Vlaams Parlement

768 (2015-2016) – Nr. 1
ingediend op 11 mei 2016 (2015-2016)

Verslag van de gedachtewisseling

namens de Commissie voor Buitenlands Beleid,
Europese Aangelegenheden, Internationale Samenwerking,
Toerisme en Onroerend Erfgoed
uitgebracht door Jan Van Esbroeck

over het EU-US Privacy Shield

verzendcode: BUI

Samenstelling van de Commissie voor Buitenlands Beleid, Europese Aangelegenheden, Internationale Samenwerking, Toerisme en Onroerend Erfgoed:

Voorzitter: Rik Daems.

Vaste leden:

Ingeborg De Meulemeester, Marc Hendrickx, Jan Van Esbroeck, Karl Vanlouwe, Karim Van Overmeire, Manuela Van Werde;

Sabine de Bethune, Vera Jans, Ward Kennes, Johan Verstreken;

Rik Daems, Herman De Croo;

Tine Soens, Güler Turan;

Wouter Vanbesien.

Plaatsvervangers:

Cathy Coudyser, Caroline Croo, Danielle Godderis-T'Jonck, Sofie Joosen, Ann Soete, Sabine Vermeulen;

Karin Brouwers, Griet Coppé, Joris Poschet, Valerie Taeldeman;

Jean-Jacques De Gucht, Marnic De Meulemeester;

Renaat Landuyt, Steve Vandenberghe;

Bart Caron.

Toegevoegde leden:

Stefaan Sintobin;

Christian Van Eyken.

INHOUD

1. Inleidende uiteenzettingen 4
1.1. Uiteenzetting van Willem Debeuckelaere 4
1.2. Uiteenzetting van Frank Robben 8
2. Vragen en opmerkingen van de leden 9
3. Antwoorden van de sprekers 11
3.1. Antwoorden van Frank Robben 11
3.2. Antwoorden van Willem Debeuckelaere 13
4. Bijkomende vragen en opmerkingen van de leden 14
5. Aanvullende antwoorden 15
Gebruikte afkortingen 17
Bijlage: zie dossierpagina op www.vlaamsparlement.be

In de Commissie voor Buitenlands Beleid, Europese Aangelegenheden, Internationale Samenwerking, Toerisme en Onroerend Erfgoed vond op 20 april 2016 een gedachtewisseling plaats over het EU-US Privacy Shield.

Aan deze gedachtewisseling werd deelgenomen door Willem Debeuckelaere, voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer en van de Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer, en Frank Robben, administrateur-generaal van de Kruispuntbank van de Sociale Zekerheid, lid van de Commissie voor de bescherming van de persoonlijke levenssfeer en de Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer.

De powerpointpresentatie die door Willem Debeuckelaere werd gebruikt voor zijn toelichting is te vinden op de dossierpagina van dit document op www.vlaamsparlement.be.

1. Inleidende uiteenzettingen

1.1. Uiteenzetting van Willem Debeuckelaere

Willem Debeuckelaere, voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer (de zogenoemde Privacycommissie) en van de Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer, is verheugd over de belangstelling van de parlementaire commissie.

Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

De Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer is opgericht door het Vlaams Parlement en is operationeel sinds 6 januari 2010. Ze bestaat naast de federale Privacycommissie en is bevoegd voor het verlenen van machtigingen en het geven van adviezen. De machtigingen betreffen het interadministratieve verkeer tussen alle geledingen van de Vlaamse administratie, maar ook het administratieve verkeer naar bedrijven en federale of internationale instellingen. Alles wat via elektronische en georganiseerde weg vanuit de Vlaamse administratie vertrekt, moet vooraf gemachtigd worden door de respectieve toezichtcommissie. Jaarlijks zijn er zo ongeveer veertig tot vijftig machtigingen door de Toezichtcommissie. Het zijn onder meer de grote machtigingen, voor bijvoorbeeld instellingen zoals VLABEL, die in één keer gebeuren voor gegevens die naar allerlei instellingen moeten. Soms gaat het ook om kleine zaken, vanuit een Vlaamse instelling bijvoorbeeld naar één gemeente bijvoorbeeld. Het jaarverslag wordt jaarlijks voorgesteld aan de voorzitter van het Vlaams Parlement.

De Vlaamse toezichtcommissie bestaat uit zes mensen die door het Vlaams Parlement zijn aangesteld. Drie ervan komen uit de federale Privacycommissie, met name de spreker zelf, Frank Robben en Frank Schuermans. Drie andere zijn experten die werden aangewezen nadat ze zijn gehoord en beoordeeld op hun kennis van administratie en privacyrecht. Er wordt nauw samengewerkt met de federale Privacycommissie en door de Privacycommissie ook Europees binnen de zogenaamde 'working party 29'. Die besprekingen vinden doorgaans plaats in Brussel, het centrum van de Europese administratie.

Europese richtlijn 95/46 EU en Belgische Privacywet van 8 december 1992

Er is een Europese richtlijn 95/46 EU inzake de privacyregeling. Hoofdstuk 4 daarvan gaat over de doorgifte van persoonsgegevens naar derde landen. Het is de basiswetgeving en mede het fundament voor de Belgische privacywetgeving van 8 december 1992, die in 1998 is aangepast aan de Europese regelgeving,

met toevoeging van een nieuw hoofdstuk 6 'Doorgifte van persoonsgegevens naar landen buiten de Europese Gemeenschap'. De twee artikelen geven aan dat er twee zones zijn: de Europese en die buiten Europa, de rest van de wereld dus. In de Europese zone moeten persoonsgegevens vrij uitgewisseld kunnen worden, net zoals dat voor goederen en diensten en kapitaal het geval is. Zowel in de Belgische als in de Europese regelgeving is voorzien dat er een negatieve of zwarte lijst kan bestaan. Men gaat ervan uit dat voor de zone buiten Europa, moet worden nagegaan of er een passend beschermingsniveau is en of er rode lichten zijn; zijn er redenen waardoor er met een land geen persoonsgegevens kunnen worden uitgewisseld? En tot slot wordt bekeken of er op een uitzonderingsregime een beroep kan worden gedaan.

De eerste stap is het passende beschermingsniveau. De Europese Commissie beslist over het al dan niet aanwezig zijn daarvan. Voor een aantal landen zoals Israël, Canada, Argentinië enzovoort is dat gebeurd. Enkele dossiers lopen en Japan heeft intussen ook een aanvraag ingediend. Het is van belang, omdat de desbetreffende beslissing van de Europese Commissie aangeeft dat een land als een quasi-Europees land wordt beschouwd. Er is geen enkele barrière of bijkomende regelgeving die dan speelt.

Tweede optie is het opmaken van een zwarte lijst van landen waarmee men absoluut geen zaken wil doen en waarmee er onder geen beding een uitwisseling van persoonsgegevens plaatsvindt. In de praktijk is dat echter nog nooit toegepast, zelfs Noord-Korea is niet op een dergelijke lijst opgenomen. De zwarte lijst is dus onbestaand en na recente goedkeuring van de vernieuwde Europese privacyregeling trouwens volkomen verdwenen.

Het derde en belangrijkste punt is het uitzonderingsregime. Op basis van een aantal uitzonderingsgronden kan de verantwoordelijke voor de verwerking – dat is wie instaat voor doel en middelen van de persoonsgegevensverwerking – op eigen risico beslissen om akkoord te gaan met het doorgeven van persoonsgegevens. Dat kan met toestemming van de persoon in kwestie, op basis van een contract, op grond van zwaarwegende belangen, in gerechtelijke verdediging, voor het vitaal belang van de persoon en als het om openbare registers gaat. Tweede mogelijkheid is dat er een uitzondering geldt via machtiging en koninklijk besluit. Dat gebeurt beperkt, maar de laatste twee tot drie jaren wel meer geregeld. Er is een nieuw systeem ontwikkeld – de binding corporate rules – dat betekent dat multinationals een voorstel kunnen doen ten aanzien van de Europese regelgever om aan te geven dat ze intern in het bedrijf de persoonsgegevens op een zekere manier verwerken en waarborgen en om het akkoord van de EU vragen ter zake. België heeft samen met Nederland, Frankrijk, Duitsland en Groot-Brittannië een methode ontwikkeld om dat vlot en gezamenlijk te regelen.

De 'binding corporate rules' of bindende bedrijfsvoorschriften zijn intussen ook opgenomen in het nieuwe Europese instrument. De Europese Commissie heeft daarbovenop ook nog de 'standard contractual clauses', die eveneens bijkomende waarborgen genereren. Het zijn standaard contracten die door de Europese Commissie vooropgesteld worden en die ervoor zorgen dat de waarborgen als voldoende beschouwd worden.

Safe Harbour

Een heel specifiek waarborgsysteem is het Amerikaanse, de Safe Harbour. In 2000 hebben de VS bij de Europese Commissie bedongen dat ze zelf een specifiek systeem zouden opzetten om het gelijke niveau van bescherming te waarborgen, niet voor heel de VS maar enkel binnen een bepaalde sector, met name de Amerikaanse bedrijven die onder de bevoegdheid van bepaalde VS-

overheden (de US Federal Trade Commission en de US Department of Transportation) ressorteren. Deze bedrijven kunnen een Safe Harbour-certificaat van het US Department of Commerce krijgen en zouden daarmee meteen ook beschouwd worden als bestemmelingen die dezelfde waarborgen bieden als bedrijven uit de EU-zone, waardoor persoonsgegevens vrij kunnen worden uitgewisseld. Het Safe Harbour-systeem is heel specifiek, gezien de sectorale aanpak, en ook het enige systeem dat met Europa op een sectorale manier is geconnecteerd. Japan probeerde het ooit ook met een eigen systeem, dat echter werd afgewezen door de Europese Commissie.

Safe Harbour wordt vaak gebruikt door administraties, organisaties en bedrijven. Een van de meest spraakmakende voorbeelden is het SWIFT-akkoord, waarrond wel wat commotie is ontstaan. Het Belgische bedrijf SWIFT werd door de Federal Reserve – de Amerikaanse nationale bank – letterlijk gebruikt als een soort van gegevensbank om wereldwijd allerhande financiële transacties te monitoren in het kader van de strijd tegen het terrorisme. Dat was niet bekend en het diende opgelost via een specifiek akkoord. Er is ook een verdrag voor gesloten tussen Europa en de VS. Ook in dat verband is Safe Harbour aangewend als waarborg voor een goed gebruik van de persoonsgegevens.

Het systeem kreeg nogal wat kritiek te verwerken, vooral in de jaren 2007 en 2008. Studies beweerden dat Safe Harbour, dat opgezet was door de Federal Trade Commission van de VS, niets meer zou zijn dan windowdressing inzake de controle op de wijze waarop bedrijven en organisaties met de gegevens omgaan. De Belgische Privacycommissie heeft in een aantal gevallen ook effectief kunnen vaststellen dat bepaalde bedrijven en organisaties bij een vraag om rechtzetting of schrapping van gegevens niet thuis gaven en zich veilig waanden in de VS. De kritiek zwol enorm aan na de revelaties van Edward Snowden. Toen bleek dat een aantal bedrijven en organisaties een soort van backdoorsysteem hadden waarlangs alle gegevens rechtstreeks naar de NSA en aanverwante instellingen gingen. Het Europees Parlement nam in 2014 een motie aan ter zake. Het vroeg aan de Europese Commissie om het systeem opnieuw onder de loep te nemen en betere waarborgen te onderhandelen om zo tot een Safe Harbour 2 te komen.

Intussen heeft de Oostenrijkse student in de rechten Maximiliaan Schrems echter een actie opgezet tegen Facebook, dat ook een backdoor naar de NSA zou hebben. Hij diende een klacht in tegen Facebook omwille van de beveiliging van gegevens die hij met vrienden en kennissen in de VS en Europa uitwisselde. Eerst deed hij dat in Oostenrijk, bij de Privacycommissie daar, die hem doorverwees naar Ierland, waar Facebook een vestiging heeft voor Europa. De Ierse Privacycommissie verschool zich evenwel achter het feit dat het ging om een beslissing van de Europese Commissie. Die keurde Safe Harbour goed en zou derhalve toezicht moeten houden. Schrems legde zich daar echter niet bij neer en ging in beroep bij het Hooggerechtshof in Dublin omdat hij vond dat zijn gegevens bescherming moesten genieten vanuit Ierland. Dat stelde een prejudiciële vraag aan het Europese Hof van Justitie in Luxemburg. Op 6 oktober 2015 oordeelde dat hof dat de Privacycommissie, van Ierland of Oostenrijk, haar werk moest doen en de Europese burger wel degelijk moet bijstaan en het onderzoek moet doen, los van wat de Europese Commissie heeft beslist. Dat het Europese Hof de integrale beslissing van de Europese Commissie van 2010 over Safe Harbour als adequaat instrument teniet zou doen, sloeg in als een bom. Het Hof motiveerde die beslissing met verwijzing naar de mass surveillance door de VS grondig in alinea's 92 tot en met 96 van zijn arrest, die opgenomen zijn in de Powerpointpresentatie.

Het arrest had tot gevolg dat er vooralsnog geen juridisch instrument meer is om de Europese zone naar de VS uit te breiden. Een ander gevolg is dat de nationale Privacycommissies in actie moeten schieten en klachten ter zake moeten

behandelen. De federale Privacycommissie behandelt intussen ook een klacht van Max Schrems, die zich behalve tot de Ierse en Belgische, ook wendde tot de Duitse Privacycommissie. Het hele dossier ligt aldus weer bij de Ierse, Belgische en Duitse Privacycommissie. Het Europees Parlement bood nog geen oplossing voor het probleem. Dat is een gevolg van het nationalisme in Europa. Het is iets beter geworden met de verzamelde Privacycommissies in een Europese instelling. Zij kunnen bij geschillen tussen landen een bindende beslissing nemen. Het is echter nog twee jaar wachten op de inwerkingtreding van de verordening en daarmee de mogelijkheid van dergelijke beslissing. In juni 2016 zou ze moeten verschijnen in het Europese Publicatieblad, twintig dagen later wordt de verordening van kracht en pas na twee jaar wordt ze van toepassing. De spreker noemt dit alvast een gemiste kans. Hij geeft nog mee dat België als enige lidstaat hamerde op een Europese oplossing zoals een Europese Privacycommissie. Dat kwam eigenlijk te laat, want de grote lidstaten beslisten al dat het beter is om voor de eigen deur te vegen en kozen voor een nationale oplossing. Dat had meteen ook gevolgen mee voor het dossier van het Privacy Shield.

Privacy Shield

Uiteindelijk kwam het toch tot een akkoord tussen de EU en de VS, het Schrikkelakkoord genoemd omdat het op 29 februari 2016 tot stand kwam. Het kreeg niet meer de naam Safe Harbour, maar Privacy Shield. Het probleem daarmee is dat het door de opinie van de verzamelde Europese Privacycommissies eigenlijk al onderuit is gehaald op 13 april 2016. Het formele standpunt luidde dat men geen positief advies kon verstrekken vanwege de vele vraagtekens en kritiekpunten. Een positief advies van de working party 29 is evenwel niet nodig. Wel nodig is een positief advies van de lidstaten, verzameld in de zogenaamde working party 31. De beide cijfers staan voor de artikelen waarnaar de Europese richtlijn verwijst. Of die goedkeuring er komt, is nog onduidelijk. Commissaris Věra Jourová is daarmee belast en er zou ten laatste juni-juli 2016 een beslissing moeten zijn. De Europese Commissie moet zich erover uitspreken of het Privacy Shield een gedegen oplossing biedt en gelijkwaardig is aan de Europese regelgeving. Het advies van working party 29 is alvast negatief. Dat is evenwel alleen richtinggevend, het advies van de lidstaten is wel nodig.

Zeker is dat het laatste woord bij het Europese Hof van Justitie berust. Er is al aangekondigd, door diverse organisaties en ook door Max Schrems, dat men geen genoegen neemt met het tussengekomen akkoord over het Privacy Shield en dus opnieuw naar het Europese Hof zal stappen. De spreker relativeert de zaak wel omdat wat onderuit gehaald is, eigenlijk een preferentieel systeem voor de VS is, en er voor de rest van de wereld de klassieke waarborgen gelden. Daar kan men mee werken en normaal gesproken kan dat dus ook voor de VS. Heel wat gegevens die worden uitgewisseld, situeren zich in de businesssfeer, zoals het personeel van multinationals, en men kan zich dus uit de slag trekken. Voor iedereen zal dezelfde waarborgregeling gelden, zowel voor Noord-Korea als voor de VS. Er is wel een kleine vooruitgang geboekt. Zo heeft het Privacy Shield belangrijke nieuwe elementen die ervoor pleiten en het mogelijk maken om de bedoelde waarborgen aan te nemen. Formeel zal de Belgische Privacycommissie moeten beslissen of de waarborgen voldoende zijn. Tegelijk zal de Belgische regelgever via een koninklijk besluit er ook in kunnen voorzien dat, als men voldoet aan het Privacy Shield en mits eventueel wat bijkomende voorwaarden, er geen probleem is voor een gegevensuitwisseling tussen Europa en de VS. Er worden in elk geval nog nieuwe onderhandelingen verwacht.

De VS kent echter al jaren een standstill op het vlak van wet en regelgeving door de strijd tussen democraten en republikeinen. Of er na de verkiezingen een oplossing zal zijn, blijft de vraag. Voorstellen van zowel de Obama-administratie als van Hilary Clinton opteren voor een regeling met Europa. Ook de Amerikaan-

se industrie volgt die redenering, maar het gaat op zich eigenlijk over macht: wie bepaalt wereldwijd de voorwaarden waaronder financiële en persoonsgegevens kunnen worden uitgewisseld en verwerkt? De Belgische Privacycommissie kan getuigen dat dit ook terugkomt in de discussies over het beheer van het internet. Dat gebeurt vooralsnog op vrij voluntaristische wijze, door de organisatie ICANN. Er lopen onderhandelingen, ook door de Raad van Europa over het wereldwijde beheer van het internet. Bedrijven zoals Amazon, Apple, Facebook en Microsoft eisen hun plek op in de organisatie en zien het liefst dat staten zich terugtrekken. Voorlopig is daar geen enkele Europese speler in mee.

1.2. Uiteenzetting van Frank Robben

Frank Robben is lid van de Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer en van de Privacycommissie, en heeft de leiding over de Kruispuntbank van de Sociale Zekerheid. De VS kennen ook nog de Patriot Act, een wetgeving die tot stad kwam na de aanslagen van 9/11. Daarmee worden zeer ruime bevoegdheden toegekend aan Amerikaanse onderzoeksinstanties om gegevens te verkrijgen via en op te vragen bij Amerikaanse bedrijven, ongeacht waar zij zich bevinden.

Een duidelijk signaal naar Europa is nodig omdat er massaal wordt geëvolueerd naar situaties waarbij gegevens niet anders dan in een cloud bewaard kunnen worden. Zoals elektriciteit kan worden afgenomen van elektriciteitscentrales wanneer men die nodig heeft, zonder te weten waar die elektriciteit gegenereerd wordt, zo geldt dat ook voor computercapaciteit. Er staan overal ter wereld computers en er wordt opslag-, verwerkings- en andere capaciteit afgenomen wanneer men die nodig heeft. Betalen moet alleen voor wat werd gebruikt, maar niemand weet nog waar wat staat en waar het vandaan komt. De enige die daarvoor het nodige potentieel hebben, zijn Amerikaanse bedrijven, die allemaal onder die regelgeving ressorteren. Er zijn geen Europese spelers. Zonder degelijke beperking, zit men vast aan die Amerikaanse leveranciers, zowel de overheid als ondernemingen. Dat is nu al merkbaar aan de licentiepolitiek. Volgens de spreker zullen er op korte termijn geen licenties meer gegeven worden om op lokale infrastructuur te draaien, alles zal in de cloud moeten gebeuren. België zal aan die evolutie weinig kunnen veranderen. Daarom is het een gemiste kans dat er geen Europees privacyorgaan in het leven is geroepen. De verordening kwam grotendeels tot stand om multinationale ondernemingen een stuk rechtszekerheid te bieden, maar er is geen Europese instantie die daar tegenop kan boksen.

Dat is een voortdurend probleem. De spreker vermeldt bij wijze van voorbeeld dat de Vlaamse overheid werkt met HP, een Amerikaans bedrijf, als serviceprovider. De data staan dan wel in België, maar de Patriot Act is daarvoor net zo goed van toepassing. Alle data staan derhalve in de cloud.

Zeker voor de overheid wordt geprobeerd om via de cloudprincipes zaken onder te brengen in eigen datacenters onder eigen beheer. In een dergelijk hybride systeem zijn goede afspraken nodig en gemaakt over wat wordt bijgehouden en wat in de publieke cloud kan. Dan gaat het vooral om niet privacygevoelige gegevens. Dat wordt wel alsmaar moeilijker.

Een ander initiatief is het zoveel mogelijk werken met opensourceomgevingen om niet afhankelijk te blijven. Open source betekent dat het om software gaat die tot het publieke domein behoort en waarvoor geen licentie moet worden betaald. Zo is men niet afhankelijk van de grote spelers en kan men het blijven gebruiken op eigen, zelf gecontroleerde omgevingen. Het blijft een permanent aandachtspunt. Op Europees vlak is absoluut een regeling nodig die ook kan worden afgedwongen. Het kan geen optie zijn om de industriële spelers, die allen onder de Patriot

Act ressorteren, het onder elkaar te laten regelen. Op termijn zal het niet mogelijk zijn om garanties te blijven bieden.

De vraag kan worden gesteld waarom de gegevens niet worden versleuteld. Dat wordt geprobeerd, maar dat is geen afdoend antwoord. Vercijferingsmechanismen geven het probleem dat hun zekerheidsgraad beperkt is in de tijd. De gehanteerde sleutels blijven drie tot vier jaar veilig. Zeker voor longitudinale gegevens, bijvoorbeeld inzake gezondheid, is dat het geval. Eenmaal vercijferd en in een opencloudomgeving gezet – waarvan overigens niemand nog weet waar die zich bevindt, dat kan zelfs op tankers in extraterritoriale wateren bijgehouden en gearchiveerd – kan iemand ze binnen enkele jaren ontcijferen. De vercijferingssleutels stoelen op systemen die momenteel niet te ontcijferen zijn op een redelijke termijn. De computercapaciteit neemt echter almaar toe en binnen enkele jaren zal dat dus wel kunnen. Als de ontcijfermechanismen zo worden ontworpen dat ze twintig jaar of langer mee kunnen, dan duurt vercijferen veel te lang. Om gegevens te verwerken, moeten ze dan bovendien toch ontcijferd worden. Dat is dus geen oplossing. Er is nood aan een veel grotere awareness in Europa om dat aan te pakken.

Zelf staat de spreker in voor uitwisseling van gezondheidsgegevens. Hij durft met bepaalde gegevens niet in de publieke cloud te gaan omdat hij niet de garantie kan bieden dat die data niet binnen enkele jaren gedecrypteerd zullen kunnen worden. Hij vreest dat de huidige oplossingen, zoals de datacenters en de open source en dergelijke, over enkele jaren niet langer zullen volstaan.

Men probeert al een tijd de onafhankelijkheid van grote spelers in te bouwen in de systemen. Geregeld worden de opensourcespelers echter opgekocht door commerciële bedrijven en dat fnuikt die oplossing dan weer. Bijvoorbeeld SUN was als bedrijf zeer opensourceminded en JAVA werd opgekocht door Oracle. De commerciële spelers lichten de opensourcezaken er dan uit. België noch Vlaanderen kunnen dat oplossen, maar er kunnen wel signalen gegeven worden. Dat is voor de spreker net zo belangrijk als het Privacy Shield: een beleidsvisie ontwikkelen ter zake. Het is niet vanzelfsprekend om zich tegen ondernemingen als Microsoft af te zetten of te verweren. Er zal voor een deel preventief moeten worden gewerkt, besluit hij.

2. Vragen en opmerkingen van de leden

Ward Kennes refereert aan zijn vraag om uitleg over het Privacy Shield (*Vragen om uitleg* Vl.Parl. 2015-16, nr. 1230). Zijn invalshoek was het handelsverkeer tussen Europa en de VS, dat alsmaar meer geconditioneerd wordt door uitwisseling van data. Hij vindt het niet geruststellend dat de problematiek veel verder blijkt te gaan dan het handelsverkeer. De mogelijke impact van de vernietiging van Safe Harbour strekt ver en de oplossing via het Privacy Shield blijkt ook niet het ei van Columbus te zijn.

Het lid onthoudt uit de toelichting de noodzaak aan een veel verdergaande samenwerking op Europees niveau. Het wordt moeilijk om nog rechten te laten gelden als burger, maar ook als overheidsadministratie, rond Facebook of de socialezekerheidsgelden.

Heel wat data zouden zelfs op tankers in extraterritoriale wateren verzameld worden. Het lid ziet in dat verband heel wat juridische problemen. Hoe zit het met het zeggenschap daarover? Onder welke vlag varen die schepen en wordt die vlag dan naar believen vervangen als er een juridische procedure dreigt? En wat als een dergelijk schip zinkt? Is er nog een back-up? Of is alles dan verloren?

Wat betreft vercijfering en versleuteling zou er nogal wat windowdressing zijn. Het lid hoopt dat er in het parlement nog verder kan worden nagedacht, ook over de eigen gegevens. Voorts blijft dat niet alle landen een even Europese impuls als België hebben en dat sommigen liever op de rem gaan staan.

Jan Van Esbroeck vraagt zich af hoe het nu verder moet met de vacuümzone die er nu in feite is. Hij begrijpt dat vooralsnog de algemene regels gelden zoals dat voor alle andere landen het geval is. Er zijn dus geen speciale regels voor de VS. Safe Harbour bestaat niet meer en het Privacy Shield is nog niet volledig in voege. Wat het lid echter ook begrijpt, is dat geen enkel systeem belet dat de Amerikaanse bedrijven alle data, ook uit de cloud, verder blijven gebruiken. De Patriot Act laat dat immers toe. Dat baart het lid zorgen. Het gaat immers niet alleen om bedrijfsgegevens. Wat met medische gegevens, bijvoorbeeld data van farmaceutische bedrijven, ziekenhuizen enzovoort? Het verontrust het lid ook dat de grote Europese landen niet bereid blijken om gezamenlijk tot inzichten en oplossingen te komen voor het Privacy Shield. Er is nochtans nood aan betere indekking, zeker tegen die grote Amerikaanse bedrijven. Het lijkt een gevaarlijke en explosieve situatie in het besef van hoeveel informatie de Vlaamse overheid en de Vlaamse bedrijven in de cloud hebben zitten.

Hoe zit het precies met de vertegenwoordiging van Vlaanderen en België in het Europese Privacycommissieverhaal? Wat als er wordt beslist om gewoon door te gaan?

Herman De Croo ziet nog veel bijkomende elementen. Met 29 leden een overeenkomst bereiken en dan ook nog de regio's in acht nemen, lijkt hem niet eenvoudig. Dat kan volgens hem hoegenaamd geen gewicht hebben.

Met de VS is er een soort van bevoorrechte werking en dat minstens om twee redenen. Ten eerste zijn ze de haven waar alles gevestigd is en kan gebeuren en ten tweede zijn ze gewoon van extraterritoriaal te werken. De VS staan op hun strepen qua eigen beveiliging, zo ook bijvoorbeeld in de Antwerpse haven.

Versleutelde informatie blijkt zonder juridische tussenkomst toch ontsleuteld te kunnen worden. Zijn er dan ontsleutelaars die sterker zijn dan de versleuteling die voorhanden is? Klopt het dat er technologieën zijn in de gebruikte hardware, die ontsnappen aan alle controles? En als dat zo is, zijn er dan geen alternatieven? China zou proberen te ontsnappen aan de Amerikaanse versleutelingstechnologie en met een eigen systeem bezig zijn. Dat zou dan weer Chinees versleuteld worden. Er zouden dan twee of drie blokken ontstaan, met ook een Chinese en Amerikaanse regeling.

Het lid stelt dat er de jongste tijd heel wat coördinatie is in de informatiebenutting van de VS en vermeldt bij wijze van voorbeeld de strijd tegen drugs, grote kapitaalsbewegingen en de terreurbestrijding. Is men een verkeerde weg ingeslagen met juridische tochtjes via het Europese Hof, de Europese Commissie enzovoort? Het lid vreest dat dit boter aan de galg zal zijn. Hij is cynisch en ziet liever dat er betrouwbare bondgenoten worden gezocht dan dat een gevecht wordt aangegaan dat niet kan worden gewonnen.

Güler Turan deelt het cynisme en de zoektocht naar oplossingen van Herman De Croo, en veronderstelt dat zij niet alleen is.

Privacygegevens zijn in België en Vlaanderen zwaar beschermd. Gegevens lijken de plaats van aandelen in te nemen in het verkrijgen van macht, stelt het lid. Ze kreeg van de sprekers de bevestiging dat we daar machteloos tegenover staan en ze vindt eveneens dat samenwerking aangewezen is om sterker te staan.

De Patriot Act maakt dat gegevens van privépersonen, bedrijven en overheden niet meer veilig zijn. Zelfs de data van het parlement zijn dat niet en het werken met eigen datacenters is beperkt qua mogelijkheden. Kan er worden gehoopt op een juridische regeling die aan de VS kan worden opgelegd? Kunnen multinationals die in Amerika gevestigd zijn wel gereglementeerd worden? De verordening die eraan komt, het Privacy Shield, zou volgens de sprekers meer dienen om de bewuste multinationals zekerheden te geven en niet zozeer om bescherming te bieden. Europa gaat dus heel omzichtig met de eigen gegevens om maar tegelijk liggen die gegevens te grabbel in de VS. Als dat de 'business as usual' is die wordt doorgezet, dan vindt de spreekster dat bijzonder verontrustend.

Het signaal dat uitgaat van de working party 29 geeft aan dat er geen duidelijkheid is. Dit is eigenlijk een negatief advies en het zou dan ook sterk verbazen mocht de Belgische overheid, die in dat adviesorgaan vertegenwoordigd is, uiteindelijk zelf wel een positief advies verstrekken voor het Privacy Shield. Het lijkt essentieel dat vanuit Vlaanderen en België de boodschap gegeven wordt dat het huiswerk opnieuw moet worden gedaan.

Het pogen reglementeren van multinationals doet het lid denken aan de problematiek van het TTIP. We staan blijkbaar machteloos tegenover praktijken en controle door een derde, de VS, inzake vrij verkeer van de eigen gegevens. Als dat ene aspect nog niet kan worden geregeld, wat wordt het dan als er allerhande normering en reglementering rond milieu, voedselveiligheid, gezondheid worden samengebracht in een commissie? Zich daartegen wapenen, zou ook moeten gebeuren in Europees verband.

De regeling rond het Privacy Shield bepaalt onder meer dat burgers een klacht kunnen neerleggen bij een bedrijf en dat die binnen de 45 dagen moet worden behandeld. Bedrijven moeten toetreden tot het Privacy Shield door de privacyprincipes te onderschrijven, door self-certification. Dat impliceert vooral dat alle betrokken gegevens 45 dagen lang vogelvrij zijn. Er kan ook een klacht worden ingediend bij de nationale privacyautoriteit, zoals bevestigd door het Europese Hof van Justitie. Die klacht wordt dan doorverwezen naar het Department of Commerce en verder behandeld door de Federal Trade Commission. Ondertussen loopt de termijn en liggen de gegevens opnieuw te grabbel. Dat de working party 29 geen advies heeft kunnen verstrekken, is dan ook niet zomaar.

De laatste boei is het Privacy Shield Panel. Die instantie kan dan uiteindelijk bindende beslissingen nemen ten aanzien van bedrijven uit de VS. Het is wel hallucinant dat er intern maandenlang gediscussieerd wordt over beschermingsrechten allerhande die gelden ten opzichte van de onderdanen, bijvoorbeeld wat betreft huiszoekingen, terwijl alle mogelijke informatie zonder meer beschikbaar is in de VS. Voor de eigen bedrijven is men in Europa nochtans streng. Hoe is de verhouding van de Belgische nationale gegevensbescherming versus wat er gebeurt voor het Privacy Shield? De spreekster ziet namelijk het beeld voor zich van een Belgisch bedrijf dat gegevens wil verkrijgen van Europeanen en Belgen. Het volstaat dan om een windowdressingbedrijf op te richten in de VS om aan al die data te geraken. Wie zich daartegen wil verzetten, moet dan maar procedures gaan inspannen. Hoe er dan van business as usual kan worden gesproken, begrijpt het lid niet.

3. Antwoorden van de sprekers

3.1. Antwoorden van Frank Robben

Frank Robben stelt dat het recht niet veel oplost in voorliggende zaak. Het is zinloos om te stellen dat er vanaf morgen geen gegevens meer mogen worden

verwerkt. Zo is het bijvoorbeeld in de gezondheidssector essentieel dat wie iemand verzorgt, zicht moet hebben op de medische achtergronden.

Tankers kunnen inderdaad zinken en er is al eens een schip gezonken van Amazon, waarbij gegevens verloren gingen, al zijn er wel back-ups. Men kan een cloud opbouwen binnen de eigen datacentra. In plaats van eigen infrastructuur te behouden, kan die ook worden gedeeld en kan er gebruik van worden gemaakt naargelang van de behoefte. Bij wijze van voorbeeld vermeldt de spreker dat de RSZ gedurende een kwartaal twee keer een piekperiode van tien dagen kent qua aangiftes en dat de infrastructuur voor het overige slechts voor 30 tot 40 percent werd gebruikt. Daarom werd ervoor gezorgd dat de RSZ geen eigen infrastructuur meer heeft, maar die deelt met een aantal instellingen van sociale zekerheid. De totale capaciteit wordt op die manier optimaal benut. De totale kostprijs van infrastructuur en licenties daalt bovendien fors, tot wel 25 tot 30 percent. Ook dat is een cloudprincipe, maar dan in eigen datacenters. Het gaat er derhalve om waar zaken worden ondergebracht en er kan niet worden gesteld dat de cloud niet goed zou zijn.

De publieke cloud houdt in dat de infrastructuur wereldwijd gedeeld wordt en men zich er dus niet meer mee bezig moet houden waar die zich bevindt. De verantwoordelijkheid voor het nemen van back-ups op diverse plaatsen kan dan elders worden gelegd. Dat kan contractueel vastgelegd worden, maar als gegevens eenmaal weg zijn, is daar niets aan te doen. De spreker raadt daarom doorgaans af van zaken op de publieke cloud te zetten, tenzij men ermee kan leven dat de kans bestaat dat die informatie verloren gaat.

Wat de vercijfering betreft, zijn er geen absolute zekerheden. Voor een korte termijn kan de veiligheid worden gegarandeerd, mits gebruik van de geschikte technologie. De spreker geeft het voorbeeld van data die tussen artsen worden verzonden. Hij maakt zich meer zorgen over data die voor een langere tijd moeten worden bijgehouden.

Veel vercijferingstechnieken zijn vaak gebaseerd op zeer lange priemgetallen. Twee van dergelijke getallen, vermenigvuldigd met elkaar, geven een product op. Als men dat product kent, maar niet een van de twee priemgetallen, dan nog kan geen computer in de wereld, zelfs na twee jaar draaien, die twee priemgetallen distilleren. Als de computercapaciteit over een periode van tien of twintig jaar nog enorm evolueert, dan zal dat wel kunnen. Bovendien mogen de priemgetallen niet te lang zijn, want dan duurt de encryptie te lang en dan is de efficiëntie zoek. Het duurt dan bijvoorbeeld heel lang voor een mail verstuurd geraakt.

Het komt erop aan een evenwicht te vinden. Bijvoorbeeld ook voor de digitale kluis eerstelijnszorg, Vitalink, wordt er regelmatig hervercijferd, om mee te zijn met de technologische evoluties. Onder meer professor Bart Preneel is in België een bijzonder goed cryptograaf, die tevens in bepaalde organen van de Privacycommissie zit. Die mensen onderzoeken onder meer wat de sleutellengte moet zijn.

De Patriot Act in de VS omvat ook een onderdeel dat een plicht tot ontcijferen bevat als bepaalde organen dat eisen. België kent dat niet, en er is geen zicht op wie wat vraagt in de VS. Het klopt natuurlijk wel dat het probleem niet beperkt blijft tot de VS. Ook China en Rusland hebben het protentieel.

Wat de backdoors betreft, gaat het niet om hardwarezaken, maar wel om software die embedded is in de hardware. Het is wellicht wel enigszins geruststellend dat er methodes bestaan om na te gaan of dergelijke elementen aanwezig zijn. Het doet alweer de vraag rijzen wat in de publieke cloud kan worden gezet en wat in een cloud waarop nog enige mate van controle is.

Opnieuw moet het belang van een preventieve aanpak worden onderstreept. Er zijn sniffersystemen. Bij Proximus is de malware tijdig ontdekt omdat er over bepaalde kanalen vreemde patronen waren over het gegevensverkeer. Er is meteen ingegrepen en vooraleer de grote hacking kon plaatsvinden, was de malware eruit. Gegevens verwerken en doorgeven heeft vele voordelen, maar het blijft iets wat permanent aandacht vergt en uiteindelijk is het wat een strijd van David tegen Goliath. Bij software van Microsoft of Oracle of IBM bijvoorbeeld, is de code niet te lezen. Opensourcecode is leesbaar en iedereen kan nagaan of daarin backdoors zitten. Dat maakt het een goede praktijk.

Er is evenwel steun nodig vanuit Europa om de opensourceomgevingen te vrijwaren. Als die worden overgenomen, staat men nog nergens. Er zou opnieuw een soort van Europese industrie moeten kunnen ontstaan. In de VS primeert de veiligheid op de privacy. Hier wordt er meer naar een evenwicht gezocht tussen efficiëntie en veiligheid, met veiligheid ingebakken in de systemen en met garanties daarvoor. Privacy is trouwens een kwestie van ervoor zorgen dat gegevens niet terechtkomen bij mensen die ze niet mogen zien. Daarnaast is ook de beschikbaarheid en de integriteit van de data belangrijk. Ze mogen niet verdwijnen en niet gewijzigd kunnen worden. Dat is een globaal verhaal waarvoor er op een ander niveau dan het Vlaamse of Belgische een oplossing moet komen. Bij grote overnames moet er een goedkeuring zijn. Europa moet ervoor zorgen dat men de opensourceomgevingen niet blijft overnemen en lamleggen.

In België zijn de privacyorganen stilaan wat te versnipperd, meent de spreker. Toen de kruispuntbank van start ging, was er een Privacycommissie die afhing van de uitvoerende macht. Nadien werd ze ondergebracht bij het parlement, waar ze thuishoort. Er werd een goed systeem uitgewerkt: preventief, geen centralisatie van gegevens maar uitwisseling, en voor elke uitwisseling machtiging door een sectoraal comité. Dat bleek een goed systeem, maar er zijn dan consecutief sectorale comités opgericht voor bepaalde domeinen. Naast de federale Privacycommissie die federaal werd benoemd, ontstonden Vlaamse en Waalse toezichtcommissies, alsook een Brusselse versie. Dat maakte coördinatie er niet gemakkelijker op. Bovendien is men inzake veiligheid maar zo sterk als de zwakste schakel.

De spreker pleit al een tijd voor een orgaan waarin mensen zitting hebben die door het Federaal, het Vlaams en het Waals Parlement worden aangeduid en dat ervoor zorgt dat een aantal afspraken gemeenschappelijk gelden, minstens in België. Bij gegevensuitwisseling in bijvoorbeeld de sector van de activering van werklozen spelen de RVA, de VDAB, Forem en de Brusselse dienst voor arbeidsbemiddeling Actiris een rol. Er moet gegevensuitwisseling gebeuren en daarvoor is een machtiging nodig. Met vier verschillende organen is dat omslachtig en riskeert men dat niemand nog een zicht heeft op het geheel. Dat zou gaten slaan in het systeem. De spreker noemt dit een aandachtspunt in het licht van staatshervorming. Hij heeft begrip voor de politieke eigenheden, maar het zou de zaken wel sterk vereenvoudigen in het werkveld.

3.2. Antwoorden van Willem Debeuckelaere

De heer *Willem Debeuckelaere* stelt vast dat heel wat opmerkingen en vragen eigenlijk over onmacht en macht gaan. Voor hem is het belangrijk zich niet neer te leggen bij het gevoel van onmacht, maar juist wel te reageren. Als de Europese Privacycommissies allemaal aan hetzelfde zeel trekken, zoals bij de SWIFT-kwestie, en er is steun van de politieke wereld, dan volgen er oplossingen. In het geval van Google, toen dat bedrijf bezig wat met de Googlemaps, is dat ook gebeurd en ook daar is een oplossing uit de bus gekomen. Die bedrijven kiezen uiteindelijk liefst voor een vreedzame oplossing als ze merken dat er druk

wordt uitgeoefend en men desnoods naar de rechtbank gaat. Ze gaan dan – zeker tot op zekere hoogte – mee in de oplossingen die worden geëist, zij het soms node. Naar aanleiding van de rechtszaak van de Belgische Privacycommissie tegen Facebook, werd er in eerste instantie schamper gedaan, maar uiteindelijk is de rechter gevolgd en heeft Facebook, zeer tegen de zin, zijn beleid in België gewijzigd.

Het lijkt de spreker daarom van belang dat er heldere signalen komen vanuit een parlementaire assemblee zoals het Vlaams Parlement, naar het federale niveau en naar Europa, om aan te geven dat men daar zijn werk moet doen. Zo heeft het ook gewerkt in de zaak-Schrems, waar het Europese Hof van Justitie de Privacycommissies en Europa heeft aangemaand te doen wat moet gebeuren.

Wat de business as usual betreft, bedoelde de spreker dat men niet stante pede met een oplossing zal kunnen komen, noch kan ophouden met het uitwisselen van gegevens met de VS. Alles is onderling geconnecteerd en afgestemd, maar net zo goed bijzonder kwetsbaar, zoals is gebleken bij de recente gebeurtenissen in Zaventem. Het komt erop aan zich steeds weerbaar op te stellen en een oplossing te zoeken, te eisen en af te dwingen.

Niet alleen België heeft een probleem qua Privacycommissies. Spanje heeft regionale Privacycommissies in drie regio's en ook daar zijn er spanningen en discussies. In Duitsland heeft elk van de länder er één. Dat is niet onwerkbaar, maar er moeten een aantal mechanismen zijn die politiek afstemmen, zodat het systeem werkbaar blijft. Als er op een bepaald moment een duidelijke meerderheid is, moet dat gevolgd worden. Dat is een democratisch beginsel, maar het is wel maar op de valreep aangenomen in de verordening.

4. Bijkomende vragen en opmerkingen van de leden

Jan Van Esbroeck voelt zich na de bijkomende toelichting wat meer gerust. Hij onderstreept het belang van overeenkomsten zoals TTIP, omdat die samenspraak en overeenstemming bevorderen om tot een oplossing te komen.

Hij hoorde ook een oproep om een nieuwe staatshervorming. De samenwerking die wordt gevraagd, ligt wel moeilijk – ook in Spanje is dat het geval – en daar zijn nieuwe akkoorden voor nodig. Een nieuwe staatshervorming kan dus inderdaad een goed idee zijn.

Ward Kennes noemt zich niet minder ongerust, maar wel wat minder moedeloos. De gevaren en problemen zijn reëel, met opensourceinitiatieven die door de Chinezen kunnen worden overgenomen en dies meer. Geruststellend is het allemaal niet. Hij begrijpt dat het zaak is er actief mee bezig te blijven vanuit het perspectief van overheid, wetgever en consumentenbeschermers.

De versnipperde besluitvorming is inderdaad een feit en een interfederale aanpak is aangewezen om de krachten te bundelen. Daarover moet worden nagedacht op en met alle niveaus.

Veel evoluties van globalisering en digitalisering zijn niet tegen te houden, ook wat gevoelige informatie betreft. Goede regelingen, intern Belgisch en tussen Europese landen maar ook tussen de handelsblokken die op elkaar aangewezen zijn, zijn essentieel. De afweging tussen efficiëntie en bescherming vergt permanente keuzes. Er moet worden nagedacht over hoe het thema verder op de agenda kan worden gehouden in het parlement.

Herman De Croo wil dat er wordt nagedacht over een andere mindset. Hij wijst op de verschillende systemen waarmee medische gegevens worden uitgewisseld.

De systemen zijn niet altijd compatibel, maar uitwisseling van die gegevens is wel nodig en vaak nuttig. Als het bijvoorbeeld over de Panama Papers gaat, is de houding tegenover uitwisseling van gegevens doorgaans helemaal anders. Hij wijst vervolgens op de quasi-informatiemuren rond de steden. Er zijn steden die er prat op gaan dat alles wat binnenkomt en buitengaat geregistreerd wordt. Dat lijkt op de middeleeuwen zonder muren en poorten. Als het erom gaat een fraudeur te pakken te krijgen en te kunnen volgen, dan is men iets minder privacygevoelig. Bij de mogelijkheid dat iedereen ook de eigen informatie en stappen kan volgen, heeft men echter een heel ander gevoel.

Men kan echter ook proberen het nut te zien van de communicatiemogelijkheden, om te weten tot waar communicatie mogelijk is met waarborgen. In dat perspectief moet technologisch en politiek gewerkt worden. Het lijkt een verloren zaak om een volkomen ondoorbreekbare, niet hackbare communicatieomgeving te creëren. Dat vermindert en verdunt de stroom ter beveiliging van de belangen die spelen.

Het lid meent dat op lange termijn de enige oplossing is zich niet te verzetten tegen de macht die de VS hebben, ook over hun eigen bedrijven, maar er gebruik van te maken en zo de problemen aan te pakken.

Güler Turan is het ermee eens dat er onderhandeld en gepraat moet worden maar dan wel tussen twee gelijkwaardige partners. De commissie is nu in elk geval op de hoogte en er kunnen initiatieven genomen worden.

De working party 29 gaf geen advies om aan te geven dat het om een onduidelijke situatie gaat. Hoe wordt er in de Privacycommissies van andere lidstaten gereageerd? Zouden de lidstaten, ondanks dat negatieve advies, alles gewoon laten doorgaan? Dat lijkt toch zeer onwaarschijnlijk.

Het belang van meer digitalisering is duidelijk. Het lid refereert aan een parlementair werkbezoek aan Estland, waar de digitalisering zeer ver is doorgedreven. Een doktersbezoek wordt er automatisch van het loon afgehouden, een apotheek levert meteen de medicatie, zonder documenten. Daarmee is men ook hier bezig. Of daarvoor een staatshervorming nodig is of niet, moet ook worden bekeken.

5. Aanvullende antwoorden

Willem Debeuckelaere geeft aan dat de meeste Europese landen wel gealarmeerd zijn. Sommige landen zijn zelfs van plan drastische maatregelen te nemen. Zo overweegt de Franse Privacycommissie de gegevensuitwisseling met de VS te verbieden. Voor de Belgische Privacycommissie is dat juridisch alvast niet mogelijk en sowieso heeft het geen zin.

Op Europees niveau is er een grote bezorgdheid gegroeid met betrekking tot het negatieve advies van de working party 29 en wat er wellicht in de working party 31 zal gebeuren. Dit zal vanuit de VS ongetwijfeld nauwgezet worden opgevolgd, maar hun prioriteit is niet de toepassing van de privacyregeling die Europa vraagt. De spreker is ervan overtuigd dat de Privacycommissies van heel wat Europese lidstaten toch alles op alles zullen zetten om gehoor te krijgen bij hun autoriteiten. Hij beklemtoont nogmaals dat hij het even belangrijk acht dat ook een assemblee zoals het Vlaams Parlement in die kwestie van zich laat horen.

Hij wil tot slot nog meegeven dat er in het TTIP-verhaal met geen woord is gesproken over de bescherming van persoonsgegevens. Voormalig commissaris De Gucht verdedigde het standpunt om dat niet te doen en commissievoorzitter Juncker heeft bevestigd dat het niet in het kader van TTIP aan bod zou komen.

De reden is het uitgangspunt dat er niet wordt onderhandeld over fundamentele grondvoorwaarden. In die stelling zitten wel wat scheuren, oppert de spreker, want de informatieverwerking is op zichzelf ook een niet onbelangrijke industrie en er gaan almaar meer stemmen op om bij het TTIP ook aandacht te hebben voor de gegevensverwerking.

Frank Robben stelt dat artsen tot voor enkele jaren via e-mail gegevens doorstuurden. Intussen hebben ze allemaal een elektronische brievenbus met encryptie. De software werd geleverd door een extern bedrijf, maar werd gecheckt en is veilig bevonden. Er is ook voor gezorgd dat het toegangsbeheers-systeem door de overheid wordt beheerd en niet in een active directory van Microsoft. De overheid kan zo voor de gezondheidssector een kader bouwen waarbinnen met eigen pakketten kan worden gewerkt. Dat moet permanent worden uitgebouwd, besluit de spreker. In die zin is er inderdaad nood aan een andere mindsetting.

Güler TURAN,
waarnemend voorzitter

Jan VAN ESBROECK,
verslaggever

Gebruikte afkortingen

EU	Europese Unie
Forem	service public wallon de l'emploi et de la formation professionelle
ICANN	Internet Corporation for Assigned Names and Numbers
KB	koninklijk besluit
NSA	National Security Agency
RSZ	Rijksdienst voor Sociale Zekerheid
RVA	Rijksdienst voor Arbeidsvoorziening
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TTIP	Transatlantic Trade and Investment Partnership
US	United States
VDAB	Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding
VLABEL	Vlaamse Belastingdienst
VS	Verenigde Staten