DOC 54 **2109/023**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

15 december 2016

ONTWERP VAN ALGEMENE UITGAVENBEGROTING

voor het begrotingsjaar 2017

ADVIES

over sectie 05 – FOD Informatietechnologie en Communicatie (*partim*: Fedict)

VERSLAG

NAMENS DE COMMISSIE VOOR DE BINNENLANDSE ZAKEN, DE ALGEMENE ZAKEN EN HET OPENBAAR AMBT UITGEBRACHT DOOR MEVROUW **Katja GABRIËLS**

INHOUD Blz.

Zie:

Doc 54 **2109/ (2016/2017):**
001: Ontwerp van Algemene Uitgavenbegroting (eerste deel).
002: Ontwerp van Algemene Uitgavenbegroting (tweede deel).
003: Amendementen.
004: Verslag.
005: Amendement.
006 tot 008: Verslagen.
009: Amendementen.
010 en 022: Verslagen.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

15 décembre 2016

PROJET DU BUDGET GÉNÉRAL DES DÉPENSES

pour l'année budgétaire 2017

AVIS

sur la section 05 – SPF Technologie de l'Information et de la Communication (*partim*: Fedict)

RAPPORT

FAIT AU NOM DE LA COMMISSION DE L'INTÉRIEUR, DES AFFAIRES GÉNÉRALES ET DE LA FONCTION PUBLIQUE PAR MME **Katja GABRIËLS**

SOMMAIRE Pages

Voir:

Doc 54 **2109/ (2016/2017):**
001: Projet du Budget général de dépenses (première partie).
002: Projet du Budget général de dépenses (deuxième partie).
003: Amendements.
004: Rapport.
005: Amendement.
006 à 008: Rapports
009: Amendements.
010 et 022: Rapports.

Samenstelling van de commissie op de datum van indiening van het verslag/
Composition de la commission à la date de dépôt du rapport
Voorzitter/Président: Brecht Vermeulen

A. — Vaste leden / Titulaires:

N-VA	Christoph D'Haese, Koenraad Degroote, Koen Metsu, Brecht Vermeulen
PS	Nawal Ben Hamou, Willy Demeyer, Eric Thiébaut
MR	Denis Ducarme, Philippe Pivin, Françoise Schepmans
CD&V	Franky Demon, Veerle Heeren
Open Vld	Katja Gabriëls, Sabien Lahaye-Battheu
sp.a	Monica De Coninck
Ecolo-Groen	Gilles Vanden Burre
cdH	Vanessa Matz

B. — Plaatsvervangers / Suppléants:

Peter Buysrogge, Renate Hufkens, Sarah Smeyers, Valerie Van Peel, Jan Vercammen
Laurent Devin, André Frédéric, Emir Kir, Laurette Onkelinx
Sybille de Coster-Bauchau, Emmanuel Burton, Caroline Cassart-Mailleux, Stéphanie Thoron
Leen Dierick, Nahima Lanjri, Veli Yüksel
Patrick Dewael, Annemie Turtelboom, Vincent Van Quickenborne
Hans Bonte, Alain Top
Wouter De Vriendt, Stefaan Van Hecke
Christian Brotcorne, Isabelle Poncelet

C. — Niet-stemgerechtigde leden / Membres sans voix délibérative:

VB	Filip Dewinter
DéFI	Olivier Maingain
PP	Aldo Carcaci

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*
Vuye&Wouters	:	*Vuye&Wouters*

Afkortingen bij de nummering van de publicaties:

DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag*
CRABV:	*Beknopt Verslag*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*

Abréviations dans la numérotation des publications:

DOC 54 0000/000:	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Compte Rendu Analytique*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

Dames en Heren,

Uw commissie heeft sectie 05 – FOD Informatietechnologie en Communicatie (*partim*: Fedict) van het ontwerp van Algemene Uitgavenbegroting voor het begrotingsjaar 2017, met inbegrip van de verantwoording en de beleidsnota (DOC 54 2109/001, 2110/006 en 2111/003), besproken tijdens haar vergadering van 7 december 2016.

I. — INLEIDENDE UITEENZETTING VAN DE VICE-EERSTEMINISTER EN MINISTER VAN ONTWIKKELINGSSAMENWERKING, DIGITALE AGENDA, TELECOMMUNICATIE EN POST

De heer Alexander De Croo, vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post, gaat in op enkele elementen uit de beleidsnota over de Digitale agenda 2017 die betrekking hebben op de digitale overheid.

Eén van die aspecten is de omvorming van Fedict naar het "*Digital Transformation Office*" (DOC 54 2111/003, blz. 14). Fedict is vandaag de dag vooral een IT-implementatieorgaan. In de toekomst zal het veeleer een beleidsorgaan zijn dat strategisch en coördinerend werkt. Het zal een IT-planning opstellen voor de verschillende FOD's en zal mee de standaarden voor de werking definiëren. Die meer uniforme manier van werken zal ook de burger ten goede komen.

Daarnaast is er ook de lancering van de G-Cloud (DOC 54 2111/003, blz. 14). Die gemeenschappelijke *cloud*-omgeving zal een einde stellen aan het bestaan van de verschillende datacenters bij de federale overheidsinstellingen. De architectuur van de nieuwe omgeving zal er tegelijk voor zorgen dat ook de private sector er makkelijk toe kan bijdragen.

MyBelgium wordt een belangrijk onderdeel van het beleid rond de digitalisering (DOC 54 2111/003, blz. 15). Tegen 2020 moet het de standaard zijn dat elke communicatie met de overheid elektronisch gebeurt, tenzij men nadrukkelijk kiest voor een papieren procedure. Op dit ogenblik biedt *MyBelgium* toegang tot meer dan 50 verschillende overheidsdiensten. Dat gebeurt echter veelal op een weinig gecoördineerde manier. Er komt bijgevolg een upgrade van het bestaande portaal naar "*MyBelgium Next Generation*", met als doel om niet alleen te zorgen voor een hogere kwaliteit en gebruiksvriendelijkheid, maar bovenal voor een grotere uniformiteit.

Mesdames, Messieurs,

Votre commission a examiné la section 05 – SPF Technologie de l'Information et de la Communication (*partim*: Fedict) du projet de budget général des dépenses pour l'année budgétaire 2017, en ce compris la justification et la note de politique générale (DOC 54 2109/001, 2110/006 et 2111/003) au cours de sa réunion le 7 décembre 2016.

I. — EXPOSÉ INTRODUCTIF DU VICE-PREMIER MINISTRE ET MINISTRE DE LA COOPÉRATION AU DÉVELOPPEMENT, DE L'AGENDA NUMÉRIQUE, DES TÉLÉCOMMUNICATIONS ET DE LA POSTE

M. Alexander De Croo, vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste, se penche sur quelques éléments de la note de politique générale sur l'Agenda numérique 2017 qui concernent les pouvoirs publics numériques.

L'un de ces aspects est la transformation de Fedict en un "*Digital Transformation Office*" (DOC 54 2111/003, p. 14). À l'heure actuelle, Fedict est surtout un organe d'implémentation IT. À l'avenir, il deviendra plutôt un organe stratégique de coordination. Il établira un planning IT pour les différents SPF et participera à la définition des normes de fonctionnement. Cette manière de travailler plus uniforme profitera également au citoyen.

Il y a par ailleurs aussi le lancement du G-Cloud (DOC 54 2111/003, p. 14). Cet environnement *cloud* commun mettra fin à l'existence des différents centres de données au sein des services publics fédéraux. L'architecture du nouvel environnement sera également telle que le secteur privé pourra, lui aussi, y contribuer.

MyBelgium devient une partie importante de la politique en matière de numérisation (DOC 54 2111/003, p. 15). D'ici 2020, la norme doit être que toute communication avec les pouvoirs publics s'effectue par la voie électronique, sauf si l'on opte expressément pour une procédure papier. Actuellement, *MyBelgium* donne accès à plus de 50 services publics différents. Cela se fait cependant souvent d'une manière peu coordonnée. Il y aura par conséquent un upgrade du portail actuel vers un portail "*MyBelgium Next Generation*", avec pour objectif de veiller non seulement à améliorer la qualité et la convivialité du service, mais avant tout à assurer une plus grande uniformité.

Vervolgens zal ook worden gestreefd naar een maximaal gebruik van intelligente webformulieren (*Intelligent Web Forms*) (DOC 54 2111/003, blz. 18). Dat betekent dat de formulieren zoveel mogelijk vooraf ingevuld zullen zijn met data die afkomstig zijn van authentieke bronnen. Die manier van werken kadert binnen het "*only once*"-principe. Dat is de regel waarbij de overheid aan de burger een bepaald gegeven slechts eenmaal vraagt en vervolgens zelf maximaal hergebruikt.

Daarnaast komt er een wetswijziging die de mobiele identiteit en authenticatie mogelijk zal maken (DOC 54 2111/003, blz. 16). Het gaat daarbij om de extensie van de elektronische identiteitskaart naar de smartphone. De meeste mobiele telefoontoestellen beschikken thans over de mogelijkheid om gebruik te maken van een authenticatie-element. Die extensie is tot op heden te weinig gebruikt. Dat zal in de toekomst wel gebeuren, waardoor de burger met zijn smartphone toegang zal hebben tot alle overheidswebsites. Het valt te vergelijken met de mogelijkheid die reeds bestaat om in plaats van de bakjes, die vandaag de dag worden gebruikt voor bankverrichtingen met de computer, gebruik te maken van een smartphone. De reacties van de gebruikers daarvan zijn alvast eenduidig positief.

De minister wijst voorts op het systeem van de elektronische brievenbus (*e-Box*) (DOC 54 2111/003, blz. 20), een communicatiemethode tussen de overheidsinstellingen, de ondernemingen en de burgers. Het is de bedoeling om dat systeem in de twee richtingen te gebruiken. Met de tool wordt het mogelijk de status van een document of communicatie na te gaan (verstuurd, ontvangen, gearchiveerd, enz.). Er zal worden gestreefd naar een maximale integratie ervan in de bestaande systemen, dit om parallelle werkmethodes te vermijden.

Het wettelijke kader voor de elektronisch aangetekende zending bestaat reeds (DOC 54 2111/003, blz. 20). Enkele marktparticipanten onderzoeken momenteel het gebruik ervan. Binnen het ecosysteem van de intelligente webformulieren en de *e-Box* zal de elektronisch aangetekende zending uiteraard haar belang opeisen. In 2017 zal worden nagegaan hoe ook enkele grote FOD's gebruik kunnen maken van de tool. De grootste verzendvolumes van aangetekende brieven vindt men vandaag terug bij de FOD Financiën en de FOD Justitie. Binnen die twee beleidsdomeinen liggen dus kansen om aanzienlijke winsten te boeken.

Ensuite, on s'efforcera également d'utiliser au maximum les formulaires web intelligents (*Intelligent Web Forms*) (DOC 54 2111/003, p. 18). Cela signifie que les formulaires seront pré-remplis dans la mesure du possible avec des données provenant de sources authentiques. Cette façon de procéder s'inscrit dans le cadre du principe "*Only Once*". C'est la règle en vertu de laquelle les autorités ne demandent qu'une seule fois une information au citoyen et la réutilisent par la suite au maximum.

Il est par ailleurs procédé à une modification de la loi qui permettra l'identité et l'authentification mobile (DOC 54 2111/003, p. 16). L'objectif est de procéder à une extension de la carte d'identité électronique au Smartphone. Les appareils téléphoniques les plus mobiles disposent aujourd'hui de la possibilité de recourir à un élément d'authentification. Cette extension a jusqu'ici trop peu été utilisée. Cela va changer à l'avenir, et le citoyen aura accès à tous les sites web publics grâce à son Smartphone. On peut comparer cela avec la possibilité qui existe déjà d'utiliser un Smartphone pour réaliser des opérations bancaires. Les réactions des utilisateurs sont unanimement positives.

Le ministre évoque ensuite le système de la boîte aux lettres électronique (*e-Box*) (DOC 54 2111/003, p. 20), un moyen de communication entre les organismes publics, les entreprises et les citoyens. L'objectif est d'utiliser ce système dans les deux sens. L'outil permettra de vérifier le statut d'un document ou d'une communication (envoyé, reçu, archivé, etc.). On s'efforcer d'intégrer au maximum ce système dans les systèmes existants, afin d'évither des méthodes de travail parallèles.

Le cadre légal de l'envoi recommandé électronique existe déjà (DOC 54 2111/003, p. 20). Plusieurs acteurs du marché en examinent actuellement l'utilisation. Dans le cadre de l'écosystème des formulaires web intelligents et de l'*e-Box*, l'envoi électronique recommandé aura en effet toute son importance. En 2017 on examinera comment plusieurs grands SPF peuvent également utiliser cet outil. Ce sont les SPF Finances et SPF Justice qui envoient aujourd'hui le plus grand volume de courriers recommandés. Il est donc possible de réaliser des gains considérables dans ces deux départements.

II. — **BESPREKING**

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

De heer Brecht Vermeulen (N-VA) wijst erop dat de snel evoluerende maatschappij gekenmerkt wordt door grote wijzigingen op vlak van werk, communicatie, informatiedeling, enz. De kennis en vooruitgang op vlak van ICT lijken onstuitbaar. Wat vandaag gloednieuw en hip is, wordt morgen al vervangen door een nog beter, performanter systeem.

In de huidige geglobaliseerde maatschappij is het cruciaal dat ook de overheid mee is om de competitiviteit van de bedrijven te faciliteren en om de dienstverlening en communicatie naar de burger vlotter, eenvoudiger en transparanter te laten verlopen.

Dat alles moet ook in een digitaal veilige omgeving gebeuren. Het Centrum voor Cybersecurity België (CCB) streeft ernaar om tegen 2020 van België een "*digital safe haven"* te maken. Het is belangrijk voor de burger en de bedrijven om op een veilige en betrouwbare manier gebruik te kunnen maken van het internet. Een goede samenwerking tussen de diensten van de minister en andere diensten zoals het CCB zullen daarbij van cruciaal belang zijn. Het CCB is belast met de uitwerking van een *cybersecurity*-strategie voor België, zowel op het vlak van de informatie- en netwerkveiligheid als inzake de strijd tegen de (georganiseerde) cybercriminaliteit. De beleidscel Digitale Agenda, Post en Telecom heeft in dat kader regelmatige contacten met het CCB als deel van de strijd tegen alle vormen van nationale en internationale cybercriminaliteit. Hoe verlopen deze contacten? Is er een vast overlegplatform? Zijn er functionele bevoegdheidsafspraken? Hoe versterken de diensten van de minister de strijd tegen de cybercriminaliteit?

Fedict geeft ook ondersteuning bij de omzetting van de Europese richtlijn inzake netwerk- en informatiebeveiliging. Ook hier is een samenwerking met het CCB van belang, aangezien het mee bevoegd is voor de omzetting van de NIS-richtlijn. Wat is de concrete verdeling is tussen het CCB en de diensten van de minister? Welke ondersteuning bieden zijn diensten concreet? De aanbieders van essentiële diensten en sommige digitale dienstverleners zullen met de omzetting van de richtlijn onderworpen worden aan vereisten inzake de veiligheid en de melding van veiligheidsincidenten. Heeft de minister zicht op het aantal meldingen van veiligheidsincidenten in dat kader?

II. — **DISCUSSION**

A. **Questions et observations des membres**

M. Brecht Vermeulen (N-VA) souligne que la société en évolution rapide se caractérise par de profondes mutations dans les domaines du travail, des communications, du partage de l'information, etc. Les connaissances et les progrès en matière de TIC semblent irrésistibles. Ce qui est aujourd'hui nouveau et *hip*, est remplacé dès demain par un système encore meilleur et plus performant.

Dans la société globalisée d'aujourd'hui il est crucial que les jouent leur rôle en vue de faciliter la compétitivité des entreprises et de rendre les services et communications en faveur du citoyen encore plus simples et transparents.

Tout cela doit également se faire dans un environnement numérique sécurisé. Le Centre pour la cybersécurité Belgique (CCB) est chargé de faire de la Belgique un havre de sécurité numérique d'ici 2020. Il est important pour les citoyens et pour les entreprises de pouvoir utiliser l'internet d'une manière sûre et fiable. Une bonne collaboration entre les services du ministre et d'autres services comme le CCB revêtira une importance cruciale dans cette optique. Le CCB est chargé d'élaborer une stratégie de cybersécurité pour la Belgique, tant au niveau de la sécurité de l'information et des réseaux que pour la lutte contre la cybercriminalité (organisée). Dans le cadre de la lutte contre toutes les formes de cybercriminalité nationale et internationale, des contacts réguliers ont lieu entre le CCB et la cellule stratégique Agenda numérique, Télécoms et Poste. Comment ces contacts se déroulent-ils? Y a-t-il une plateforme de concertation permanente? Y a-t-il des accords fonctionnels en matière de compétences? Comment les services du ministre renforcent-ils la lutte contre la cybercriminalité?

Fedict apporte également son soutien à la transposition de la directive européenne sur la sécurité des réseaux et de l'information. Une collaboration avec le CCB s'avère ici aussi importante, dès lors qu'il est coresponsable de la transposition de la directive SRI. Quelle est la répartition concrète entre le CCB et les services du ministre? Quel soutien ses services proposent-ils concrètement? Les fournisseurs de services essentiels et certains fournisseurs de services numériques devront, à la suite de la transposition de la directive, respecter des conditions en matière de sécurité et de signalement d'incidents de sécurité. Le ministre peut-il préciser le nombre de signalements d'incidents de sécurité dans ce cadre?

Op het vlak van de digitale overheid werd reeds een aantal stappen gezet. Het aantal elektronische facturen is gestegen en er wordt ook gewerkt aan de modernisering van het Rijksregister. Het belang van open data en de uitwisseling van informatie zijn evenzeer aanzienlijk. De omstandigheden hebben aangetoond dat er nog steeds te weinig uitwisseling is van relevante en cruciale informatie. De overheid dient er bijzondere aandacht aan te besteden en er prioritair werk van te maken.

In de beleidsnota wordt gesteld dat naast de *Federal Authentication Service* (FAS) ook Fedict een autorisatieservice aanbiedt (DOC 54 2111/003, blz. 17). Wat is het verschil tussen beiden? Kan de autorisatieservice niet door één dienst gedaan worden?

Aan welke projecten zal Fedict prioriteit geven bij de uitrol ervan tijdens het komend beleidsjaar?

De heer Alain Top (sp.a) duidt aan dat de minister bij de start van de regeerperiode heeft aangegeven dat het de ambitie moet zijn dat de overheid na 5 jaar "*digital by default*" werkt. De communicatie met de overheid moet dan met andere woorden in principe digitaal zijn. De papieren documenten zullen blijven bestaan, doch slechts als uitzondering of op aanvraag.

Een dergelijke werkmethode zou een aanzienlijke efficiëntiewinst met zich mee kunnen brengen. *eGovernment* kan inderdaad voor tijdswinst en budgettaire efficiëntie zorgen. In het licht daarvan wijst de spreker op de *redesign* van de federale overheid. Fedict zal zijn personeels- en werkingskredieten overdragen in het kader van de *redesign*. Thans blijkt echter dat de vooropgestelde doelstellingen van dat project niet worden bereikt. Heeft die vaststelling ook gevolgen voor het personeel en de werking van Fedict?

De spreker wijst er daarnaast op dat de cyberveiligheid en de strijd tegen de cybercriminaliteit belangrijke aandachtspunten vormen. In hoeverre wordt rond het thema voor een samenwerking gezorgd tussen alle overheidsinstellingen (het CCB, de FOD's, de deelstaten en de lokale besturen)? Hoe wordt gezorgd voor de veiligheid en de bescherming van het *eGovernment* en de identiteit van de burgers?

B. **Antwoorden van de minister**

De minister licht toe dat het CCB de strategie rond de cyberveiligheid moet uitstippelen, en tegelijk ook

Un certain nombre de pas ont déjà été effectués dans la direction des autorités numériques. Le nombre de factures électroniques a augmenté et le Registre national est en cours de modernisation. L'importance de données ouvertes et de l'échange d'informations est également à souligner. Les circonstances ont montré que l'on procède encore trop peu à l'échange d'informations pertinentes et cruciales. Les autorités doivent y prêter une attention toute particulière et en faire une priorité.

Dans la note de politique générale on peut lire qu'outre le *Service Fédéral d'Authentification* (FAS), Fedict offre lui aussi un service d'autorisation (DOC 54 2111/003, p. 17). Quelle est la différence entre les deux? Le service d'autorisation ne peut-il pas être pris en charge par un seul service?

Quels sont les projets auxquels Fedict compte accorder la priorité au niveau de leur mise en œuvre en 2017?

M. Alain Top (sp.a) indique que le ministre a annoncé, au début de l'actuelle législature, que l'ambition devait être d'avoir des pouvoirs publics "numériques par défaut" dans un délai de cinq ans. En d'autres termes, les communications avec les pouvoirs publics doivent en principe se faire par la voie numérique. Les documents papier subsisteront, mais à seulement à titre d'exception ou sur demande.

Une telle méthode de travail permettrait un gain d'efficacité considérable. *EGovernment* peut en effet permettre de gagner du temps et d'améliorer l'efficacité budgétaire. À la lumière de ces éléments, l'intervenant renvoie au projet *redesign* de l'administration fédérale. Dans le cadre de ce programme, Fedict transférera ses crédits de personnel et de fonctionnement. Pour l'instant, les objectifs posés dans le cadre de ce projet ne sont pas atteints. Ce constat a-t-il également des conséquences pour le personnel et le fonctionnement de Fedict?

Ensuite, l'intervenant souligne que la cybersécurité et la lutte contre la cybercriminalité constituent des points d'attention importants. Dans quelle mesure y a-t-il collaboration entre tous les organismes publics en la matière (le CCB, les SPF, les entités fédérées et les pouvoirs locaux)? Comment assure-t-on la sécurité et la protection d'*eGovernement* et de l'identité des citoyens?

B. **Réponses du ministre**

Le ministre explique que le CCB est chargé de définir la stratégie en matière de cybersécurité, mais que

een coördinatieorgaan is. Het is dus verantwoordelijk voor de coördinatie van de werkzaamheden van de talrijke instanties die rond het thema werken: de ADIV, de Veiligheid van de Staat, BelNIS, Belnet, het BIPT, CERT.be, de FCCU, enz. Het is logisch dat heel veel instanties met de problematiek te maken hebben.

De omvorming van Fedict naar het "*Digital Transformation Office*" is een onderdeel van de *redesign*. Het niet behalen van de doelstellingen van dat project heeft geen enkele impact op die transformatie. De ambitie van de digitalisering van de overheid ligt erin die laatste efficiënter te doen werken, alsook – en hierin ligt het verschil met de *redesign* – om de overheid beter te maken. Dat laatste komt neer op de vraag: hoe wordt ervoor gezorgd dat de dienstverlening naar de burger en de bedrijven verbetert? Met "beter" wordt bedoeld: maximaal gesteund op gegevens waarover men reeds beschikt ("*only once*"), een communicatie die meer toegespitst is op de beoogde doelgroep, enz. Dat is de specifieke invalshoek van het "*Digital Transformation Office*". Op budgettair vlak is er dus geen bijkomende impact buiten de reeds gemaakte algemeen geldende besparingsafspraken.

Bij de omzetting van de NIS-richtlijn neemt het BIPT de grootste rol voor zijn rekening, gelet op diens bevoegdheid voor de netwerkinfrastructuur. Fedict werkt er ook aan mee vanuit het perspectief van de overheidsnetwerken waarvoor het bevoegd is.

De richtlijn werd terecht onder de aandacht gebracht, gelet op het belang ervan. Een veiligheidssysteem is maar zo sterk als de zwakste schakel. Positief aan de richtlijn is dat zij zeer sterk de nadruk legt op de veiligheid bij kmo's. Die veiligheid is deels de verantwoordelijkheid van de overheid, maar ook deels die van de kmo's zelf. Net zoals de burger zijn woning goed moet afsluiten bij het verlaten ervan, moet ook een kmo zorg dragen voor haar eigen (cyber)veiligheid. De bijzondere aandacht van de richtlijn voor de kmo's is terecht, omdat zij doorgaans minder goed beveiligd zijn dan grote ondernemingen, en ook omdat hun systemen vaak een toegang verlenen tot de systemen van de grotere bedrijven, gelet op de informatie-uitwisseling tussen de kleinere en de grotere ondernemingen.

Wat het aantal veiligheidsmeldingen betreft, nodigt de minister de heer Vermeulen uit daarover een schriftelijke vraag in te dienen, waarna de data zullen worden opgevraagd, verzameld en ter beschikking gesteld.

c'est également un organe de coordination. Il est donc chargé de la coordination des travaux de nombreuses instances qui travaillent dans des domaines liés à la cybersécurité: le SGRS, la Sûreté de l'État, BelNIS, Belnet, l'IBPT, CERT.be, la FCCU, etc. Il est logique que de nombreuses instances soient concernées par cette problématique.

La transformation de Fedict en "*Digital Transformation Office*" s'inscrit dans le cadre du projet *redesign*. Le fait que les objectifs du projet ne soient pas atteints n'a aucune répercussion sur cette transformation. L'ambition de la politique de numérisation des autorités publiques est d'accroître l'efficacité de ces dernières, mais également – et c'est là toute la différence avec le projet *redesign* – d'améliorer l'action des autorités publiques. Ce dernier objectif tient en une question: comment faire pour assurer un meilleur service aux citoyens et aux entreprises? Par "meilleur", il y lieu d'entendre une exploitation optimale des données déjà disponibles ("*only once"*) et une communication davantage axée sur le groupe-cible visé, etc. C'est l'angle d'attaque spécifique du "*Digital Transformation Office"*. Sur le plan budgétaire, il n'y a donc aucune répercussion supplémentaire en dehors des accords de réduction de dépenses d'application générale déjà conclus.

Dans le cadre de la transposition de la directive SRI, c'est l'IBPT qui assure l'essentiel du travail, vu sa compétence en matière d'infrastructure réseau. Fedict y collabore également, compte tenu de sa compétence en matière de réseaux administratifs.

Il était justifié d'attirer l'attention sur cette directive, vu son importance. La force d'un système de sécurité se mesure à la force de son maillon le plus faible. Un élément positif de cette directive est qu'elle met très nettement l'accent sur la sécurité des PME. Tant les autorités que les PME elles-mêmes sont responsables de cette sécurité. Tout comme le citoyen doit bien fermer la porte de sa maison lorsqu'il la quitte, la PME doit également veiller à sa propre (cyber) sécurité. L'attention spécifique accordée aux PME dans cette directive est justifiée, car elles sont généralement moins bien protégées que les grandes entreprises, et car leurs systèmes permettent souvent d'accéder aux systèmes de plus grandes entreprises compte tenu de l'échange d'informations entre les petits et les grandes entreprises.

Concernant le nombre de signalements de problèmes de sécurité, le ministre invite M. Vermeulen à lui adresser une question écrite à ce propos, après quoi les données à ce sujet seront demandées, rassemblées et mises à disposition.

In verband met de autorisatie door de FAS en Fedict, legt de minister uit dat één element handelt over de toegang tot de federale overheidssites. Daarvoor is Fedict bevoegd. Daarnaast zijn er de privéauthentificatiediensten van de FAS. Uiteraard steunen de beide op dezelfde technologie.

C. **Repliek**

De heer Brecht Vermeulen (N-VA) gaat akkoord dat er voldoende aandacht moet zijn naar de cyberveiligheid van de kmo's. Grote bedrijven zijn veel meer in staat om zichzelf te beschermen. Uiteraard moeten ook de kmo's dus aandacht hebben voor hun veiligheid. Die zorg kan hen in de toekomst wellicht ook terugverdieneffecten opleveren, bijvoorbeeld in de vorm van lagere verzekeringspremies voor ICT-schade. De overheid moet er van haar kant voor zorgen dat die verantwoordelijkheid geen al te zware last om dragen wordt.

De spreker geeft aan te zullen nagaan of en welke wetgevende initiatieven op dat vlak aangewezen zijn. Zoals reeds vermeld, moet er bijvoorbeeld over gewaakt worden dat de voor- en nadelen minstens in evenwicht zijn.

III. — **ADVIES**

De commissie brengt met 9 stemmen en 3 onthoudingen een gunstig advies uit over sectie 05 – FOD Informatietechnologie en Communicatie (partim: Fedict) van het ontwerp van Algemene Uitgavenbegroting voor het begrotingsjaar 2017.

De rapporteur, *De voorzitter,*

Katja GABRIËLS Brecht VERMEULEN

Concernant l'autorisation délivrée par le FAS et Fedict, le ministre explique qu'un seul élément concerne l'accès aux sites publics fédéraux. Fedict est compétent en la matière. Il y a par ailleurs les services d'authentification privés du FAS. Ils recourent évidemment tous deux à la même technologie.

C. **Réplique**

M. Brecht Vermeulen (N-VA) est d'accord sur le fait qu'il convient de consacrer suffisamment d'attention à la cybersécurité des PME. Les grandes entreprises sont bien plus en mesure d'assurer leur propre sécurité. Il est très juste de souligner que les PME doivent dès lors également veiller à leur sécurité, ce qui se traduira sans doute plus tard par des retours sur investissements, sous la forme par exemple d'une diminution du montant des polices d'assurance ICT. De leurs côtés, les pouvoirs publics doivent veiller à ce que cette responsabilité ne devienne pas trop lourde à porter pour les PME.

L'intervenant indique qu'il examinera si des initiatives législatives sont indiquées en la matière et quelle forme elles pourraient prendre. Comme mentionné précédemment, il convient par exemple de veiller à ce qu'il y ait au moins un équilibre entre les avantages et les inconvénients.

III. — **AVIS**

La commission émet, par 9 voix et 3 abstentions, un avis favorable sur la section 05 – SPF Technologie de l'Information et de la Communication (*partim*: Fedict) du projet de budget général des Dépenses pour l'année budgétaire 2017.

La rapporteuse, *Le président,*

Katja GABRIËLS Brecht VERMEULEN

Centrale drukkerij – Imprimerie centrale