

Commission de l'Économie, de la
Protection des consommateurs et
de l'Agenda numérique

Commissie voor Economie,
Consumentenbescherming en
Digitale Agenda

du

van

MERCREDI 8 MARS 2023

WOENSDAG 8 MAART 2023

Après-midi

Namiddag

De openbare commissievergadering wordt geopend om 13.39 uur en voorgezeten door de heer Stefaan Van Hecke.

La réunion publique de commission est ouverte à 13 h 39 et présidée par M. Stefaan Van Hecke.

Les textes figurant en italique dans le Compte rendu intégral n'ont pas été prononcés et sont la reproduction exacte des textes déposés par les auteurs.

De teksten die in cursief zijn opgenomen in het Integraal Verslag werden niet uitgesproken en steunen uitsluitend op de tekst die de spreker heeft ingediend.

01 **Vraag van Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Cybersecurity" (55033396C)**

01 **Question de Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "La cybersécurité" (55033396C)**

01.01 **Erik Gilissen** (VB): Mijnheer de voorzitter, mijnheer de staatssecretaris, een goede beschermingsstrategie is van essentieel belang voor alle organisaties, zowel voor scholen als voor bedrijven en lokale besturen. Bij een onvoldoende weerbaarheid vormen die immers een gemakkelijke prooi voor ransomwareaanvallen.

De bescherming komt met een aanzienlijk kostenplaatje. Dus wordt de afweging gemaakt tussen de graad van bescherming en het beschikbare budget. Idealiter zijn de IT-systemen na een aanval meteen opnieuw volledig operationeel, maar dat kost handenvol geld.

Daarom opteren veel organisaties voor back-upsystemen, waarbij het herstel veel langer op zich laat wachten. Een dergelijke back-upstrategie moet er ook rekening mee houden dat de downtime van de facturatie bijvoorbeeld niet langer uitvalt dan de cashflow toelaat.

Mijn vragen zijn de volgende.

Hoeveel cyberincidenten werden in 2022 gerapporteerd bij grote ondernemingen, kmo's, scholen en lokale besturen? Hoeveel van die organisaties beschikken over een cyberverzekering? Welke controles zijn er op de degelijkheid van hun databeschermingsstrategieën? In welke mate staat het risico van ransomwareaanvallen de digitale transformatieplannen van organisaties in de weg? Ten slotte, hoeveel organisaties rapporteren moeilijkheden na de heropstart van hun IT-systemen?

01.02 Staatssecretaris **Mathieu Michel**: Mijnheer de voorzitter, mijnheer Gilissen, ik dank u voor uw vraag. Na het Centre for Cybersecurity Belgium te hebben geraadpleegd, kan ik u het volgende mededelen.

Inzake het aantal cyberaanvallen heeft in 2022 het federaal Computer Emergency Response Team of het CERT, zijnde de operationele dienst van het CCB, 24 grote cyberaanvallen behandeld waarvoor technische bijstand werd gevraagd. Het ging om drie aanvallen bij lokale besturen, elf aanvallen bij administratieve diensten, vier aanvallen bij ziekenhuizen en zes aanvallen bij diverse industrieën.

Deze gegevens houden geen rekening met meldingen en/of adviezen van het CCB die een cyberaanval

tegenhielden of kleinschaliger waren. Er is geen informatie over het aantal organisaties met een cyberverzekering. Audits van gegevensbeschermingsstrategieën zijn momenteel slechts beperkt vereist. In het kader van de NIS-verordening zijn verplichtingen opgelegd die door de sectorale autoriteiten worden gecontroleerd.

Daarnaast is er nu een vrijwillige ISO 27001-certificeringsregeling, waarmee bedrijven de omvang van hun informatiebeveiligingsmaatregelen kunnen aantonen. Het CCB houdt, als bevoegde autoriteit, toezicht op de certificeringsinstanties die deze certificering onder accreditatie aanbieden.

Om verschillende belanghebbenden, zoals bedrijven, overheden en andere organisaties, in staat te stellen hun gegevensbeschermingsstrategieën op evenredige wijze te ontwikkelen, heeft het CCB het cyberfundamentalskader ontwikkeld en openbaar gemaakt. Dit kader moet bedrijven niet alleen in staat stellen hun cyberveiligheid te verbeteren, maar ook om in de toekomst de robuustheid van de beschermingsmaatregelen te controleren en aan te tonen aan klanten en overheden, door middel van een geaccrediteerde nalevingsbeoordeling.

Cyberincidenten, zoals aanvallen met ransomware, hebben al dan niet een directe impact op het vertrouwen van digitale gebruikers. Daarom is het belangrijk om aandacht te besteden aan cyberbeveiliging, om ervoor te zorgen dat het vertrouwen in digitale transformatie niet wordt ondermijnd.

Om de cyberveiligheid te versterken en van België een van de minst kwetsbare landen in Europa te maken, verzamelt het CCB voortdurend informatie over de kwetsbare systemen in ons land. Het doet dat in vier fasen: monitoring van de belangrijkste kwetsbaarheden, de identificatie van de kwetsbare systemen, de identificatie van de eigenaar van het kwetsbare systeem en het waarschuwen en informeren van de eigenaar van het kwetsbare systeem.

Verschillende CCB-projecten verstrekken informatie aan bedrijven over de door aanvallers uitgebuite kwetsbaarheden.

Voor kritieke dienstverleners beheert het CCB een systeem voor vroegtijdige waarschuwing dat verschillende van de bovengenoemde fases automatiseert. Het CCB werkt ook aan een project om verschillende van deze waarschuwingdiensten vanaf eind dit jaar aan te bieden aan alle organisaties in ons land, via een nieuw portaal, SafeOnWeb @Work.

In antwoord op uw laatste vraag, volgens het CCB had ten minste een derde van de incidenten waarbij het moest ingrijpen een grote of zeer grote impact op de getroffen organisatie.

01.03 Erik Gilissen (VB): Mijnheer de staatssecretaris, dank u voor uw antwoorden.

Dat ransomware en hacking bij onze bedrijven, besturen en ziekenhuizen voor heel wat financieel verlies zorgt door het lekken van gegevens, is voor iedereen wel duidelijk. Het niet operationeel zijn van servers en het stilleggen van hele bedrijven en productieprocessen kost onze bedrijven, besturen en ook onze economie handenvol geld.

U zei dat u geen informatie hebt over hoeveel bedrijven een cyberverzekering hebben. Het lijkt mij in deze tijden toch een goede zaak zo'n verzekering af te sluiten.

Nog al te vaak is er sprake van een slechte beveiliging in bedrijven. Wij hebben al berichten gehoord over te zwakke wachtwoorden. De mazen in het net moeten worden verkleind door de telecomoperatoren, met hulp van het CCB, die de kennis hebben hoe de cyberveiligheid te verbeteren, maar daarnaast moeten wij ook inzetten op sensibilisering.

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

02 **Samengevoegde vragen van**

- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Storingen bij overheidswebsites" (55034393C)

- Erik Gilissen aan Petra De Sutter (VEM Ambtenarenzaken en Overheidsbedrijven, Telecommunicatie en Post) over "Storingen bij overheidswebsites" (55034394C)

02 **Questions jointes de**

- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Les perturbations sur les sites internet des pouvoirs publics" (55034393C)

- Erik Gilissen à Petra De Sutter (VPM Fonction publique et Entreprises publiques, Télécoms et Poste) sur "Les perturbations sur les sites des pouvoirs publics" (55034394C)

02.01 Erik Gilissen (VB): Mijnheer de staatssecretaris, de e-governmenttoepassingen moeten toelaten om ook buiten de kantooruren administratieve verrichtingen met de overheid te doen. Op 15 februari 2023 waren er problemen met verschillende overheidstoepassingen. Een aantal websites was moeilijk of niet bereikbaar en ook de identificatie via de Federal Authentication Service, dat de toegang tot de beveiligde toepassingen regelt, werkte niet naar behoren. Volgens BOSA werden de problemen veroorzaakt door het slecht functioneren werking van het netwerk.

Kunt u verduidelijken wat er precies aan de hand was? Welke maatregelen zult u nemen om gelijkaardige incidenten te voorkomen?

02.02 Staatssecretaris **Mathieu Michel**: Mijnheer Gilissen, ondanks goed voorbereid onderhoud is er in de infrastructuur van het FOD BOSA-datacenter een manuele fout opgetreden op DNS-niveau, waardoor de interne communicatie van de diensten in het datacenter werd verstoord. Hierdoor waren bepaalde diensten zoals websites en de FAS niet of nauwelijks beschikbaar voor de eindgebruiker.

De FOD BOSA constateerde op 15 februari 2023 tussen 11.15 uur en 12.00 uur een probleem waardoor de diensten niet beschikbaar waren voor de eindgebruikers tussen 12.00 uur en 13.40 uur. Terwijl de configuratie en de interne communicatie werden hersteld, waren de diensten beperkt beschikbaar, wat de gebruikerservaring voor de eindgebruiker beïnvloedde. Tegen 13.40 uur waren alle diensten weer beschikbaar en tegen 15.00 uur was de volledige capaciteit van het datacenter hersteld.

Daar het om een manuele fout ging, zal de procedure worden geoptimaliseerd om dergelijke manuele fouten uit te sluiten. Parallel daarmee worden de scenario's beter afgesteld om in geval van gelijkaardige incidenten de *business continuity* te verbeteren en de robuustheid van de datacenterinfrastructuur te versterken.

02.03 Erik Gilissen (VB): Dank u, mijnheer de staatssecretaris. De overheid zet alsmaar meer in op digitalisatie en de burger moet zijn administratieve verrichtingen steeds vaker zelf doen. Administraties zijn ook steeds moeilijker bereikbaar via de telefoon of andere traditionele kanalen. Wanneer de digitale diensten van e-government dan niet beschikbaar zijn, zorgt dat voor problemen. Wat gebeurt er als cruciale diensten, om welke reden dan ook, voor langere tijd niet beschikbaar zijn? Ligt dan het hele land plat? Zijn er hier wel noodprotocollen voor?

Ook al hoeft u mij als ICT'er geenszins te overtuigen van de voordelen van digitalisatie, ik ben me bewust van mogelijke gevaren. Ik hoop dat ook u zich daar bewust van bent.

Het incident is gesloten.

L'incident est clos.

03 Samengevoegde vragen van

- Michael Freilich aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Blockchain4Belgium" (55034460C)

- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Het Blockchain4Belgium-initiatief" (55034484C)

03 Questions jointes de

- Michael Freilich à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Blockchain4Belgium" (55034460C)

- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'initiative Blockchain4Belgium" (55034484C)

03.01 **Michael Freilich** (N-VA): Mijnheer de staatssecretaris, ik verwijs naar mijn ingediende vraag.

Mijnheer de staatssecretaris, u wil het debat over de uitdagingen van Web3, blockchain en digitale activa aanwakkeren. Ze hebben alle drie een enorm potentieel. Hun wereldwijde markt groeit al enkele jaren exponentieel. De prognoses voor de komende jaren zijn positief.

U heeft besloten het Blockchain4Belgium-initiatief te lanceren. Dat moet de verschillende Belgische spelers in staat stellen een reeks bevindingen en aanbevelingen op te stellen voor de regering, met het oog op het opstellen van een plan. Blockchain4Belgium wordt, via de FOD BOSA, een platform voor spelers uit de industrie, academici, het maatschappelijk middenveld en de verschillende betrokken overheden (economie, financiën, justitie, ...).

Meer dan 500 professionals zouden zich reeds hebben aangemeld en steunen het initiatief. Twee belangrijke werkpunten werden geïdentificeerd. Het eerste richt zich op innovatie in de particuliere sector en zal met verschillende werkgroepen aanbevelingen opstellen. De tweede werkt vooral op het gebruik van deze innovatieve technologieën binnen de overheid door verschillende use cases voor te stellen in verschillende domeinen.

Vandaar volgende vragen:

- 1. Welk budget werd voorzien voor het Blockchain4Belgium-initiatief? Waarvoor moet het allemaal dienen?*
- 2. Welke spelers uit de industrie, de academische wereld, het maatschappelijk middenveld en de verschillende overheden (economie, financiën, justitie, ...) zijn bij het project betrokken? Hoe zullen ze in de praktijk samenwerken?*
- 3. Wordt er vanaf het begin samengewerkt met het CCB en de GBA? Wat is hun rol in het project?*
- 4. Kan u de rol van de FOD BOSA toelichten? Wat is uw rol in het project?*
- 5. Hoeveel werkgroepen zijn er binnen het initiatief? Wat gaan zij specifiek onderzoeken?*
- 6. Wanneer worden de bevindingen en aanbevelingen overgemaakt aan de regering? Wanneer mogen we het plan verwachten?*

03.02 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, ik verwijs naar mijn ingediende vraag.

U hebt recent het Blockchain4Belgium-initiatief gelanceerd en aangekondigd dat het de bedoeling is om van België het Zwitserland van de blockchain te maken.

Met dit initiatief kunnen verschillende spelers een reeks aanbevelingen opstellen voor de regering om een bottom-up ecosysteem te creëren met betrekking tot Blockchain, digitale activa en Web3-technologieën.

- 1. Op welke financiering via de programma's van de Europese Commissie kan u rekenen?*
- 2. Welke bedrijven zijn al betrokken bij dit project?*
- 3. Wat zijn de taken, onderzoeksopdrachten en deliverables van de aangemelde bedrijven?*
- 4. Hoeveel middelen gaat er naar deze bedrijven?*
- 5. Wat is het voorziene tijdspad?*
- 6. Welke waarborgen zijn er t.a.v. digitaal kwetsbaren?*

03.03 Staatssecretaris **Mathieu Michel**: Geachte Kamerleden, Blockchain4Belgium is een open ecosysteem dat vanuit het terrein is ontstaan en dat ik heb gesteund nadat ik de noodzaak zag om het

debat in ons land over die kwestie te verduidelijken. De actoren en de coalitie zijn divers, afkomstig uit de privésector, de academische wereld, overheidsdiensten en het maatschappelijk middenveld. Tot heden brengt Blockchain4Belgium meer dan 1.000 mensen samen. Ook met het CCB en de GBA werden al contacten gelegd.

Het initiatief Blockchain4Belgium wordt ondersteund door de FOD BOSA, DG Vereenvoudiging & Digitalisering. De FOD BOSA organiseert, ondersteunt en coördineert de thematische werkgroepen rond de zonet vermelde thema's. Daarnaast worden verschillende evenementen voorbereid om ervaringen uit te wisselen en te delen. Momenteel werkt één voltijds equivalent daaraan. Dat faciliteert het werk van de thematische groepen om aanbevelingen voor de overheid te formuleren over de uitdagingen van Web3, blockchain en digitale activa.

Er zijn verschillende Europese projectoproepen die een alternatieve financiering bieden. Het platform beoordeelt de mogelijkheid om daaraan deel te nemen en verspreidt informatie onder de belanghebbenden, bijvoorbeeld in het kader van het Digital Europe Programme 2023-2024, een programma uitgaand van EBSI, het Digital Decade Policy Programme en het Next Generation Internet initiative. De verschillende thema's van Blockchain4Belgium zijn te vinden op de website www.blockchain4belgium.eu. De leden nemen deel op vrijwillige basis.

Er zijn acht themagroepen gedefinieerd die in de komende maanden hun aanbevelingen zullen indienen. De thema's die aan bod zullen komen, zijn België en zijn financiering aantrekkelijk maken, internationale referentie, de oprichting van het blockchainecosysteem aanmoedigen, de blockchain technologie demystificeren, dus begrijpen, opleiden en communiceren, de evolutie van de juridische aspecten, het gebruik van blockchain- en Web3-technologieën in onze economie bevorderen, de verduidelijking van het fiscaal kader en de overheid, dus de definiëring van *use cases*.

In hun aanbevelingen zullen de groepen aandacht moeten besteden aan de digitale kloof en inclusie, met inbegrip van bewustmaking, opleiding en onderwijs in de thematische werkgroep demystificatie van blockchaintechnologie, dus begrijpen, opleiden en communiceren.

03.04 Michael Freilich (N-VA): Mijnheer de staatssecretaris, proficiat, u hebt nog iets gelanceerd. Aan de krant zei u dat u wenst dat ons land het Zwitserland van de blockchain wordt. Ik ben evenwel teleurgesteld, want u opent een nieuwe praatbarak. Er zullen 500 actoren bij deze zaak worden betrokken. Er zullen aanbevelingen worden geformuleerd in werkgroepen enzovoort. De legislatuur duurt nog iets meer dan een jaar. Dat proces zal nu starten en over een jaar zullen er aanbevelingen zijn, die dan gedistilleerd moeten worden. U weet wel hoe dat gaat. Hoe meer spelers erbij betrokken worden, hoe moeilijker het wordt om tot een consensus te komen. In plaats van zelf te bepalen welke richting we uitgaan en zelf met uw administratie te bekijken wat u in de resterende vijftien maanden kunt realiseren, is dit een tweede *Digital Minds*. Dat was ook een van uw paradepaardjes, maar ik heb daar uiteindelijk niets meer van gehoord, behalve dat enkele groepsleden vertrokken zijn omdat ze vonden dat het de verkeerde kant uitging.

Ik ben dus teleurgesteld want ik had meer verwacht. Het is een initiatief zoals er zoveel zijn, maar ik vrees dat we opnieuw in het niets zullen verzanden. Er zijn 500 participanten voor verschillende werkgroepen en thema's: dat zal niets opleveren.

03.05 Erik Gilissen (VB): Mijnheer de staatssecretaris, iedereen aan de blockchain, dat lijkt tegenwoordig zowat de leuze. We hebben daarover recent nog een reeks zittingen van het adviescomité voor wetenschappelijke en technologische vraagstukken gehad. In welke mate denkt u dat de gemiddelde Belg zit te wachten op de blockchaintechnologie en de blockchainwallet? Het overgrote deel van de Belgen weet niet eens wat dat is of heeft vaag gehoord dat dit iets met bitcoin te maken heeft. Ik begrijp dat u een early adopter, een voortrekker wil zijn en in deze legislatuur nog iets verwezenlijkt wil hebben, maar welk nut zal dit hebben voor de helft van de bevolking die digitaal kwetsbaar is? De digitale kloof in de maatschappij lijkt steeds groter te worden. Ik denk dat we in de eerste plaats daarop moeten focussen.

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

04 Vraag van **Kathleen Verhelst** aan **Mathieu Michel** (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "De bereikbaarheid van multinationals/internetgiganten" (55034463C)

04 Question de **Kathleen Verhelst** à **Mathieu Michel** (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'accessibilité des multinationales/géants de l'internet" (55034463C)

04.01 **Kathleen Verhelst** (Open Vld): Mijnheer de staatssecretaris, wij zijn vandaag meer dan ooit geconnecteerd en netwerken breiden zich uit, zowel voor consumenten als voor b2b. De risico's op misbruik zijn echter ook legio.

Gelet op de misbruiken is een fysiek of minstens een telefonisch aanspreekpunt van internetgiganten als Microsoft, Amazon, Facebook en Instagram voor mij heel belangrijk, maar dat blijkt eigenlijk onbestaande. Ik ken ondernemers van wie de Instagramaccount na hacking permanent geblokkeerd werd, waardoor zij hun hele klantenbestand verloren zagen gaan. Ik ken klanten die het slachtoffer zijn van malafide verkopers, via bijvoorbeeld Amazon, maar bij Amazon kan niemand worden bereikt. Ik ken ook een groot bedrijf waarvan het paswoord van zijn Microsoftaccount en van zijn leverancier van zijn ICT-materiaal werd gehackt. Hij had daar zelf geen enkel uitstaans mee, maar hij kreeg wel een factuur van 360.000 euro van Microsoft voor een week hacking. Nochtans kan de onderneming daar niets aan doen en beseft zij de hacking zelfs niet. Er zijn dus echt grote en angstaanjagende cases.

Het begint bij de klantvriendelijkheid en bereikbaarheid van de betrokken internetgiganten, zodat problemen vlugger worden geïdentificeerd, oplossingen kunnen worden aangereikt, herhaling van dergelijk misbruik wordt vermeden en misschien zelfs eerste stappen kunnen worden gezet in de richting van vervolging van fraudeurs. Marktmacht komt ook met verantwoordelijkheid.

Ontvangt uw administratie op eender welke wijze klachten over de gebrekkige bereikbaarheid van internetgiganten? Zo ja, hoeveel waren er dat jaarlijks sinds 2020? Is een trend vast te stellen?

Wat is het wettelijk kader voor de bereikbaarheid en de verantwoordelijkheden van internetgiganten, als de gebruiker het slachtoffer wordt van illegale activiteiten? Bestaan er sancties voor de internetbedrijven die duidelijk onvoldoende inspanningen leveren?

04.02 Staatssecretaris **Mathieu Michel**: Eerst en vooral beschik ik niet over concrete cijfers over de meldingen inzake een gebrekkige toegankelijkheid van de internetgiganten. Trouwens, meldingen kunnen ons zeer verspreid bereiken, hetzij via een beleidscel, hetzij via meerdere administraties of nog via regulatoren zoals het BIPT.

De internetgiganten moeten, net als alle platformen, de wettelijke verplichtingen inzake elektronische handel en consumentenrechten naleven. Die verplichtingen vloeien voort uit de Europese richtlijn betreffende consumentenrechten, die werd omgezet in Belgisch recht, de Europese richtlijn die platformen verplicht de aard van de persoon met wie de consument de overeenkomst sluit, mee te delen, en de Europese richtlijn inzake elektronische handel die een algemene informatieverplichting bevat voor bedrijven die op het internet actief zijn. De bepalingen zijn omgezet in Belgisch recht en gaan gepaard met strafrechtelijke sancties.

Ook op Europees niveau zijn verschillende andere initiatieven genomen om zowel bedrijven als eindgebruikers in de zogenaamde platformeconomieën te beschermen. Allereerst werd op 20 juni 2019 een platform-to-businessverordening aangenomen. Die zal bepaalde schadelijke praktijken reguleren of zelfs verbieden. Platforms moeten ook zorgen voor een gemakkelijk toegankelijk klachtenbehandelingssysteem. Overtredingen van die verordening worden bestraft.

Daarnaast is er de Digital Services Act, die in oktober 2022 is aangenomen. Die biedt belangrijke middelen om bepaalde frauduleuze praktijken beter te bestrijden. Zo zal elke tussenpersoon verplicht zijn een enkel contactpunt aan te wijzen voor de afnemer van diensten, zullen marktplaatsen een zekere traceerbaarheid van professionele verkopers die op hun platform actief zijn, moeten vaststellen en zullen controles worden uitgevoerd op producten die als illegaal worden beschouwd.

Die tussenpersonen zullen ook de gebruiker die vermoedelijk een dergelijk illegaal product heeft gekocht, moeten informeren, met name over de identiteit van de verkoper en de mogelijke rechtsmiddelen.

Bij niet-naleving van de verplichtingen volgen er sancties, eventueel van financiële aard, die kunnen oplopen tot 6 % van de totale omzet van de betrokken tussenpersoon.

Er zijn dus tal van juridische instrumenten voorhanden, die het mogelijk moeten maken om een betere toegankelijkheid te garanderen en de verantwoordelijkheid van de grote internetplatformen te versterken.

04.03 **Kathleen Verhelst** (Open Vld): Ik dank u voor uw antwoord. Ik had de vraag eveneens voorgelegd aan de staatssecretaris van Begroting en de minister van Economie.

Het is alvast duidelijk dat er veel middelen voorhanden zijn om het probleem te verhelpen.

Ik zou nog de volgende suggestie willen meegeven. De internetgiganten zijn niet massaal aanwezig in België. Het zou ons alvast een stap dichterbij brengen, mocht de overheid al eens bij de top 10 van hen in België nagaan of zij wel degelijk een telefoonnummer vermelden op hun website. Men maakt vaak geen gebruik van de rechtsmiddelen, omdat men zich de moeite ontziet een rechtszaak tegen die giganten in te spannen.

Ik roep de overheid op om minstens voor de top 5 of de top 10 ervan te controleren of ze de verplichting om bereikbaar zijn wel naleven.

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

De **voorzitter**: Aangezien de heer D'Amico afwezig is zonder verontschuldiging, vervalt zijn vraag nr. 55034771C.

*De behandeling van de vragen en interpellaties eindigt om 14.03 uur.
Le développement des questions et interpellations se termine à 14 h 03.*