CRIV 55 **COM 738**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

# COMPTE RENDU INTÉGRAL
**AVEC**
**COMPTE RENDU ANALYTIQUE TRADUIT**
**DES INTERVENTIONS**

# INTEGRAAL VERSLAG
**MET**
**VERTAALD BEKNOPT VERSLAG**
**VAN DE TOESPRAKEN**

COMMISSION DE L'ÉCONOMIE, DE LA PROTECTION DES CONSOMMATEURS ET DE L'AGENDA NUMERIQUE

COMMISSIE VOOR ECONOMIE, CONSUMENTENBESCHERMING EN DIGITALE AGENDA

**Mercredi**

**23-03-2022**

**Après-midi**

**Woensdag**

**23-03-2022**

**Namiddag**

| | |
|---|---|
| *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 :* | | *Afkortingen bij de nummering van de publicaties* : | |
|---|---|---|---|
| *DOC 55 0000/000* | *Document parlementaire de la 55e législature, suivi du n° de base et du n° consécutif* | *DOC 55 0000/000* | *Parlementair stuk 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 définitif 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 (op beigekleurig 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*
*e-mail : publications@lachambre.be*

*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*

SOMMAIRE



INHOUD

# COMMISSION DE L'ÉCONOMIE, DE LA PROTECTION DES CONSOMMATEURS ET DE L'AGENDA NUMERIQUE

du

MERCREDI 23 MARS 2022

Après-midi

_____

# COMMISSIE VOOR ECONOMIE, CONSUMENTENBESCHERMING EN DIGITALE AGENDA

van

WOENSDAG 23 MAART 2022

Namiddag

_____

De openbare commissievergadering wordt geopend om 15.32 uur en voorgezeten door de heer Stefaan Van Hecke.
La réunion publique de commission est ouverte à 15 h 32 et présidée par M. Stefaan Van Hecke.

**01 Question de Daniel Senesael à Petra De Sutter (VPM Fonction publique et Entreprises publiques) sur "Les risques liés à l'eID" (55024227C)**
**01 Vraag van Daniel Senesael aan Petra De Sutter (VEM Ambtenarenzaken en Overheidsbedrijven) over "De risico's van de eID" (55024227C)**

01.01 **Daniel Senesael** (PS): L'identification en ligne via un lecteur de carte d'identité ou une application est un phénomène qui s'intensifie continuellement et ce, principalement depuis le déclenchement de la pandémie mondiale. En effet, ces outils possèdent de nombreux points positifs comme la réduction des contacts – ce qui va dans le bon sens – ou encore l'automatisation des procédures administratives. Par ailleurs, plusieurs ministres, dont Mme la ministre de l'Intérieur dans sa NPG, ont indiqué souhaiter accélérer la numérisation de l'identification des citoyens. Bien que l'objectif soit la simplification des démarches administratives, il ne faudrait pas oublier le fait que l'ensemble de la population belge n'a, toujours pas en 2022, un accès plein et direct aux outils numériques et informatiques requis pour une identification en ligne. Ainsi, et comme indiqué par Mme Verlinden, une phase de pré-étude concernant l'identité mobile a d'ores et déjà été réalisée par BOSA.

Mes questions sont donc les suivantes: pourriez-vous nous donner quelques précisions sur ces résultats préliminaires? Des risques pour la vie privée des citoyens ont-ils été identifiés? Quelles suites concrètes seront données à cette étude? Une analyse d'impact relative à la vie privée sera-t-elle établie ou l'a-t-elle déjà été? Quel est le calendrier à venir pour ce projet?

Que comptez-vous faire afin de ne délaisser aucune frange de la population en ce qui concerne l'identification en ligne sur les différentes plateformes fédérales? Le maintien d'un système d'identification "100% public" fait-il bien partie des options étudiées? Le cyberterrorisme n'arrêtant pas de gagner en dangerosité, comment pouvez-vous assurer la sécurité identitaire numérique de nos concitoyens? Comment collaborez-vous avec vos collègues afin de protéger l'identité numérique de nos concitoyens?

01.01 **Daniel Senesael** (PS): De online-identificatie met behulp van een identiteitskaartlezer of een app heeft veel voordelen, zoals de vermindering van onnodige contacten of de automatisering van administratieve procedures. Verscheidene ministers hebben de wens geuit de digitalisering van de identificatie van de burgers te bespoedigen. We mogen niet vergeten dat niet iedereen volledig en rechtstreeks toegang heeft tot IT-tools.

Wat zijn de resultaten van de voorstudie door BOSA over dit onderwerp? Werden er risico's voor de privacy van de burgers vastgesteld? Wat is het tijdpad voor dit project? Hoe wilt u voorkomen dat een deel van de bevolking uit de boot valt? Behoort het behoud van een volledig openbaar identificatiesysteem tot de mogelijke opties? Hoe kan de veiligheid gewaarborgd worden in het licht van het toenemend cyberterrorisme?

01.02 **Mathieu Michel**, secrétaire d'État: Votre question me permet de revenir sur un projet très particulier qui me tient à cœur, en l'occurrence le portefeuille digital. Comme vous l'avez dit, le SPF BOSA et le SPF Intérieur ont effectivement travaillé sur un *proof of concept* pour une identité numérique. – digital identity – mobile. Il s'agit de disposer d'une identité disponible sur un appareil informatique sans forcément recourir à un support physique. Ce *proof of concept* est parfaitement aligné avec la proposition de révision du règlement eIDAS.

Cette proposition européenne prévoit que chaque État membre devra mettre à disposition gratuitement pour les citoyens dans les 12 mois après l'entrée en vigueur du règlement eIDAS, prévu au plus tôt en 2023, un *European digital identity wallet*. Dans notre pays, ce sera le portefeuille digital belge qui répondra à ces standards.

Il se présentera sous la forme d'une application utilisable sur un *smartphone*, avec une identité numérique et des services d'identification permettant de s'authentifier sur des services en ligne. Cette pré-étude du SPF a validé les concepts généraux relatifs notamment à la protection de la vie privée et à la sécurité des données. Elle doit maintenant être suivie d'une analyse plus complète. En 2022, le SPF BOSA et le SPF Intérieur travailleront ensemble à l'élaboration de cette identité numérique qui offrira le même niveau de sécurité que la carte d'identité électronique. L'élaboration de ce portefeuille digital sera, bien entendu, accompagnée d'une analyse d'impact relative à la protection des données personnelles.

Pour rappel, le portefeuille digital doit permettre l'identification, par le biais d'un schéma d'identification électronique national qui a été notifié; le stockage et le partage d'attributs, tant en ligne que hors ligne et la création de signatures électroniques qualifiées. Il permettra également de donner aux citoyens et entreprises un accès aux données et services publics qui les concernent, mais également d'apporter plus de transparence et d'améliorer la confiance. Il contiendra donc l'identité électronique, le passeport, le permis de conduire, etc., mais donnera également accès à My e-Box, e-loket, eSafe, qui sont toutes des applications mises à disposition des citoyens. J'ai fixé à ces administrations comme objectif que chaque Belge puisse disposer d'un tel portefeuille digital dès 2023. Dans ce cadre, chaque citoyen aura le contrôle total de son portefeuille digital et de l'utilisation de ses données personnelles.

Dans ce processus de digitalisation de l'identité, il est hors de question de laisser certains citoyens sur le côté. Cette identité numérique est le fruit d'un choix délibéré et éclairé. Le portefeuille digital sera complémentaire aux services existants et chacun sera libre de l'utiliser. La carte d'identité et les documents annexes, tels qu'ils sont utilisés aujourd'hui, continueront d'exister en version papier aussi longtemps que nécessaire. De même, spécifiquement en matière d'identification en ligne, les besoins des différentes franges de la population sont pris en compte de manière constante. Plusieurs types de clé sont actuellement disponibles: l'eID, que tout le monde possède, mais qui nécessite un lecteur de carte; itsme®, pour les détenteurs de s*martphone*; mais également une clé qui ne nécessite que l'accès à une adresse électronique, à savoir une clé composée d'un code de sécurité à durée de validité limitée, envoyé par courriel.

01.02 Staatssecretaris **Mathieu Michel**: De FOD's BOSA en Binnenlandse Zaken hebben aan een *proof of concept* gewerkt voor een mobiele digitale identiteit, die volledig in de lijn ligt van het voorstel tot herziening van de eIDAS-verordening. Die bepaalt dat elke lidstaat gratis een elektronische portefeuille ter beschikking van de burgers moet stellen.

Het zal de vorm aannemen van een smartphoneapp met een digitale identiteit en identificatiediensten waarmee men zich online kan authenticeren. Middels die voorstudie werden de algemene concepten op het stuk van de bescherming van de privacy en de veiligheid van de gegevens gevalideerd.

In 2022 zullen de FOD's BOSA en Binnenlandse Zaken samenwerken met het oog gericht op de uitwerking van die digitale identiteit, die even veilig zal zijn als de elektronische identiteitskaart. Met de portefeuille moeten de burgers en de bedrijven zich kunnen identificeren, bepaalde gegevens kunnen opslaan en delen, geldige elektronische handtekeningen kunnen aanmaken en toegang kunnen krijgen tot publieke gegevens en overheidsdiensten.

Vanaf 2023 moet elke Belg over zo een portefeuille kunnen beschikken. Die zal complementair zijn met de bestaande diensten en het zal iedereen vrij staan om hem al dan niet te gebruiken. De identiteitskaart en de aanverwante documenten op papier zullen zolang als nodig beschikbaar blijven. Voor de online identificatie zal er met de behoeften van iedereen rekening gehouden worden. We werken aan bepaalde projecten om voor een gemakkelijke toegang tot die nieuwe tools te zorgen.

De digitale portefeuille is een

L'accessibilité pour tous à ces systèmes et le soutien à tous dans leurs démarches administratives est essentiel. Pour y parvenir de manière concrète, nous travaillons actuellement sur des projets que vous découvrirez dans les prochaines semaines, et qui visent vraiment à permettre l'accès de tous à ces nouveaux outils digitaux, pour autant qu'ils en fassent le choix.

À noter que, concernant le portefeuille numérique, il s'agit bien d'un projet de développement public. La gestion de l'identité reste une fonction régalienne. Le fournisseur de l'identité reste l'administration, mais des partenariats avec le secteur privé sont aussi envisagés pour des services dérivés.

Le système d'identification est développé, maintenu et opéré par le SPF BOSA et est utilisable par les administrations de tous les niveaux de pouvoir. Les principales clefs numériques sont la propriété du secteur public, mais le système intègre également des clefs du secteur privé, tel Itsme que je viens de citer. Cela permet d'offrir toute une palette de clefs conviviales, sécurisées et adaptées aux besoins de chacun.

Enfin, pour ce qui concerne la sécurité du système d'identification en ligne, les applications et les informations sont sécurisées suivant une politique de sécurité de l'information régulièrement mise à jour. Des analyses et des audits sont régulièrement réalisés en collaboration avec le Centre pour la cybersécurité en Belgique et permettent d'améliorer constamment la sécurité.

Le projet de portefeuille numérique suivra les mêmes prescriptions et, en outre, il devra être certifié selon les exigences du règlement eIDAS, comme je l'énonçais auparavant.

ontwikkelingsproject van de overheid. Identiteitsbeheer blijft een regale functie: de administratie is de verstrekker van de identiteit, hoewel er voor afgeleide diensten partnerschappen met de privésector overwogen worden.

Het identificatiesysteem wordt ontwikkeld en geïmplementeerd door de FOD BOSA, DG Digitale Transformatie. Elke administratie kan er gebruik van maken. De belangrijkste digitale sleutels zijn eigendom van de publieke sector maar in het systeem worden er ook sleutels van de privésector geïntegreerd.

Toepassingen en gegevens worden online beschermd volgens een regelmatig bijgewerkt veiligheidsprotocol. Het project van de digitale portefeuille zal aan dezelfde voorschriften moeten beantwoorden en ook gecertificeerd moeten worden volgens de eisen uit de eIDAS-verordening.

01.03 **Daniel Senesael** (PS): Monsieur le secrétaire d'État, qu'il me soit permis de vous adresser mes remerciements, puisque voilà une réponse complète, précise et structurée et qui répond à toutes mes interrogations.

C'est un projet important que vous avez bien détaillé. Je ne manquerai pas de suivre le dossier et de revenir vers vous au cours du second semestre pour en connaître l'état d'avancement.

Je me réjouis de l'arrivée de mon collègue du PS. Notre parti est en masse, monsieur le président!

Le **président**: C'est vraiment l'armée PS qui est arrivée dans notre commission.

*L'incident est clos.*
*Het incident is gesloten.*

Vraag nr. 55024728C van mevrouw Verhaert wordt omgezet in een schriftelijke vraag.

**02 Questions jointes de**
**- Patrick Prévot à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Le virus informatique BRATA" (55024889C)**
**- Kattrin Jadin à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'hameçonnage" (55025068C)**
**02 Samengevoegde vragen van**
**- Patrick Prévot aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie**

**der Gebouwen) over "Het computervirus BRATA" (55024889C)**
**- Kattrin Jadin aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Phishing" (55025068C)**

Mme Jadin est absente.

02.01 **Patrick Prévot** (PS): Monsieur le président, monsieur le secrétaire d'État, un logiciel malveillant nommé BRATA circule depuis trois ans sur le web.

Conçu comme un cheval de Troie, il a d'abord commencé à se propager sur le Google Play Store en tant que fausse mise à jour de WhatsApp auprès des utilisateurs d'Android au Brésil; 10 000 personnes auraient été lésées.

À l'instar du covid, ce virus informatique s'est ensuite exporté jusqu'en Europe et a muté pour s'attaquer cette fois aux données des applications bancaires européennes, les *hackers* imitant à la perfection les logos des grandes agences. BRATA serait ainsi capable de récupérer des informations sensibles afin de voler de l'argent sur un compte bancaire et de rendre un smartphone Android inutilisable après son passage.

Selon certains sources, BRATA sévit depuis le mois de décembre au Royaume-Uni, en Pologne et en Italie. Il devrait logiquement s'étendre à d'autres pays.

Monsieur le secrétaire d'État, avez-vous connaissance d'utilisateurs d'Android victimes du virus BRATA en Belgique, attestant de sa circulation dans notre pays? Avez-vous une stratégie de contre-attaque contre BRATA, éventuellement en concertation avec les autres pays européens également touchés par ce logiciel? Je vous remercie.

02.01 **Patrick Prévot** (PS): Sinds drie jaar waart een kwaadaardig softwareprogramma met de naam BRATA rond op het internet. Dat Trojaanse paard verspreidde zich in de Google Play Store als een nepupdate die 10.000 Brazilianen schade berokkende, kwam daarna Europa binnen en muteerde om banktoepassingen aan te vallen. Via BRATA zou men gevoelige informatie kunnen buitmaken om geld van een bankrekening te stelen en een Android-smartphone onbruikbaar te maken.

Hebt u weet van slachtoffers in ons land? Hebt u een strategie voor een tegenaanval?

02.02 **Mathieu Michel**, secrétaire d'État: Monsieur le député, merci pour votre question. Avant toute chose, avant de rentrer dans la réponse à proprement parler, je voudrais vraiment préciser qu'aujourd'hui, en fait, dans le domaine de la sécurité digitale, nous sommes tous acteurs de cette sécurité. En effet, la cybersécurité ou la sécurité digitale de façon globale concerne tant les PME que les services de police et services gouvernementaux. C'est un élément qu'il est essentiel d'avoir en tête.

En dépit du fait que la vigilance des citoyens porte de plus en plus ses fruits, le *phishing* continue de faire de nombreuses victimes. En 2020, la police fédérale a constaté une augmentation de 204 % du nombre de victimes de *phishing* par rapport à 2009, avec un total de 7 502 signalements. Je ne parle ici que des signalements.

En 2020, les cybercriminels ont effectué 67 000 transactions frauduleuses, pour un montant net total de 34 millions d'euros. En outre, il s'avère que 12 % des Belges n'ont jamais entendu parler du *phishing*. Chez les jeunes, ce pourcentage atteint même parfois les 30 %, selon les chiffres de Febelfin en 2020.

Ainsi, parmi les risques de *phishing*, on peut relever le virus BRATA que vous citez dans votre question. C'est un logiciel malveillant qui est capable, entre autres, de voler des données

02.02 Staatssecretaris **Mathieu Michel**: Wij hebben allemaal belang bij digitale veiligheid. Burgers zijn steeds meer op hun hoede, maar phishing blijft zijn tol eisen. De federale politie stelde een stijging vast van 204 % ten opzichte van 2019 en 7.502 meldingen. Criminelen hebben 67.000 frauduleuze transacties verricht, ter waarde van 34 miljoen euro. Bovendien heeft 12 % van de Belgen nog nooit van phishing gehoord (en zelfs 30 % van de jongeren).

Het BRATA-virus is een van die praktijken. Spanje, de Verenigde Staten en, sinds december 2021, het Verenigd Koninkrijk, Polen, Italië en Latijns-Amerika, aangevoerd door Brazilië, werden er al door getroffen.

personnelles sensibles, y compris des codes pin, des mots de passe, des coordonnées GPS, et de capter les données liées aux applications bancaires installées sur l'appareil de la victime.

Parmi les pays visés, on compte l'Espagne, les États-Unis et, depuis décembre 2021, le Royaume-Uni, la Pologne, l'Italie et l'Amérique latine, avec le Brésil en tête.

À ce jour et selon les chiffres du CCB, aucune victime n'a été signalée en Belgique. Le CCB n'a reçu aucun signalement à ce sujet et les sources commerciales faisant le suivi des logiciels malveillants ne font pas état de cas en Belgique. Dès 2019, Google a bloqué ce *malware,* ce qui signifie qu'il ne peut plus être téléchargé sur Google Play Store par les appareils équipés d'un système Android. Toutefois, BRATA continue à se propager via des messages de *phishing* envoyés par sms.

Aujourd'hui, la stratégie de lutte contre ce type de virus repose principalement sur la sensibilisation des utilisateurs. En effet, le champ d'action va de la vulnérabilité humaine aux mesures technologiques de pointe. Plusieurs mesures préventives peuvent être prises pour éviter la propagation de ce virus ou tout autre *malware*:
- ne pas télécharger d'applications mobiles dont le développeur n'est pas clairement identifié;
- ne jamais télécharger d'application via un hyperlien reçu via un sms suspect;
- s'assurer que les autorisations qu'une application demande sont conformes à l'objectif de l'application;
- ne jamais diminuer la sécurité de son appareil à la demande d'une application;
- s'assurer que toutes les applications et logiciels d'un appareil sont mis à jour avec les dernières pages de sécurité;
- installer un bon anti-*malware* à jour et activer la protection en temps réel ou encore, si un utilisateur en est infecté, désactiver les applications ayant des privilèges de gestion et désinstaller ces applications en mode sans échec et réinitialiser son appareil.

Je me rends compte que ma réponse est très précise quant au *vade-mecum* du parfait protecteur en sécurité digitale.

En outre, le CCB a créé une adresse mail vers laquelle le citoyen peut envoyer des messages suspects, qu'il s'agisse d'emails ou de sms: suspect@safeonweb.be, adresse mail communiquée allègrement par le CCB. Il est possible de faire bloquer, via ses adresses mail, les liens suspects dans ces messages. En 2021, le CCB a reçu 4,5 millions de messages suspects provenant d'alertes de citoyens, soit en moyenne près de 12 000 messages par jour. Il a ainsi été en mesure de notifier plus de 1,4 million de sites internet frauduleux à Google et Microsoft qui les ont bloqués. En 2020, il y avait encore près de 3,2 millions de messages reçus par le CCB et 667 000 sites bloqués.

De même, le CCB envoie environ 27 000 redirections par jour vers une page sécurisée, après les clics par les utilisateurs belges sur des liens malicieux. Si une personne vient à cliquer sur un lien malicieux, elle recevra un message d'alerte clair lui signalant de ne pas surfer sur cette page. De cette manière, chacun peut contribuer à un

Het Centrum voor Cybersecurity Belgium (CCB) heeft geen enkele melding ontvangen en de commerciële bronnen die de malware monitoren signaleren geen gevallen in ons land. Sinds 2019 kan die malware niet meer op Google Play Store worden gedownload. BRATA blijft zich echter verspreiden via phishing sms'en.

De strijd tegen dit virustype berust voornamelijk op sensibilisering. Er moet toegezien worden op de bronnen en op de informatie die verstrekt worden vóór het downloaden van mobiele apps en men moet ervoor zorgen dat men over een efficiënt en geüpdatet veiligheidssysteem beschikt.

Het CCB heeft een mailadres gecreëerd waarnaar verdachte berichten kunnen worden gestuurd. In 2021 heeft het CCB 4,5 miljoen berichten ontvangen die door gealarmeerde burgers werden doorgestuurd en heeft het meer dan 1,4 miljoen frauduleuze websites aan Google en Microsoft gemeld, die ze geblokkeerd hebben. In 2020 heeft het CCB bijna 3,2 miljoen berichten ontvangen en werden er 667.000 websites geblokkeerd. Het CCB doet dagelijks ongeveer 27.000 redirects naar een beveiligde pagina met een duidelijke informatieboodschap nadat gebruikers op kwaadaardige links hadden geklikt.

environnement numérique sécurisé.

02.03 **Patrick Prévot** (PS): Monsieur le secrétaire d'État, je vous remercie pour votre réponse complète. Vous avez raison de le signaler, la cybersécurité concerne tout le monde. Dans un monde idéal, il faudrait encore accroître la sensibilisation du grand public. En effet, il ne se passe pas une semaine sans qu'un de nos contacts se laisse prendre au piège, tantôt en cliquant sur un lien qui a pour but de pénétrer dans ses réseaux sociaux, tantôt pour hameçonner ou récolter des données, mêmes bancaires.

Pour en revenir au logiciel malveillant BRATA, je suis content d'entendre que notre pays semble pour l'instant épargné. C'est en tout cas ce que vous a confirmé le Centre pour la cybersécurité Belgique (CCB), puisqu'il n'y a eu aucune plainte. Pour le reste, nous devons rester vigilants et continuer à avoir de vraies mesures contraignantes et structurelles pour lutter pour la cybersécurité. Il faut aussi accroître la sensibilisation du grand public afin que nous soyons tous des acteurs de cette cybersécurité, sans nous faire prendre au piège aussi facilement.

02.03 **Patrick Prévot** (PS): We zouden het grote publiek meer moeten sensibiliseren, want er gaat geen week voorbij zonder dat een van onze contacten in de val loopt. Het verheugt me dat het computervirus BRATA blijkbaar nog niet in ons land toegeslagen heeft. We moeten waakzaam blijven en bindende en structurele maatregelen nemen om onze cyberveiligheid te vrijwaren.

*L'incident est clos.*
*Het incident is gesloten.*

De **voorzitter**: Vraag nr. 55025421C van mevrouw Dierick wordt uitgesteld.

*La réunion publique de commission est levée à 15 h 49.*
*De openbare commissievergadering wordt gesloten om 15.49 uur.*