévu dans le projet de loi?

Il est en outre impossible de savoir si les personnes et les moyens nécessaires seront prévus, combien la mise en œuvre de la réglementation en projet coûtera et qui se chargera de son financement.

Il n'est pas non plus clairement indiqué quelles informations seront effectivement échangées, entre quelles entités, ni si la protection de la vie privée ne sera pas violée à cet égard.

Les services d'inspection disposent de compétences très étendues en ce qui concerne le contrôle du respect du Règlement sur la cybersécurité et de la loi.

Enfin, l'avis de l'APD relatif à l'avant-projet de loi n'a pas été suivi sur certains points. Le projet de loi déroge aux règles relatives au respect de la vie privée.

II. — **BESPREKING**

A. **Vragen en opmerkingen van de leden**

De heer Michael Freilich (N-VA) onderschrijft de doelstellingen van het voorliggende wetsontwerp.

Organisaties, fabrikanten en aanbieders die betrokken zijn bij het ontwerp en de ontwikkeling van ICT-producten, -diensten en -processen moeten er immers toe worden aangespoord om al in de eerste fase van ontwerp en ontwikkeling maatregelen te treffen om ervoor te zorgen dat het beveiligingsniveau van deze producten, diensten en processen zo hoog mogelijk is, zodat cyberaanvallen zijn ingecalculeerd en de gevolgen daarvan zijn ingeschat en tot een minimum beperkt.

De harmonisatie van cyberbeveiligingspraktijken in de EU is volgens het lid een goede zaak, net als het in aanmerking nemen van innovaties op het vlak van cyberbeveiliging.

Niettemin plaatst het lid kanttekeningen bij de voorliggende tekst, die immers voorziet in een hele reeks machtigingen aan de Koning, waardoor het niet duidelijk is wie precies wat gaat doen. Hoe zal bijvoorbeeld de samenwerking worden geregeld tussen de verschillende overheden, inspectiediensten en private actoren? Waarom kan dat niet bepaald worden in het wetsontwerp?

Het is voorts koffiedik kijken of de noodzakelijke mensen en middelen zullen worden uitgetrokken, hoeveel de uitvoering van de ontworpen regeling zal kosten en wie de factuur zal betalen.

Het is evenmin helder welke informatie er allemaal zal worden uitgewisseld, tussen welke entiteiten en of daarbij de bescherming van de persoonlijke levenssfeer niet met de voeten zal worden getreden.

De inspectiediensten beschikken over zeer ruime bevoegdheden om controles uit te voeren op de naleving van de Cyberbeveiligingsverordening en van de wet.

Ten slotte werd het advies van de GBA over het voorontwerp van wet op bepaalde punten niet gevolgd. Het wetsontwerp wijkt af van de privacyregels.

M. Freilich espère que le vice-premier ministre lui fournira des précisions au sujet des préoccupations précitées.

M. Albert Vicaire (Ecolo-Groen) souligne l'utilité de procédures européennes pour un texte aussi technique afin de standardiser et d'ouvrir le marché: cela permet d'avoir des équipements qui sont à taille d'une production industrielle pour lancer un marché. La législation sur la cybersécurité a aujourd'hui une utilisation quotidienne: placements d'alarmes, équipements électroniques dans les habitations,… Il souhaiterait savoir si cette législation protège également le risque des équipements placés dans les habitations privées.

Mme Leslie Leoni (PS) explique qu'il s'agit d'un projet technique, mais important, parce que les cyberattaques sont une menace croissante à laquelle les citoyens sont confrontés, parce que le contexte géopolitique est menaçant et parce que le monde se numérise de plus en plus. Et dans ce cadre, elle estime que la Belgique a besoin d'un cadre robuste pour diminuer la vulnérabilité aux cyber menaces. C'est ce à quoi contribue le Cybersecurity Act, qui est mis en œuvre par ce projet de loi.

Avec ce projet de loi la Belgique pourra jouer son rôle dans le mécanisme européen de certification de cybersécurité, en désignant une autorité nationale de certification de cybersécurité et en mettant en place une certification de cybersécurité des produits et services TIC. Ces mesures sont soutenues par le groupe PS, en raison de leur impact positif.

L'intervenante estime que ces mesures auront un impact positif pour les consommateurs, qui en achetant des produits ou des services certifiés, seront mieux protégés des cyber menaces. Il y aura également un impact positif pour les différents secteurs, par exemple le secteur de la santé. Les hôpitaux ont recours quotidiennement aux technologies de l'information et des communications; en recourant à des produits et des services certifiés en matière de cybersécurité, ils seront moins vulnérables aux cyber menaces.

Finalement, ce mécanisme de certification permettra d'augmenter la confiance dans les technologies numériques, de mieux protéger le citoyen en ligne, et donc contribuera à l'indépendance et au soutien de l'économie. Le groupe PS soutiendra ce projet de loi.

M. Erik Gilissen (VB) souligne la grande importance que revêt la cybersécurité dans une société toujours plus numérique. Tout le monde se souvient encore des cyberattaques menées récemment contre des sites d'autorités publiques.

De heer Freilich hoopt van de vice-eersteminister duiding te bekomen bij bovenvermelde bezorgdheden.

De heer Albert Vicaire (Ecolo-Groen) benadrukt het nut van Europese procedures voor een dergelijke technische tekst die de markt beoogt te normaliseren en open te stellen: aldus kan men met betrekking tot overheidsopdrachten beschikken over apparatuur op het niveau van een industriële productie. De cyberbeveiligingswetgeving heeft vandaag een praktisch toepassingsgebied: plaatsen van alarmsystemen, elektronische apparatuur in woningen enzovoort. De spreker wil weten of deze wetgeving ook de risico's van apparatuur in privéwoningen behelst.

Mevrouw Leslie Leoni (PS) stelt dat het wetsontwerp weliswaar technisch is, maar niettemin belangrijk, want cyberaanvallen zijn een steeds grotere bedreiging voor de burgers, de geopolitieke context is bedreigend en de wereld wordt steeds digitaler. In dat opzicht is zij van mening dat België een robuust kader nodig heeft om minder kwetsbaar te zijn voor cyberdreigingen. Dat is onder meer het opzet van de Cyberbeveiligingsverordening, waaraan dit wetsontwerp uitvoering geeft.

Met dit wetsontwerp zal België in het Europese cyberbeveiligingscertificeringsmechanisme zijn rol kunnen spelen door een nationale cyberbeveiligingscertificeringsautoriteit aan te wijzen en door te voorzien in een cyberbeveiligingscertificering voor ICT-producten en -diensten. Gelet op hun gunstige impact steunt de PS-fractie die maatregelen.

De spreekster is van mening dat deze maatregelen een goede zaak zijn voor de consument, die bij de aankoop van gecertificeerde producten of diensten beter beschermd zal zijn tegen cyberdreigingen. Er zal ook een positief effect zijn voor de verschillende sectoren, bijvoorbeeld de gezondheidssector. Ziekenhuizen maken dagelijks gebruik van informatie- en communicatietechnologieën; door gecertificeerde cyberbeveiligingsproducten en -diensten te gebruiken, zullen zij minder kwetsbaar zijn voor cyberdreigingen.

Tot slot zal dit certificeringsmechanisme het vertrouwen in digitale technologieën vergroten, de burger beter beschermen online en zo bijdragen tot de onafhankelijkheid en de ondersteuning van de economie. De PS-fractie zegt haar steun aan dit wetsontwerp toe.

De heer Erik Gilissen (VB) onderstreept het grote belang van cyberbeveiliging in een steeds verder digitaliserende samenleving. De recente cyberaanvallen op bepaalde overheidswebsites liggen nog vers in het geheugen.

Les produits, services et processus numériques ainsi que leurs fournisseurs doivent atteindre un certain niveau de sécurité. Une certification peut éclairer le consommateur à cet égard.

Certains points du projet de loi ont été adaptés à la suite des avis rendus par l'Organe de contrôle de l'information policière (COC) et l'APD sur l'avant-projet de loi. Toutes les observations n'ont toutefois pas été prises en compte. M. Gilissen estime dès lors qu'il serait utile de recueillir l'avis écrit de la FeWeb, la Fédération des métiers du Web, concernant le projet de loi à l'examen.

Le texte à l'examen prévoit de confier un nombre relativement élevé de décisions au Roi. M. Gilissen déplore que le parlement n'ait désormais plus voix au chapitre à cet égard.

Mme Florence Reuter (MR) confirme le soutien du groupe MR à ce projet de loi.

Aujourd'hui, la croissance des services technologiques numériques offre pas mal de possibilités et d'opportunités de développement pour les citoyens avec en contrepartie l'augmentation des cyber menaces qui peuvent accroître les risques et compromettre les avantages que présentent les nouvelles technologies.

C'est un projet de loi qui complète la stratégie nationale actualisée qui propose un cyber espace ouvert, libre et sécurisé. Le texte permet de répondre à ces cyber menaces qui pourraient cibler la Belgique.

Mme Leen Dierick (CD&V) fait observer que le texte à l'examen est très technique mais également très important. Nous devons lutter contre les cyberattaques visant les entreprises. Ces attaques non seulement causent des préjudices financiers et économiques considérables mais sapent également la confiance du citoyen envers le monde numérique.

Il n'est pour autant pas possible d'échapper à la numérisation. Notre société doit encore se numériser davantage. Il est encore apparu récemment que la Belgique est à la traîne en Europe dans le domaine du commerce électronique. Nous ratons ainsi l'opportunité de créer de nombreux emploi.

Notre pays doit dès lors encore plus miser sur la numérisation. Il va de soi que ce processus doit être sûr. Le projet de loi, qui vise à mettre en œuvre le Règlement sur la cybersécurité, peut compter sur le soutien du groupe CD&V. Une coordination européenne est nécessaire pour garantir des conditions de concurrence équitables.

Digitale producten, diensten en processen, alsook hun aanbieders, moeten een zeker niveau van beveiliging behalen. Een certificering kan de consument duidelijkheid ter zake verschaffen.

Het wetsontwerp werd op bepaalde punten aangepast naar aanleiding van de adviezen van het Controleorgaan op de Politionele Informatie (COC) en van de GBA op het voorontwerp van wet. Niet alle opmerkingen werden echter ter harte genomen. Het lijkt de heer Gilissen daarom nuttig het schriftelijk advies omtrent het wetsontwerp in te winnen van FeWeb, de beroepsvereniging van digitale bedrijven.

Nogal wat beslissingen worden door de voorliggende tekst aan de Koning toevertrouwd. De heer Gilissen betreurt dat het Parlement daarover geen zeggenschap meer zal hebben.

Mevrouw Florence Reuter (MR) bevestigt de steun van de MR-fractie voor dit wetsontwerp.

Het toenemende aanbod van digitale technologische diensten biedt de burger thans tal van ontwikkelingsmogelijkheden en -kansen. Daartegenover staat dat ook de cyberdreiging toeneemt, waardoor de risico's groter worden en de voordelen van de nieuwe technologieën in het gedrang komen.

Dit wetsontwerp vormt een aanvulling op de geactualiseerde nationale strategie voor een open, vrije en beveiligde cyberspace en maakt het mogelijk het hoofd te bieden aan eventuele cyberdreigingen tegen België.

Mevrouw Leen Dierick (CD&V) merkt op dat de voorliggende tekst erg technisch, maar ook erg belangrijk is. Het is belangrijk de strijd tegen cyberaanvallen jegens bedrijven aan te gaan, die niet enkel veel financieel-economische schade veroorzaken, maar ook het vertrouwen van de burger in de digitale wereld ondermijnen.

Aan de digitalisering valt nochtans niet te ontkomen. Onze samenleving moet nog meer de digitale toer op. Onlangs nog bleek dat België achterophinkt in Europa op het vlak van de e-commerce. We laten daarbij veel jobs liggen.

Ons land moet dus nog meer inzetten op de digitalisering. Uiteraard moet dit wel op een veilige manier gebeuren. Het wetsontwerp, dat beoogt uitvoering te geven aan de Cyberbeveiligingsverordening, kan op de steun rekenen van de CD&V-fractie. Een Europees gecoördineerde aanpak is nodig om een gelijk speelveld te waarborgen.

Mme Dierick souhaiterait en revanche obtenir un peu plus de précisions au sujet de l'Autorité nationale de certification de cybersécurité qui devra être mise en place. Une nouvelle entité sera-t-elle créée à cet effet ou les tâches d'une instance existante seront-elles élargies? Des recrutements supplémentaires sont-ils prévus?

M. Roberto D'Amico (PVDA-PTB) est assez étonné en lisant l'avis de l'Autorité de protection des données (APD) qui est particulièrement critique à l'égard du projet de loi en question. L'APD cite l'avis du Contrôleur européen à la protection des données n° 05/2021 sur la stratégie en matière de cybersécurité et la directive SRI 2.0, qui rappelle que "la poursuite des objectifs de cybersécurité peut donner lieu au déploiement de mesures qui constituent une ingérence dans les droits à la protection des données et au respect de la vie privée des personnes. Il convient donc de veiller à ce que toute limitation potentielle du droit à la protection de la vie privée et des données à caractère personnel réponde aux exigences de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, et en particulier qu'elle soit mise en œuvre par le biais d'une mesure législative, qu'elle soit à la fois nécessaire et proportionnée et qu'elle respecte le contenu essentiel du droit".

L'APD pointe ensuite comme problématique les échanges de données que permettrait ce projet de loi. Des échanges qui "posent question au vu de leur objet très large". On parle d'échanges pour appliquer "toute sorte de disposition légale", sans indiquer de quelles dispositions il s'agit. Il estime donc qu'on ne peut donc pas vérifier le lien avec la cybersécurité ni la nécessité de ces échanges de données.

L'intervenant relève que le gouvernement va encore plus loin en indiquant que les données des clients pourront être collectées et utilisées par des services publics qui ne disposent pas de mission spécifique liée à la cybersécurité comme, par exemple, les services de police ou les services de renseignement et ce, pour leur propres missions de prévention et de détection de n'importe quelles infractions pénales, d'enquêtes et de poursuites ou encore pour n'importe quelle mission de la Sûreté de l'État et du Service Général du Renseignement et de la Sécurité.

Selon M. D'Amico, le partage d'informations doit se limiter aux produits, services et processus TIC. Ce règlement européen ne nécessite pas, selon l'Autorité, de devoir échanger les données à caractère personnel des citoyens. Il rappelle que l'APD est donc très claire

Wel zou mevrouw Dierick graag wat meer informatie krijgen over de op te richten nationale autoriteit voor de certificering van cyberbeveiliging. Wordt hiervoor een nieuwe instantie opgericht, of zal het takenpakket van een bestaande instantie worden uitgebreid? Worden er bijkomende aanwervingen gepland?

De heer Roberto D'Amico (PVDA-PTB) is behoorlijk verbaasd bij het doorlezen van het advies van de Gegevensbeschermingsautoriteit (GBA), dat bijzonder kritisch is over dit wetsontwerp. De GBA citeert uit advies nr. 05/2021 van de Europese Toezichthouder voor gegevensbescherming over de strategie voor cyberveiligheid en over de richtlijn NIS 2.0, waarin het volgende te lezen staat: "*la poursuite des objectifs de cybersécurité peut donner lieu au déploiement de mesures qui constituent une ingérence dans les droits à la protection des données et au respect de la vie privée des personnes. Il convient donc de veiller à ce que toute limitation potentielle du droit à la protection de la vie privée et des données à caractère personnel réponde aux exigences de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, et en particulier qu'elle soit mise en œuvre par le biais d'une mesure législative, qu'elle soit à la fois nécessaire et proportionnée et qu'elle respecte le contenu essentiel du droit*.".

Vervolgens bestempelt de GBA de gegevensuitwisseling die dit wetsontwerp mogelijk zou maken als problematisch. Naar verluidt zouden deze uitwisselingen vragen doen rijzen in verband met hun zeer ruime onderwerp. Men heeft het over uitwisselingen om allerhande wettelijke bepalingen toe te passen zonder aan te geven om welke bepalingen het gaat. De heer D'Amico is dus van oordeel dat het verband met cyberveiligheid niet kan worden nagegaan, evenmin als de noodzaak die gegevens uit te wisselen.

De spreker merkt op dat de regering nog een stap verder wil gaan door te bepalen dat de klantgegevens kunnen worden verzameld en gebruikt door overheidsdiensten die geen specifieke cyberbeveiligingsopdracht hebben, zoals de politie of inlichtingendiensten, ten bate van hun eigen opdrachten van preventie en opsporing van strafbare feiten, onderzoek en vervolging, of nog voor allerhande opdrachten van de Veiligheid van de Staat en de Algemene Inlichtingen- en Veiligheidsdienst.

De heer D'Amico vindt dat het delen van informatie beperkt moet blijven tot de producten, diensten en processen van de informatie- en communicatietechnologie. Volgens de GBA vereist die Europese verordening geen uitwisseling van de persoonsgegevens van burgers. De

dans son avis n° 08/2022: ce texte est disproportionné (point 9).

Pourtant, il déplore que le gouvernement agisse de manière disproportionnée en indiquant dans l'exposé des motifs que "conformément à ce que préconise l'Autorité de protection des données dans son avis […], il est possible de prévoir, dans le projet de loi, un échange d'informations pouvant porter sur des données à caractère personnel."

Etant donné que les services de police et les services judicaires auront accès aux données comme indiqué précédemment, M. D'Amico souhaiterait que soit demandé un avis aux commissions de la Justice et de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre

Par ailleurs, au vu de l'avis particulièrement sévère de l'APD concernant l'avant-projet de loi, le groupe PVDA-PTB aimerait demander un nouvel avis à l'Autorité sur le projet de loi tel que rédigé actuellement.

Mme Kathleen Verhelst (Open Vld) exprime son soutien au texte à l'examen, qui est important tant pour les entreprises que pour les consommateurs. Elle espère que la réglementation en projet ne restera pas lettre morte, mais qu'elle sera déployée efficacement et qu'elle sera perceptible sur le terrain.

M. Bert Moyaers (Vooruit) estime que le projet de loi, qui met en œuvre le Règlement sur la cybersécurité, est une initiative louable que son groupe peut soutenir. Les normes de cybersécurité permettent aux acteurs privés de procéder à une évaluation des risques.

B. **Réponses du vice-premier ministre**

M. Pierre-Yves Dermagne, vice-premier ministre et ministre de l'Économie et du Travail, explique que le gouvernement a demandé l'avis de l'APD sur l'avant-projet de loi. L'avis de l'APD était, comme le dit à juste titre M. D'Amico, critique. En conséquence, le gouvernement a apporté des adaptations au texte. Le projet de loi à l'examen n'est donc pas le texte sur lequel l'APD s'est penché.

Sur les différents domaines de cybersécurité concernés par le texte, le vice-premier ministre rappelle que c'est un processus qui est en cours au sein de l'Union européenne et des États membres. Le programme de travail de l'Union pour la certification européenne de cybersécurité est un document stratégique qui permet à l'industrie, aux autorités nationales et aux organismes

GBA is dus volgens de spreker heel duidelijk in haar advies nr. 08/2022 (punt 9): het wetsontwerp is niet proportioneel.

Niettemin betreurt hij dat de regering disproportioneel te werk gaat door in de memorie van toelichting aan te geven dat "zoals de Gegevensbeschermingsautoriteit in haar advies (…) aanbeveelt (…) het wetsontwerp bijgevolg informatie-uitwisseling mogelijk [maakt] die persoonsgegevens kan betreffen.".

Aangezien de politiediensten en de gerechtelijke diensten, zoals eerder aangegeven, toegang tot de gegevens zouden hebben, dringt de heer D'Amico erop aan het advies in te winnen van de Kamercommissies voor Justitie en voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken.

Gelet op het bijzonder strenge advies van de GBA over het voorontwerp van wet, wil de PVDA-PTB-fractie de GBA voorts om een nieuw advies over het wetsontwerp in zijn huidige vorm vragen.

Mevrouw Kathleen Verhelst (Open Vld) spreekt haar steun uit voor de voorliggende tekst, die belangrijk is voor zowel het bedrijfsleven als de consument. Zij hoopt dat de ontworpen regeling geen dode letter zal blijven, maar efficiënt zal worden uitgerold en voelbaar zal zijn in het veld.

De heer Bert Moyaers (Vooruit) stelt dat het wetsontwerp, dat uitvoering geeft aan de Cyberbeveiligingsverordening, een lovenswaardig initiatief betreft waarmee zijn fractie kan instemmen. Cyberbeveiligingsnormen stellen private actoren in staat een risico-inschatting te maken.

B. **Antwoorden van de vice-eersteminister**

De heer Pierre-Yves Dermagne, vice-eersteminister en minister van Economie en Werk, legt uit dat de regering het advies van de GBA heeft ingewonnen omtrent het voorontwerp van wet. Het advies van de GBA was, zoals de heer D'Amico terecht stelt, kritisch. Daarop heeft de regering de tekst aangepast. Het voorliggende wetsontwerp is dus niet de tekst waarover de GBA zich heeft gebogen.

Aangaande de diverse domeinen van de cyberveiligheid waarop het wetsontwerp betrekking heeft, stipt de vice-eersteminister aan dat het gaat om een proces dat in de EU en de lidstaten aan de gang is. Het EU-werkprogramma voor de Europese cyberbeveiligingscertificering is een strategisch document waarmee de industrie, de nationale overheden en de normalisatie-instellingen

de normalisation de se préparer aux futurs schémas européen de certification de cybersécurité. Le programme de travail fixe également une série de priorités stratégiques et offre un aperçu des demandes spécifiques de schémas de certification de cybersécurité. Il établit une distinction entre les futurs schémas candidats: *internet of things*, *industrial automation and control systems*, *secure development lifecycle* et les domaines soumis à une réflexion future (*areas for future reflection*). L'intervenant confirme que trois schémas sont actuellement en préparation (EUCC, EUCS, EU5G). Le premier schéma (*Common Criteria-based European candidate cybersecurity certification scheme* – EUCC) est prévu pour 2022. Cela aura des implications dans la vie de tous les jours, comme l'Internet des objets.

En ce qui concerne l'organisation des flux d'information entre l'ANCC et les administrations concernées, l'article 6 du projet de loi précise cette coopération au niveau national entre l'autorité nationale de certification de cybersécurité et les autorités publiques dont l'Institut belge des services postaux et des télécommunications (IBPT) et l'autorité nationale d'accréditation. Ces autorités s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, notamment en matière de délivrance de certificats, de contrôle, de sanction et de réclamation.

Lorsqu'un échange porte sur des données à caractère personnel, il se fait dans le respect des dispositions du chapitre 8 de la loi, notamment les articles 36 et 37.

Sur la question des organismes d'évaluation de conformité (*conformity assessment bodies* – CAB), ils ne peuvent donner des certificats que sur la portée pour laquelle ils sont accrédités. Trois organismes sont accrédités en Belgique pour la norme ISO/CEI 27001 par BELAC, l'organisme belge d'accréditation, placé sous la responsabilité du SPF Economie. BELAC fonctionne selon un système de management conforme aux exigences internationales relatives à la gestion des organismes d'accréditation. Il existe aussi 380 instances ailleurs dans l'Union européenne qui peuvent évaluer et établir des certificats de conformité en Belgique. Sous le *CyberSecurity Act*, les CAB seront accrédités de manière individualisée. Les autorités publiques communiqueront au marché pour permettre aux entreprises d'avoir l'information pour se faire accréditer. Les CAB existants seront repris dans une base de données "Nando" qui est gérée par le SPF Economie.

zich kunnen voorbereiden op de aankomende Europese cyberbeveiligingscertificeringsregelingen. Het werkprogramma legt tevens een aantal strategische speerpunten vast en biedt een overzicht van de specifieke aanvragen van cyberbeveiligingscertificeringsregelingen. In dat programma wordt een onderscheid gemaakt tussen de toekomstige potentiële regelingen: *internet of things*, *industrial automation and control systems*, *secure development lifecycle* en de domeinen waarover in de toekomst zal worden nagedacht (*areas for future reflection*). De spreker bevestigt dat thans drie regelingen op stapel staan (EUCC, EUCS en EU5G). De eerste regeling (*Common Criteria-based European candidate cybersecurity certification scheme* – EUCC) is gepland voor 2022. Het zal gevolgen hebben voor het alledaagse leven, net als het internet der dingen.

In verband met de organisatie van de informatiestroom tussen de NCCA en de betrokken overheden, strekt artikel 6 van het wetsontwerp tot verduidelijking van die samenwerking op nationaal niveau tussen de nationale cyberbeveiligingscertificeringsautoriteit en de overheden, waaronder het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT) en de nationale accreditatieautoriteit. Die overheden wisselen onderling de nodige informatie uit met het oog op de toepassing van de Cyberbeveiligingsverordening, de met dit wetsontwerp beoogde wet of nog de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten.

Wanneer informatie inzake persoonsgegevens wordt uitgewisseld, moet zulks geschieden overeenkomstig de bepalingen van hoofdstuk 8 van de wet, meer bepaald de artikelen 36 en 37.

De instellingen voor de conformiteitsbeoordeling (*conformity assessment bodies* – CAB) mogen certificaten alleen uitreiken inzake die aspecten waarvoor ze geaccrediteerd zijn. In België zijn drie instellingen geaccrediteerd voor de norm ISO/CEI 27001. Die accreditatie hebben ze verkregen van BELAC, de Belgische Accreditatie-instelling die onder toezicht staat van de FOD Economie. BELAC werkt volgens een beheersysteem overeenkomstig de internationale vereisten inzake het beheer van de accreditatie-instellingen. Er bestaan ook 380 instellingen elders in de Europese Unie, die conformiteitscertificaten in België kunnen evalueren en opstellen. Op basis van de *CyberSecurity Act* worden CAB's op individuele basis geaccrediteerd. De overheden zullen de markt informeren opdat de bedrijven over de nodige informatie beschikken om te worden geaccrediteerd. De bestaande CAB's zullen worden opgenomen in een zogenaamde Nando-databank, die door de FOD Economie wordt beheerd.

Les frais d'experts externes requis par le service d'inspection peuvent être mis à charge des organismes d'évaluation de la conformité, des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne dès lors que, d'une part, ces derniers sollicitent volontairement une autorisation ou une certification, et d'autre part, ces derniers pourraient en tirer un avantage pécuniaire ou commercial.

De kosten voor externe experten die door de inspectiedienst worden opgeroepen, kunnen ten laste worden gelegd van de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen, aangezien die laatsten enerzijds zelf een toelating of certificering aanvragen en daar anderzijds een financieel of commercieel voordeel uit kunnen halen.

À l'attention de M. D'Amico, le vice-premier ministre précise que l'accès aux produits, services ou processus TIC faisant l'objet de la certification dont serait titulaire une personne soumise à l'article 458 du Code pénal pourra être nécessaire afin de mener à bien les missions de supervision du service d'inspection. Les membres assermentés doivent pouvoir, le cas échéant, avoir accès à ces produits, services ou processus TIC.

Ter attentie van de heer D'Amico verduidelijkt de vice-eersteminister dat de toegang tot ICT-producten, -diensten of -processen die het voorwerp uitmaken van het certificaat waarvan een onder artikel 458 van het Strafwetboek ressorterende betrokkene houder is, noodzakelijk kan zijn om de toezichtsopdrachten van de inspectiedienst uit te voeren. In voorkomend geval moeten de beëdigde leden toegang kunnen krijgen tot die ICT-producten, -diensten of -processen.

Néanmoins, étant donné la criticité de ces informations et la protection qu'il convient de lui fournir, la disposition prévoit, de manière claire, que l'accès à ces informations n'est possible pour les membres assermentés, seulement lorsque cet accès est nécessaire à leurs missions de supervision. Par ailleurs, il faut souligner que les membres assermentés ne sont pas des officiers de police judicaire.

Wegens de kritieke aard van die informatie en de bescherming die ter zake moet worden geboden, wordt in de bepaling echter duidelijk aangegeven dat de beëdigde leden alleen toegang tot die informatie kunnen krijgen indien zulks noodzakelijk is voor hun toezichtsopdrachten.

Ils ne peuvent faire usage de la contrainte à l'encontre des personnes contrôlées et ne peuvent, dès lors, forcer l'accès aux informations protégées par l'article 458 du Code pénal. De cette manière, la disposition s'aligne à ce que prévoit l'article 86 de la loi du 7 décembre 2016 portant organisation de la profession et de la supervision publique des réviseurs d'entreprises.

Voorts moet worden beklemtoond dat de beëdigde leden geen officieren van gerechtelijke politie zijn. Zij mogen geen gebruik maken van dwang jegens de gecontroleerde personen en kunnen bijgevolg geen toegang afdwingen tot de op grond van artikel 458 van het Strafwetboek beschermde informatie. De bepaling loopt dus gelijk met de inhoud van artikel 86 van de wet van 7 december 2016 tot organisatie van het beroep van en het publiek toezicht op de bedrijfsrevisoren.

L'Autorité de protection des données préconise une disposition reprenant des garanties similaires à ce que prévoient les articles 56*bis* et 90*octies* du Code d'instruction criminelle. À défaut, le projet de loi doit préciser qu'aucune collecte de ces informations protégées n'est possible.

De Gegevensbeschermingsautoriteit pleit voor een bepaling met gelijkaardige waarborgen als die welke zijn vervat in de artikelen 56*bis* en 90*octies* van het Wetboek van strafvordering. Bij gebrek daaraan zou in het wetsontwerp moeten worden vermeld dat die beschermde informatie niet kan worden verzameld.

Étant donné que les pouvoirs du service d'inspection sont bien plus limités que ce que prévoit le Code d'instruction criminelle aux article 56*bis* et 90*octies*, il a été décidé de ne pas implémenter les garanties demandées par l'Autorité de protection des données dans son avis.

Aangezien de bevoegdheden van de inspectiedienst veel beperkter zijn dan wat in de artikelen 56*bis* en 90*octies* van het Wetboek van strafvordering is bepaald, werd beslist de in het advies van de Gegevensbeschermingsautoriteit gevraagde waarborgen niet op te nemen.

M. Valéry Vander Geeten, responsable juridique du Centre pour la Cybersécurité Belgique (CCB), complète la réponse du ministre en précisant qu'il ne s'agit pas de

De heer Valéry Vander Geeten, juridisch verantwoordelijke van het Centrum voor Cybersecurity België (CCB), geeft ter aanvulling van het antwoord van de minister

créer une nouvelle autorité administrative car les tâches qui incombent à l'ANCC rejoignent les missions légales existantes du CCB. Elles relèvent de l'arrêté royal du 10 octobre 2014 et de 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 ("loi NIS"). Il est prévu un mécanisme éventuel de délégation de certaines missions en fonction des schémas de certification à une autre autorité que le CCB pour tenir compte des compétences ou des missions d'inspection existantes dans d'autres administrations (IBPT, SPF Economie etc.).

L'orateur ajoute que la partie échange de données à caractère personnel du projet de loi a bien été adaptée en tenant compte des remarques reprises dans l'avis de l'APD. Elles sont limitées uniquement aux justifications légales liées aux traitements de données en matière de certification de cybersécurité.

C. **Répliques et réponses supplémentaires**

M. Michael Freilich (N-VA) apprend que le CCB deviendra l'autorité nationale de certification de cybersécurité (ANCC). Selon l'intervenant, il semble donc logique, et tout à fait préférable, de l'indiquer en toutes lettres dans le projet de loi, plutôt que d'habiliter le Roi à désigner l'ANCC. M. Freilich n'est pas enclin à donner carte blanche à l'exécutif à cet égard. Il envisage de présenter un amendement afin que le parlement puisse voter sur la question de savoir quelle instance remplira le rôle d'ANCC.

En outre, M. Freilich a compris de la réponse du vice-premier ministre que les coûts de la réglementation en projet seront supportés par les entreprises inspectées. Cela signifie-t-il concrètement qu'une entreprise soumise à une inspection recevra ensuite une facture? Il s'agit là d'une façon étrange de procéder, surtout si l'inspection prouve que l'entreprise respecte correctement les règles.

Enfin, M. Freilich s'interroge sur le fait que le projet de loi confie des pouvoirs de contrôle étendus à des fonctionnaires n'ayant pas de compétences policières ou judiciaires.

M. Pierre-Yves Dermagne, vice-premier ministre et ministre de l'Economie et du Travail, ajoute, en réponse à la question de M. Freilich sur les pouvoirs du Roi

aan dat het niet de bedoeling is een nieuwe administratieve instantie te creëren, want de taken van de NCCA sluiten aan bij de bestaande wettelijke opdrachten van het CCB. Zij ressorteren onder het koninklijk besluit van 10 oktober 2014 en onder 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 (de zogenoemde "NIS-wet"). Er is voorzien in een regeling op grond waarvan naar gelang van de certificeringsschema's bepaalde opdrachten eventueel kunnen worden gedelegeerd aan een andere instantie dan het CCB, teneinde rekening te houden met bestaande bevoegdheden of inspectietaken van andere overheidsdiensten (BIPT, FOD Economie enz.).

De spreker voegt eraan toe dat het onderdeel van het wetsontwerp inzake uitwisseling van persoonsgegevens wel degelijk werd aangepast, rekening houdend met de opmerkingen in het advies van de GBA. Zij zijn beperkt tot louter de wettelijke rechtvaardigingsgronden in verband met de verwerking van gegevens betreffende cyberbeveiligingscertificering.

C. **Replieken en bijkomende antwoorden**

De heer Michael Freilich (N-VA) verneemt dat het CCB de nationale cyberbeveiligingscertificeringsautoriteit (NCCA) zal worden. Het lijkt de spreker dan ook logisch, en alleszins verkieslijk, dit met zoveel woorden op te nemen in het wetsontwerp, in plaats van te voorzien in een machtiging aan de Koning om de NCCA aan te wijzen. De heer Freilich is niet geneigd de uitvoerende macht hiervoor carte blanche te geven. Hij overweegt daartoe een amendement in te dienen, zodat het Parlement zal kunnen stemmen over de vraag welke instantie de rol van NCCA zal vervullen.

Daarnaast maakte de heer Freilich uit het antwoord van de vice-eersteminister op dat de kosten van de ontworpen regeling zullen worden gedragen door de geïnspecteerde bedrijven. Betekent dit dan concreet dat een bedrijf dat onderworpen wordt aan een inspectie, daarvoor een factuur zal ontvangen? Dat is toch een rare manier van werken, niet het minst als de inspectie aantoont dat het bedrijf de regels correct naleeft.

Tot slot stelt de heer Freilich zich vragen bij het feit dat het wetsontwerp verregaande controlebevoegdheden toevertrouwt aan ambtenaren zonder politionele of gerechtelijke bevoegdheden.

In antwoord op de vraag van de heer Freilich betreffende de machtiging aan de Koning inzake de aanwijzing van NCCA voegt *de heer Pierre-Yves Dermagne,*

concernant la désignation de l'ANCC, que ce choix a été fait sur la base des recommandations du Conseil d'État.

Le vice-premier ministre indique avoir répondu sur les coûts des inspections et experts externes. La certification se fera sur base volontaire des entreprises qui en supporteront les coûts.

M. Valéry Vander Geeten, CCB, complète la réponse du vice-premier ministre en précisant que le Roi est compétent pour les attributions des autorités administratives fédérales (en ce compris le CCB). La loi ne pourrait pas désigner le CCB directement. Cette compétence revient au Roi selon le prescrit constitutionnel.

Le vice-premier ministre précise que le Règlement sur la cybersécurité ne s'applique pas directement aux aspects liés à la sécurité publique et à l'ordre public.

Il souligne également que le projet de loi a bel et bien fait l'objet d'une concertation avec les entreprises, en particulier avec la Fédération des entreprises de Belgique.

M. Stefaan Van Hecke, président, suggère qu'à la lumière de la réponse du vice-premier ministre, une nouvelle demande d'avis auprès de l'APD serait peu utile. Il constate également qu'il n'y a pas de majorité en faveur de la demande d'un avis aux commissions de la Justice et de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives et à la FeWeb.

M. Roberto D'Amico (PVDA-PTB) et M. Erik Gilissen (VB) ne demandent pas de vote sur ce point.

III. — **VOTES**

CHAPITRE 1ER

Définitions et dispositions générales

Article 1er

L'article 1 est adopté à l'unanimité.

vice-eersteminister en minister van Economie en Werk, eraan toe dat die keuze werd gemaakt op basis van de aanbevelingen van de Raad van State.

De vice-eersteminister stelt dat hij de vraag betreffende de kosten van inspecties en externe deskundigen heeft beantwoord. De ondernemingen zullen zich vrijwillig laten certificeren en zullen de daarmee samenhangende kosten dragen.

De heer Valéry Vander Geeten (CCB) vervolledigt het antwoord van de vice-eersteminister door aan te stippen dat de Koning bevoegd is om federale administratieve overheden (inclusief het CCB) bevoegdheden toe te wijzen. Het CCB zou niet rechtstreeks in de wet kunnen worden aangewezen, want de Grondwet bepaalt dat zulks de bevoegdheid van de Koning is.

De vice-eersteminister verduidelijkt dat de Cyberbeveiligingsverordening niet rechtstreeks van toepassing is op aspecten in verband met openbare veiligheid en openbare orde.

Daarnaast wijst hij erop dat er over het wetsontwerp wel degelijk is overlegd met het bedrijfsleven, in het bijzonder met het Verbond van Belgische Ondernemingen.

De heer Stefaan Van Hecke, voorzitter, oppert dat, in het licht van het antwoord van de vice-eersteminister, een nieuwe adviesaanvraag bij de GBA weinig zoden aan de dijk zou zetten. Voorts stelt hij vast dat er geen meerderheid bestaat voor het inwinnen van een advies van de commissies voor Justitie en voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken en van FeWeb.

De heren Roberto D'Amico (PVDA-PTB) en Erik Gilissen (VB) dringen niet aan op een stemming over dit punt.

III. — **STEMMINGEN**

HOOFDSTUK 1

Definities en algemene bepalingen

Artikel 1

Artikel 1 wordt eenparig aangenomen.

Art. 2

L'article 2 est adopté par 14 voix et 1 abstention.

Art. 3

L'article 3 est adopté par 10 voix et 5 abstentions.

Art. 4

L'article 4 est adopté par 14 voix et 1 abstention.

CHAPITRE 2

Autorités compétentes et coopération au niveau national

Art. 5 à 7

Les articles 5 à 7 sont successivement adoptés par 10 voix et 5 abstentions.

CHAPITRE 3

Autorité nationale de certification de cybersécurité

Art. 8 et 9

Les articles 8 et 9 sont successivement adoptés par 14 voix et 1 abstention.

CHAPITRE 4

Délivrance des certificats européens

Art. 10 à 12

Les articles 10 et 12 sont successivement adoptés par 14 voix et 1 abstention.

Art. 2

Artikel 2 wordt aangenomen met 14 stemmen en 1 onthouding.

Art. 3

Artikel 3 wordt aangenomen met 10 stemmen en 5 onthoudingen.

Art. 4

Artikel 4 wordt aangenomen met 14 stemmen en 1 onthouding.

HOOFDSTUK 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

Art. 5 tot 7

De artikelen 5 tot 7 worden achtereenvolgens aangenomen met 10 stemmen en 5 onthoudingen.

HOOFDSTUK 3

Nationale cyberbeveiligingscertificeringsautoriteit

Art. 8 en 9

De artikelen 8 en 9 worden achtereenvolgens aangenomen met 14 stemmen en 1 onthouding.

HOOFDSTUK 4

Afgifte van Europese certificaten

Art. 10 tot 12

De artikelen 10 tot 12 worden achtereenvolgens aangenomen met 14 stemmen en 1 onthouding.

CHAPITRE 5

Contrôle

Art. 13

L'article 13 est adopté par 10 voix et 5 abstentions.

Art. 14

L'article 14 est adopté par 14 voix et 1 abstention.

Art. 15 à 17

Les articles 15 à 17 sont successivement adoptés par 10 voix et 5 abstentions.

Art. 18

L'article 18 est adopté par 14 voix et 1 abstention.

CHAPITRE 6

Sanctions

Art. 19 et 20

Les articles 19 et 20 sont successivement adoptés par 12 voix et 3 abstentions.

Art. 21 et 22

Les articles 21 et 22 sont successivement adoptés par 14 voix et 1 abstention.

Art. 23 et 24

Les articles 23 et 24 sont successivement adoptés par 12 voix et 3 abstentions.

Art. 25 à 28

Les articles 25 à 28 sont successivement adoptés par 10 voix et 5 abstentions.

HOOFDSTUK 5

Toezicht

Art. 13

Artikel 13 wordt aangenomen met 10 stemmen en 5 onthoudingen.

Art. 14

Artikel 14 wordt aangenomen met 14 stemmen en 1 onthouding.

Art. 15 tot 17

De artikelen 15 tot 17 worden achtereenvolgens aangenomen met 10 stemmen en 5 onthoudingen.

Art. 18

Artikel 18 wordt aangenomen met 14 stemmen en 1 onthouding.

HOOFDSTUK 6

Sancties

Art. 19 en 20

De artikelen 19 en 20 worden achtereenvolgens aangenomen met 12 stemmen en 3 onthoudingen.

Art. 21 en 22

De artikelen 21 en 22 worden achtereenvolgens aangenomen met 14 stemmen en 1 onthouding.

Art. 23 en 24

De artikelen 23 en 24 worden achtereenvolgens aangenomen met 12 stemmen en 3 onthoudingen.

Art. 25 tot 28

De artikelen 25 tot 28 worden achtereenvolgens aangenomen met 10 stemmen en 5 onthoudingen.

CHAPITRE 7

Réclamations

Art. 29 à 35

Les articles 29 à 35 sont successivement adoptés par 14 voix et 1 abstention.

CHAPITRE 8

Traitements des données à caractère personnel

Art. 36 à 38

Les articles 36 à 38 sont successivement adoptés par 12 voix et 3 abstentions.

CHAPITRE 9

Dispositions modificatives

Art. 39 à 46

Les articles 39 à 46 sont successivement adoptés par 12 voix et 3 abstentions.

Art. 47

L'article 47 est adopté par 14 voix et 1 abstention.

Art. 48

L'article 48 est adopté par 12 voix et 3 abstentions.

Art. 49

L'article 49 est adopté par 14 voix et 1 abstention.

Art. 50 et 51

Les articles 50 et 51 sont successivement adoptés par 12 voix et 3 abstentions.

HOOFDSTUK 7

Klachten

Art. 29 tot 35

De artikelen 29 tot 35 worden achtereenvolgens aangenomen met 14 stemmen en 1 onthouding.

HOOFDSTUK 8

Verwerking van persoonsgegevens

Art. 36 tot 38

De artikelen 36 tot 38 worden achtereenvolgens aangenomen met 12 stemmen en 3 onthoudingen.

HOOFDSTUK 9

Wijzigingsbepalingen

Art. 39 tot 46

De artikelen 39 tot 46 worden achtereenvolgens aangenomen met 12 stemmen en 3 onthoudingen.

Art. 47

Artikel 47 wordt aangenomen met 14 stemmen en 1 onthouding.

Art. 48

Artikel 48 wordt aangenomen met 12 stemmen en 3 onthoudingen.

Art. 49

Artikel 49 wordt aangenomen met 14 stemmen en 1 onthouding.

Art. 50 en 51

De artikelen 50 en 51 worden achtereenvolgens aangenomen met 12 stemmen en 3 onthoudingen.

CHAPITRE 10

Entrée en vigueur

Art. 52

L'article 52 est adopté par 14 voix et 1 abstention.

*
* *

À la demande de M. Erik Gilissen (VB), la commission décide, en application de l'article 83.1 du Règlement, de procéder à une deuxième lecture. Elle souhaite à cet effet disposer d'une note de légistique du Service juridique.

La rapporteure, *Le président,*

Leslie LEONI Stefaan VAN HECKE

HOOFDSTUK 10

Inwerkingtreding

Art. 52

Artikel 52 wordt aangenomen met 14 stemmen en 1 onthouding.

*
* *

Op verzoek van de heer Erik Gilissen (VB) beslist de commissie, met toepassing van artikel 83.1 van het Reglement, over te gaan tot een tweede lezing. Zij wenst daartoe te beschikken over een wetgevingstechnische nota van de Juridische Dienst.

De rapportrice, *De voorzitter,*

Leslie LEONI Stefaan VAN HECKE

Imprimerie centrale – Centrale drukkerij