DOC 53 **2639/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

7 février 2013

PROPOSITION DE RÉSOLUTION

relative à la sécurisation des supports électroniques de données

(déposée par M. Peter Dedecker et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

7 februari 2013

VOORSTEL VAN RESOLUTIE

met betrekking tot de bescherming van elektronische gegevensdragers

(ingediend door de heer Peter Dedecker c.s.)

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
VB	:	*Vlaams Belang*
cdH	:	*centre démocrate Humaniste*
FDF	:	*Fédéralistes Démocrates Francophones*
LDD	:	*Lijst Dedecker*
MLD	:	*Mouvement pour la Liberté et la Démocratie*

Abréviations dans la numérotation des publications:

DOC 53 0000/000:	*Document parlementaire de la 53e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral (couverture verte)*
CRABV:	*Compte Rendu Analytique (couverture bleue)*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes) (PLEN: couverture blanche; COM: couverture saumon)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Afkortingen bij de nummering van de publicaties:

DOC 53 0000/000:	*Parlementair document van de 53e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag (groene kaft)*
CRABV:	*Beknopt Verslag (blauwe kaft)*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen) (PLEN: witte kaft; COM: zalmkleurige kaft)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (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

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Après avoir consulté les groupes, le Comité d'avis des questions scientifiques et technologiques de la Chambre des représentants a décidé d'approfondir le thème suivant: "La cybersécurité et, en particulier, la sécurisation des supports électroniques de données tels que la RFID et la carte MOBIB (voir ci-dessous), notamment du point de vue du respect de la vie privée".

Dans ce contexte, plusieurs auditions ont été organisées, au cours desquelles les experts suivants ont été entendus:

— M. Peter Strickx, directeur général de FEDICT;
— M. Jean Jacques Quisquater, professeur émérite de cryptographie — UCL;
— M. Jos Dumortier, professeur à l'ICRI — KUL;
— M. Pascal Poty, Agence wallonne des télécommunications.

En quoi la RFID consiste-t-elle?

Une nouvelle dimension s'est récemment ajoutée à l'internet, au gsm et au gps: la RFID ou "*Radio Frequency Identification*". Jusqu'à présent, ces petites puces lisibles à distance ont surtout été utilisées dans le domaine de la logistique pour l'identification de marchandises. Aujourd'hui, la RFID est introduite en masse dans le domaine public pour l'identification des personnes: badges d'accès pour bureaux, clubs et stades de football, carte à puce MOBIB, passeport biométrique, systèmes de suivi dans les parcs récréatifs et systèmes de paiement locaux. Les utilisateurs de ces environnements "intelligents" aperçoivent les facilités offertes par la RFID en matière d'accès et de transactions, tandis que les gestionnaires découvrent les possibilités offertes par la RFID en termes de services supplémentaires et de contrôle de cet environnement.

Comment fonctionne la RFID?

Pour classifier les systèmes RFID, on fait généralement une distinction entre les puces RFID actives et passives, entre les puces à lecture seule et les puces réinscriptibles, et entre les systèmes ouverts et fermés. Une puce passive ne dispose pas de sa propre source d'énergie, mais utilise celle que le signal du lecteur RFID génère (par induction) dans une antenne spiralée qui se trouve sur la puce. Par conséquent, la distance

TOELICHTING

DAMES EN HEREN,

Na een bevraging van de fracties heeft het Adviescomité voor wetenschappelijke en technologische vraagstukken van de Kamer van volksvertegenwoordigers besloten om als nader te onderzoeken thema aan te wijzen: "De cyberveiligheid en meer bepaald de beveiliging van elektronische datadragers, zoals RFID en MOBIB (zie *infra*) onder meer uit het oogpunt van de privacy".

Daarom werden een aantal hoorzittingen georganiseerd met de volgende deskundigen:

— de heer Peter Strickx, directeur-generaal FEDICT;
— de heer Jean Jacques Quisquater, emeritus hoogleraar Cryptografie — UCL;
— de heer Jos Dumortier, hoogleraar ICRI - KUL;
— de heer Pascal Poty, *Agence wallonne des télécommunications*.

Wat is RFID?

Naast internet, gsm en gps heeft de digitale ruimte er sinds kort een nieuwe dimensie bij: RFID, oftewel *Radio Frequency IDentification*. De kleine op afstand uitleesbare chips werden tot nu toe vooral toegepast in de logistiek om goederen te identificeren. Nu wordt RFID massaal ingevoerd in het publieke domein om mensen te herkennen: toegangspasjes voor kantoren, clubs en voetbalstadions, de MOBIB-chipkaart, het biometrisch paspoort, volgsystemen in pretparken en lokale betalingssystemen. Gebruikers van deze "slimme" omgevingen zien het gemak dat RFID biedt bij toegangverlening en transacties, terwijl de beheerders de mogelijkheden ontdekken van RFID voor aanvullende dienstverlening en controle van die omgeving.

Hoe werkt RFID?

Om RFID-systemen in te delen wordt over het algemeen een onderscheid gemaakt tussen actieve en passieve RFID-*chips*, *read-only* en *rewriteable chips* en tussen open en gesloten systemen. Een passieve chip heeft geen eigen energiebron, maar gebruikt de energie die het signaal van de RFID-chiplezer opwekt in een spiraalvormige antenne op de chip (inductie). De afstand waarop de chip kan worden gelezen is dan ook

à laquelle la puce peut être lue n'est pas très grande: en théorie quelques mètres, mais, dans la pratique, quelques centimètres seulement. Une puce active dispose en revanche d'une pile et peut donc émettre elle-même un signal. Dans ce cas, la distance de lecture est beaucoup plus grande et varie en fonction de la radiofréquence et de l'intensité de la source d'énergie. La plupart des puces ont un code fixe qui peut être uniquement lu (*read-only*), tandis que dans d'autres puces, ce code peut en outre être modifié (*read-write*).

Certains systèmes RFID sont des systèmes fermés, ce qui signifie que le code de la puce n'a de signification que dans le cadre de la base de données du système pour lequel cette puce a été conçue. Il existe cependant de plus en plus de systèmes ouverts. Dans ce cas, la communication entre la puce et le lecteur s'effectue par le biais de standards utilisant différents codes et fréquences. Cette technique permet de relier entre elles les bases de données sous-jacentes de différents environnements. L'exemple de système ouvert le plus connu est l'EPC (*Electronic Product Code*), qui devrait remplacer le code à barres.

La RFID est, tout comme l'internet et le réseau GSM, une technologie de réseau. Mais la RFID a sa logique propre. Les systèmes RFID sont gérés par des intervenants très différents et la plupart des systèmes ne communiquent pas entre eux, alors que dans le cas du réseau GSM et de l'internet, en principe, tous les terminaux sont reliés les uns avec les autres. Ceci signifie que pour les différents propriétaires, il est facile de se faire une idée des comportements individuels, tandis qu'avec la RFID, il est plus difficile d'avoir une vue d'ensemble.

Dans la pratique, les petites puces RFID passives ne peuvent être lues qu'à une distance de quelques centimètres, ce qui se sent généralement. Les puces RFID actives peuvent être lues à de plus grandes distances, parfois même au-delà du kilomètre, mais leur pile les rend clairement visibles.

Une application RFID particulière est la carte MOBIB de la STIB utilisée dans les transports en commun bruxellois. La carte MOBIB contient un microprocesseur électronique et une antenne radio. Grâce à la technologie "sans contact", la carte peut être lue par le valideur dans un rayon de 5 cm, et il ne faut plus insérer le ticket (papier) dans le valideur. Cette carte à puce électronique est un système de paiement qui, à terme, pourra être utilisé partout dans les transports publics belges; selon des articles de presse récents (voir De Standaard du 23 novembre 2011), la SNCB introduira la carte à puce à partir de la mi-2012 comme titre de transport et on se dirige, à terme, vers une carte de transport unique qui

niet heel groot: in theorie tot op enkele meters, maar in de praktijk slechts op enkele centimeters. Een actieve chip beschikt daarentegen over een batterij en kan daardoor zelf een signaal uitzenden. De leesafstand is dan veel groter, afhankelijk van de sterkte van de energiebron en de radiofrequentie. De meeste chips hebben een vaste code die kan worden uitgelezen, *read-only*, terwijl die code bij andere chips ook kan worden aangepast: *read-write*.

Sommige RFID-systemen zijn gesloten systemen. Dat betekent dat de code op de chip alleen betekenis heeft binnen de database van het systeem waarvoor de chip is gemaakt. Steeds meer systemen zijn echter open systemen. De communicatie tussen chip en chiplezer verloopt dan via standaarden in soorten codes en frequenties. Daardoor kunnen de achterliggende databases van verschillende omgevingen worden gekoppeld. Het bekendste voorbeeld van een open systeem is de Elektronische Productcode (EPC), de beoogde opvolger van de streepjescode.

RFID is net als internet en gsm een netwerktechnologie. Toch is het zo dat RFID zijn eigen logica heeft. RFID-systemen worden beheerd door uiteenlopende partijen en de meeste systemen communiceren niet met elkaar, terwijl via internet en gsm alle terminals in principe met elkaar zijn verbonden. Dat betekent dat het voor de verschillende eigenaren gemakkelijk is inzicht te krijgen in individueel gedrag, maar dat het lastiger is om met RFID een totaalbeeld te krijgen.

De kleine, passieve RFID-chips kunnen in de praktijk slechts op enkele centimeters afstand worden uitgelezen en dat is meestal merkbaar. Actieve RFID-chips kunnen grotere afstanden overbruggen, soms zelfs meer dan een kilometer, maar zijn door hun batterij duidelijk zichtbaar.

Een bijzondere RFID-toepassing is de zogenaamde MOBIB-kaart van de MIVB in het Brusselse openbaar vervoer. De MOBIB-pass beschikt over een microprocessorchip en een radioantenne. Dankzij de "zonder contact"-technologie kan de pas worden gelezen door de ontwaarder binnen een straal van 5 cm, men hoeft het (papieren) ticket niet langer in de ontwaarder te stoppen. Deze chipkaart is een betaalsysteem dat op termijn overal op het openbaar vervoer in België zal kunnen worden gebruikt: volgens recente persberichten (De Standaard, 23 november 2011) voert de NMBS vanaf midden 2012 de chipkaart in als vervoerbewijs en zal men op termijn komen tot één enkele transportkaart die

pourra être utilisée par les quatre sociétés de transports en commun belges (STIB, TEC, DE LIJN, SNCB).

D'autres applications fréquentes de la RFID dans la vie quotidienne sont, notamment, les contrôles d'accès (dans un nombre croissant de bureaux et d'entreprises, les systèmes d'accès sont équipés de la RFID), la clé de voiture électronique "sans contact", la puce RFID dans le collier des chiens, les bracelets à puce RFID dans les maisons de retraite, *etc*.

Empreintes numériques dans les systèmes RFID

Les utilisateurs de la RFID laissent des empreintes numériques dans des environnements divers. Certains des systèmes décrits peuvent dès lors être utilisés de manière impropre pour suivre et contrôler des personnes sans en avoir demandé l'autorisation. Mais, pour l'instant, les choses se passent relativement bien, certainement si l'on tient compte de l'échelle à laquelle la RFID est aujourd'hui utilisée dans le domaine public. Les possibilités de suivre des personnes sont en outre limitées dans la pratique, parce que les différents systèmes ne permettent que de dresser un profil limité des utilisateurs. Toutefois, cela pourrait changer. De nombreux systèmes d'accès et de paiement fonctionneront sans doute bientôt exclusivement avec la RFID. Les systèmes RFID peuvent aussi de plus en plus souvent être reliés entre eux et à d'autres technologies. Les utilisateurs deviennent alors, de par leurs empreintes numériques, de plus en plus transparents pour les gestionnaires de ces environnements. À l'inverse, les environnements RFID deviennent justement de moins en moins transparents pour les utilisateurs. L'équilibre actuel entre choix, confort et contrôle peut dès lors être rompu.

Cela peut aussi avoir des conséquences pour le rôle des autorités. D'une part, il sera plus difficile de faire respecter la législation sur la protection de la vie privée. D'autre part, les autorités pourront elles-mêmes utiliser davantage les empreintes numériques, par exemple lors de la recherche de suspects ou de témoins.

Sur la voie d'un "internet des objets"

Il ressort d'interviews de divers utilisateurs de systèmes RFID que le Rathenau Instituut a réalisées notamment à l'étranger[1] que la majorité d'entre eux ne sont guère préoccupés par les empreintes numériques qu'ils laissent dans les environnements RFID. Les utilisateurs

[1] Voir, par exemple, Rathenau-instituut: "*RFID is meer keuze, gemak en controle in de digitale publieke ruimte*", Rathenau Instituut, La Haye, 2007. Un certain nombre de données reprises dans ce chapitre sont tirées de cette publication.

door de vier openbare vervoersmaatschappijen in België (MIVB, TEC, DE LIJN, NMBS) kan worden gebruikt.

Andere frequente RFID-toepassingen in het dagelijkse leven zijn onder andere toegangscontrole (op steeds meer kantoren en bedrijven worden de toegangssystemen uitgerust met RFID), de elektronische "contactloze" autosleutel, de RFID-chip in de halsband van de hond, arm- of enkelbanden met RFID-chip in bejaardentehuizen enz.

Digitale voetsporen in RFID-systemen

Gebruikers van RFID laten digitale voetsporen achter in uiteenlopende omgevingen. Enkele van de beschreven systemen kunnen dan ook oneigenlijk worden gebruikt om mensen ongevraagd te volgen en te controleren. Maar vooralsnog gaat het — zeker door de schaal waarop RFID nu in het publieke domein wordt ingevoerd — relatief goed. De mogelijkheden om mensen te volgen zijn in de praktijk bovendien begrensd, omdat de afzonderlijke systemen slechts een beperkt beeld geven van de gebruikers. Dat kan echter veranderen. Veel toegangs- en betaalsystemen zullen straks wellicht uitsluitend werken met RFID. RFID-systemen kunnen ook steeds meer aan elkaar en aan andere technologieën worden gekoppeld. Gebruikers worden dan via hun digitale voetsporen steeds transparanter voor de beheerders van die omgevingen. Omgekeerd worden de RFID-omgevingen voor gebruikers juist steeds minder inzichtelijk. De huidige balans tussen keuze, gemak en controle kan dan verstoord raken.

Dat kan ook gevolgen hebben voor de rol van de overheid. Enerzijds zal de handhaving van de wetgeving op de privacybescherming lastiger worden. Anderzijds zal de overheid zelf meer gebruik kunnen maken van digitale voetsporen, bijvoorbeeld bij de opsporing van verdachten of getuigen.

Op weg naar een "internet van dingen"

Uit interviews onder meer in het buitenland[1] die het Rathenau Instituut hield met diverse gebruikers van RFID-systemen blijkt dat de meeste weinig problemen zien in de digitale voetsporen die ze achterlaten in RFID-omgevingen. Wel moet het voor gebruikers duidelijk zijn

[1] Zie bijvoorbeeld Rathenau-instituut: "RFID is meer keuze, gemaken controle in de digitale publieke ruimte", Rathenau Instituut,Den Haag, 2007. Een aantal gegevens uit deze publicatie werden in dit hoofdstuk opgenomen.

doivent cependant savoir qui gère l'environnement et ils doivent avoir une contrepartie: facilité, rabais ou sécurité. La plupart des utilisateurs voient surtout la facilité de la RFID comme un avantage et partent du principe que la RFID n'est rien de plus qu'un portemonnaie ou une clé électroniques. Cette confiance est dans un certain sens justifiée. Car, à l'inverse du trafic internet et GSM, par exemple, les empreintes numériques des utilisateurs de la RFID ne dévoilent pas grand-chose d'eux. Les systèmes ne recouvrent qu'un domaine limité: un parcours unique, un immeuble de bureaux ou un club. En outre, il existe encore souvent des alternatives, telles que les cartes à sections, les codes-barres, les cartes magnétiques, les clés ou l'argent liquide. Cela limite parfois la facilité d'emploi, mais cela donne une certaine dose de liberté de choix, tandis que les gestionnaires ont des possibilités de contrôle plus limitées. Ils ne peuvent, en effet, avoir une vision globale de tous les mouvements de tous les gens.

Diverses évolutions montrent que cette situation pourrait changer. Tout d'abord, l'utilisation d'un certain nombre de systèmes RFID récemment instaurés va sensiblement augmenter au cours des prochaines années. Si, dans quelques années, la carte MOBIB devient le seul mode de paiement dans les transports en commun, les banques de données sous-jacentes auront une vision globale de tous les utilisateurs, y compris de leurs mouvements au sein du système.

En deuxième lieu, la liaison de différents systèmes RFID est une évidence. Elle facilite la vie de l'utilisateur, qui dispose de plus de possibilités avec moins de cartes, et du gestionnaire, qui peut étendre ses services et qui exerce un contrôle accru sur l'environnement.

Troisièmement, il existe une tendance à coupler les systèmes RFID à d'autres systèmes présents au sein de l'espace numérique, tels que le téléphone mobile, l'internet ou les caméras numériques. À l'échelle mondiale, les banques et les entreprises de téléphonie coopèrent pour permettre la réalisation de paiements par *Near Field Communication* (NFC). Le téléphone mobile servira dans ce cadre à la fois de puce et de lecteur RFID et il pourra en outre relier toutes sortes de données par le biais d'internet.

Enfin, l'instauration de l'IPv6 (*Internet Protocol* version 6) a donné une nouvelle impulsion à la combinaison de ces différents réseaux. L'IPv6 comporte une telle quantité de nouvelles adresses qu'il est en principe possible de conférer un numéro unique à chaque objet — et donc également à chaque puce RFID — et à chaque être humain.

wie de omgeving beheert en er moet iets tegenover staan: gemak, korting of veiligheid. De meeste gebruikers zien vooral in het gemak van RFID een voordeel en ze gaan ervan uit dat RFID niet meer is dan een elektronische portemonnee of sleutel. Die berusting is in zekere zin terecht. Want anders dan bijvoorbeeld internet- en gsm-verkeer, vertellen de digitale sporen van RFID-gebruikers nog niet zo heel veel over hen. De systemen beslaan slechts een beperkt gebied: een enkel reistraject, een kantoorgebouw of een club. Bovendien bestaan er nog vaak alternatieven, zoals strippenkaarten, streepjescodes, magneetkaarten, sleutels of contant geld. Dat beperkt soms het gebruiksgemak, maar geeft wel enige mate van keuzevrijheid, terwijl beheerders beperktere mogelijkheden hebben voor controle. Ze kunnen immers geen totaalbeeld krijgen van alle bewegingen van alle mensen.

Diverse ontwikkelingen wijzen erop dat dit zou kunnen veranderen. Allereerst zal het gebruik van een aantal recentelijk ingevoerde RFID-systemen de komende jaren sterk toenemen. Als over een paar jaar de MOBIB-kaart de enige betaalwijze in het openbaar vervoer is, bevatten de achterliggende databanken opeens een totaalbeeld van alle gebruikers, inclusief hun bewegingen binnen het systeem.

Ten tweede ligt ook de koppeling van verschillende RFID-systemen voor de hand. Dat dient het gemak van de gebruiker, die meer mogelijkheden krijgt met minder pasjes, en van de beheerder, die zijn dienstverlening kan uitbreiden en meer controle krijgt over de omgeving.

Ten derde is er een tendens om RFID-systemen te koppelen aan andere systemen binnen de digitale ruimte, zoals de mobiele telefoon, internet of digitale camera's. Wereldwijd werken banken en telefoniebedrijven samen om betaling via *Near Field Communication* (NFC) mogelijk te maken. De mobiele telefoon dient dan als RFID-chip en RFID-lezer tegelijk en kan bovendien via het internet allerlei gegevens koppelen.

Tot slot heeft het samengaan van al deze verschillende netwerken een nieuwe impuls gekregen door de invoering van IPv6 (*Internet Protocol* versie 6). IPv6 bevat zoveel nieuwe adressen, dat het in principe mogelijk is elk object — dus ook elke RFID-chip — en elke persoon op aarde een uniek nummer te geven.

Les initiés prédisent ainsi la naissance d'un "internet des objets" universel au sein duquel presque tous les gestes et actes posés dans le monde physique auront leur réplique dans l'espace virtuel. Grâce au confort d'utilisation qu'elle offre et à son coût limité, la RFID est en outre considérée comme une technologie clé.

Tout cela prendra du temps. Mais il est manifeste que les applications RFID actuelles ne constituent que le début d'un processus de développement bien plus vaste, dans le cadre duquel les relations entre utilisateurs et gestionnaires des environnements RFID risquent de se modifier drastiquement. Si on utilise et interconnecte des systèmes recourant exclusivement à la RFID, de plus en plus de gestionnaires auront la possibilité de se faire une idée de plus en plus précise du comportement des utilisateurs.

Applicabilité de la législation relative à la protection de la vie privée

Les utilisateurs des systèmes RFID bénéficient de la protection de la loi relative à la protection de la vie privée (LPVP), qui fixe les conditions d'utilisation des données renvoyant d'une façon ou d'une autre à une personne physique. Il est toutefois permis de se demander si la législation actuelle sera suffisante en la matière (voir les auditions) et comment les autorités pourront garantir le respect de la vie privée des consommateurs sans freiner l'innovation technologique.

Le 14 octobre 2009, la Commission de la protection de la vie privée a rendu de sa propre initiative un avis sur la RFID (avis n° 27/2009 du 14 octobre 2009). Cet avis peut être consulté sur son site internet.

Éléments tirés des auditions

M. Strickx souligne que l'eID constitue un élément essentiel de la politique belge en matière d'e-government des dix dernières années; il renvoie aux trois applications que sont l'eID, la *kids-ID* et la carte d'étranger. En ce qui concerne les données eID présentes sur la puce, celles-ci sont actuellement identiques aux données visibles sur la carte, il n'y a donc pas (encore) de données biométriques, d'argent électronique, ni d'autres données stockées. Grâce aux possibilités d'authentification, la puce permet de signer valablement des documents électroniques ("signature électronique"). Les applications de l'eID concernent aujourd'hui notamment la fiscalité, la déclaration à la police, l'*e-health*, le guichet électronique de certaines villes et communes, mais elles sont en principe illimitées (*home-banking, e-commerce*, soins de santé, …). À la suite de certains

Volgens ingewijden zal hiermee een alomvattend "internet van dingen" ontstaan, waarin vrijwel alle bewegingen en handelingen in de fysieke wereld een evenbeeld krijgen in de virtuele ruimte. RFID wordt daarbij vanwege het gebruiksgemak en de lage kosten gezien als een sleuteltechnologie.

Het zal nog de nodige tijd duren voor het zover is. Ondertussen is het wel al duidelijk dat de huidige RFID-toepassingen nog maar het begin zijn van een veel omvangrijkere ontwikkeling, waarbij de onderlinge verhoudingen tussen gebruikers en beheerders van RFID-omgevingen drastisch kunnen veranderen. Als systemen uitsluitend met RFID gaan werken en onderling worden gekoppeld, krijgen steeds meer beheerders steeds beter inzicht in het gedrag van gebruikers.

Toepasbaarheid van de privacywetgeving

Gebruikers van RFID-systemen genieten bescherming onder de wet bescherming privacy (WBP). Daarin is vastgelegd onder welke voorwaarden gegevens mogen worden gebruikt die op de een of andere manier verwijzen naar een fysiek persoon. De vraag is echter of de huidige wetgeving hier zal volstaan (zie de hoorzittingen) en hoe de overheid de consumentenprivacy kan waarborgen zonder de technologische innovatie af te remmen.

De Privacycommissie heeft op 14 oktober 2009, op eigen initiatief, een advies uitgebracht over RFID (advies nr. 27/2009 van 14 oktober 2009), raadpleegbaar op de website van de Privacycommissie).

Elementen uit de hoorzittingen

De heer Strickx benadrukt dat de e-ID een essentiële bouwsteen is van het Belgisch *e-government*beleid van de laatste 10 jaar; hij verwijst naar de 3 toepassingen e-id, *kids-id* en de vreemdelingenkaart. Wat betreft de e-id-info op de chip, deze is momenteel identiek aan de visueel zichtbare informatie op de kaart, dus (nog) geen biometrische data, geen elektronisch geld en geen opslag van andere data. Met de authenticatiemogelijkheden kan de chip elektronische documenten rechtsgeldig ondertekenen ("elektronische handtekening"). De toepassingen van e-ID zijn momenteel onder meer fiscaliteit, aangifte politie, *e-health*, e-loket van bepaalde steden en gemeenten, maar ze zijn in principe onbeperkt (*homebanking*, *e-commerce*, gezondheidszorg, …). Naar aanleiding van bepaalde foute krantenartikels benadrukt de heer Strickx dat de

articles erronés parus dans la presse, M. Strickx souligne que l'architecture de sécurité de l'eID a été conçue et contrôlée en collaboration avec divers chercheurs de la KUL (dont le Prof. Dumortier — voir *infra* — et le Département de Cryptographie).

En ce qui concerne l'eID et la vie privée, l'orateur souligne que si l'eID est un moyen sûr, elle ne constitue pas une garantie d'application sûre (autrement dit, comment l'application intègre-t-elle l'eID?). L'eID constitue en tout cas un élément clé dans le cadre de services d'e-government sécurisés.

En outre, les nouvelles eID sont munies d'un code-barres au verso. Ce code-barres est un numéro unique qui est indépendant du numéro de registre national. La carte peut dès lors être utilisée comme carte de fidélité ou comme autre moyen d'identification, sans qu'il soit fait usage du numéro de registre national, comme le proscrit la Commission de la protection de la vie privée. C'est l'utilisateur lui-même qui décide des données à caractère personnel qu'il acceptera ou refusera de relier à ce numéro unique.

Fedict envisage en effet d'intégrer la RFID à une nouvelle version de cartes d'identité. Le fonctionnement serait identique, prévoyant un numéro unique indépendant du numéro de registre national. Le titulaire doit lui-même (faire) établir la liaison avec ses données personnelles, faute de quoi ce numéro reste anonyme. Lors du remplacement de la carte d'identité électronique, toutes les traces sont effacées dès lors qu'un nouveau tag est créé. La liaison avec ces données devra alors être rétablie ou non. Du point de vue de la protection de la vie privée, il est dès lors préférable de prévoir une durée de validité de cinq ans plutôt que de dix ans pour les cartes d'identité.

Le professeur Jean Jacques Quisquater (UCL Crypto Group) s'est penché plus spécifiquement sur la protection des données électroniques à caractère personnel. En 2011, l'orateur souhaitait lancer explicitement une mise en garde, étant donné que l'on a affaire à des données à caractère personnel qui sont disponibles partout, peuvent être copiées immédiatement, avec des capacités de mémoire illimitées et permanentes et des méthodes de recherche efficaces à l'aide de mots clés (Google), d'une part, et, d'autre part, un trop grand nombre de données à caractère personnel, qui sont utilisées, voire traitées par des inconnus de manière non protégée. À cela, on peut encore ajouter: des objets intelligents tels que la RFID, les cartes à puce comme la carte MOBIB, l'eID, les caméras de surveillance et des objets du quotidien comme les voitures et les GSM, qui sont de plus en plus équipés de ces gadgets "intelligents".

beveiligingsarchitectuur van de e-ID werd ontworpen en geverifieerd in samenwerking met diverse onderzoekers van de KUL (waaronder professor Dumortier — zie verder — en het Departement Cryptografie).

Wat betreft e-id en privacy, benadrukt de spreker dat e-id een veilig middel is maar dat het geen garantie biedt op een veilige toepassing (met name over de integratie van e-id in de toepassing). E-id vormt in elk geval een sleutelbouwsteen voor beveiligde e-governmentdiensten.

De nieuwe eID's bevatten op de achterkant tevens een barcode. Deze barcode is een uniek nummer dat losstaat van het rijksregisternummer. Hierdoor kan de kaart worden gebruikt als klantenkaart of een ander identificatiemiddel zonder gebruik te maken van het rijksregisternummer, wat niet is toegelaten door de Privacycommissie. De gebruiker dient zelf te beslissen of en welke persoonsgegevens hij/zij al dan niet laat koppelen aan dat unieke nummer.

Fedict overweegt inderdaad om RFID te integreren in de nieuwe versie van de identiteitskaarten. Dit zou op dezelfde manier werken, met een uniek nummer los van het rijksregisternummer. De eigenaar dient zelf de koppeling met zijn/haar persoonsgegevens te (laten) maken, zoniet blijft dit een anoniem nummer. Wanneer de eID wordt vervangen, lopen meteen ook alle sporen dood omdat er een nieuwe tag komt. Dan zullen de gegevens opnieuw moeten worden gekoppeld, of net niet. Privacygewijs is een levensduur van 5 jaar voor identiteitskaarten dan ook te verkiezen boven een van 10 jaar.

Professor Jean Jacques Quisquater (UCL Crypto Group) ging meer specifiek in op de bescherming van elektronische persoonsgegevens. Spreker wenst anno 2011 uitdrukkelijk te waarschuwen, vermits er enerzijds sprake is van persoonsgegevens die overal beschikbaar zijn, onmiddellijk kopieerbaar, met onbeperkte en permanente geheugencapaciteiten en efficiënte opzoekingsmethoden met sleutelwoorden (Google) en anderzijds te veel onbeschermde persoonsgegevens die op een onbeschermde manier worden gebruikt en verwerkt door onbekenden. Men kan daar nog aan toevoegen: intelligente objecten als RFID, chipkaarten als MOBIB, e-id, bewakingscamera's, dagdagelijkse objecten als auto's en gsm's, die ook meer en meer zijn uitgerust met dergelijke "intelligente" snufjes.

S'ajoutent à cela une série de développements factuels récents tels que:

— interconnexion globale, rapide des personnes: ADSL, GSM, wifi: internet;
— stockage permanent, global, peu coûteux (*cloud computing*);
— moteurs de recherche (Google);
— géolocalisation (IP, GSM, voiture, …);
— processeurs et mémoires partout: cartes à puce (*smart card,* RFID, NFC, …), passeport, eID ;
— réseaux sociaux (Facebook, Twitter, Linkedin, …, Skype);
— bases de données ;
— *mobile mapping* (*Google Street*);
— Wikileaks et autres leaks.

Tous ces éléments démontrent l'importance de la cybersécurité et les menaces potentielles qui pèsent sur la protection de la vie privée.

En ce qui concerne l'eID, MOBIB et la RFID, l'intervenant formule les observations suivantes:

a. une carte sans contact n'est pas une version améliorée d'une carte avec contact; elle peut généralement être lue sans le consentement de l'utilisateur. Il convient de tenir compte de cet aspect;

b. l'anonymat dans le cadre du RFID est une question particulièrement délicate: une variabilité dans le design des antennes suffit à reconnaître un passeport, en dépit de tous les logiciels et crytages dont il est équipé;

c. une solution partielle si l'on recherche une solution "sans fil": disposer d'une sorte d'interrupteur nécessitant un geste du porteur pour activer l'objet;

d. ne pas accepter de standards fermés: ne pas savoir ce qu'il y a dans la carte est le meilleur moyen de se casser la figure très violemment à un moment. (IUn crytage bien étudié se dégrade généralement progressivement (DES, SHA, *etc*.), celui par obscurité tombe généralement d'un coup (Mifare, *etc*.));

e. il convient d'examiner pourquoi un standard comme Calypso (MOBIB, TEC?) se répand.

En ce qui concerne la protection de la vie privée en général, l'intervenant formule les observations suivantes:

Daarbovenop komen een aantal recente feitelijke ontwikkelingen zoals:

— alomvattende, snelle interconnectie tussen personen onderling: adsl, gsm, wifi internet;
— permanente en alomvattende opslag voor een lage kostprijs (*cloud computing*);
— zoekrobotten (Google);
— geolocalisatie (ip, gsm, wagen enzovoort);
— processoren en geheugens overal: chipkaarten (*smart card,* RFID, NFC enzovoort), passen, e-id;
— sociale netwerken (facebook, twitter, LinkedIn enzovoort, skype);
— databanken;
— mobile mapping (*Google Street*);
— Wikileaks en andere leaks.

Dit alles toont het belang aan van de zogenaamde "*cybersecurity*" en de potentiële bedreigingen voor de privacy.

Wat E-id, MOBIB en RFID betreft, maakt de spreker volgende opmerkingen:

a. een contactloze kaart is geen verbeterde versie van een contactkaart; doorgaans kan ze worden gelezen zonder de toestemming van de gebruiker. Daarmee moet rekening worden gehouden;

b. anonimiteit op RFID is een uiterst heikele zaak: louter door de uiteenlopende antenneontwerpen kan een pas worden herkend, ondanks alle software en versleuteling waarmee ze is uitgerust;

c. gedeeltelijke oplossing als men naar een "draadloze" oplossing streeft: beschikken over een soort van schakelaar die een gebaar van de drager vereist om het object te activeren;

d. geen gesloten standaarden aanvaarden: niet weten wat zich in de kaart bevindt, is de beste manier om op een bepaald moment stevig onderuit te gaan (een goed bestudeerde versleuteling geeft doorgaans gaandeweg haar geheimen prijs (DES, SHA enzovoort), maar de cryptografie die berust op de "*security through obscurity*"-techniek gaat meestal als één geheel voor de bijl (Mifare enzovoort));

e. nagaan waarom een standaard als Calypso (MOBIB, TEC?) uitbreiding neemt.

Wat de privacybescherming in het algemeen betreft, maakt spreker volgende opmerkingen:

— la cryptographie s'est développée à un tel point que beaucoup de choses inconcevables sur un support papier sont maintenant possibles sur un support numérique (ZK, crédits anonymes, et bientôt chiffrement fonctionnel);

— la vie privée ne peut être considérée comme une "couche" greffée au-dessus d'un système: une seule brèche provoquerait l'effondrement du système entier;

— le protection de la vie privée doit être intégrée à la conception (tout comme la sécurité, d'ailleurs);

— nécessité d'être clair sur ce qu'on veut. Anonymat et intraçabilité ne sont pas la même chose, mais on demande souvent l'anonymat alors qu'on veut l'intraçabilité.

— de bonnes solutions sont souvent empêchées lors d'appels d'offres (marchés publics, …) par ignorance: des personnes n'imaginant pas qu'il y a moyen de bien faire les choses écrivent un cahier de charges qui au final empêche de bien faire les choses (difficulté vient du fait qu'on spécifie souvent comment le système doit fonctionner plutôt que les propriétés qu'il doit garantir).

— utilité d'un genre d'ANSSI[2] en Belgique: quelques experts qui font de la veille technologique, vont aux conférences, produisent des recommandations, aident le gouvernement dans ses cahiers de charges, … Usages: Mobib, *e-health*, vote électronique, communications diplomatiques, *etc*. Nécessité d'une action des pouvoirs publics: il est plus coûteux de faire les choses convenablement, et les industriels ne le feront probablement pas si on ne les y encourage pas.

— la Belgique est l'un des pays les mieux armés en compétences crypto au monde, il faut en profiter, ces compétences étant reconnues mondialement.

Et encore:

— absolue nécessité d'indépendance de la Commission vie Privée (CPVP);

— importance dans les entreprises et administrations d'avoir des préposés à la protection des données (leur existence est prévue depuis 1998 et pourtant aucun arrêté royal n'a encore été pris), à ne pas confondre avec les délégués "Sécurité" de la Smals;

— donner des pouvoirs d'injonction et d'amendes à la CPVP soumis au contrôle des tribunaux;

— l'administration devrait être mieux contrôlée et pas uniquement par des comités sectoriels trop reliés aux administrations (voir *e-health* et la banque-Carrefour BCSS);

[2] Agence nationale de la sécurité des systèmes d'information (France).

— de cryptografie heeft zich dermate ontwikkeld dat veel zaken die niet mogelijk zijn op een papieren drager, nu wel digitaal mogelijk zijn (ZK, anonymous credentials, en binnenkort *functional encryption*);

— de persoonlijke levenssfeer mag niet worden beschouwd als een "laag" waarmee een systeem wordt toegedekt: één bres doet het hele systeem kapseizen;

— de privacy moet worden geïntegreerd in het ontwerp (net als de beveiliging overigens);

— men moet weten wat men wil. Anonimiteit is niet hetzelfde als onopspoorbaarheid; vaak wordt anonimiteit gevraagd terwijl men onopspoorbaarheid bedoelt;

— bij offerteaanvragen (overheidsopdrachten enzovoort) staat onwetendheid vaak goede oplossingen in de weg: mensen die een goede oplossing niet voor mogelijk houden, schrijven een bestek uit dat uiteindelijk zelf een goede oplossing verhindert (vaak wordt immers de werking zelf van het beoogde systeem beschreven in plaats van de eigenschappen die het mogelijk moet maken);

— nut van een soort ANSSI[2] in België: een groep deskundigen die aan technologische bewaking doet, naar conferenties gaat, aanbevelingen formuleert, de regering helpt bij het uitschrijven van de bestekken enzovoort. Toepassingen: Mobib, *e-Health*, elektronische stemming, diplomatieke communicatie enzovoort. Nood aan overheidsinitiatief: kwaliteit kost meer, maar zonder stimuli is de kans klein dat de industriëlen zelf het voortouw zullen nemen;

— België heeft een uitstekende reputatie op het vlak van cryptologie; onze *knowhow* ter zake wordt wereldwijd erkend en daar moet gebruik van worden gemaakt.

Voorts:

— de Privacycommissie (CBPL) moet volstrekt onafhankelijk kunnen werken;

— ondernemingen en overheidsdiensten moeten kunnen beschikken over gegevensbeschermingsambt enaren(deze functie bestaat bij wet sinds 1998,maar er werd nog geen koninklijk besluit uitgevaardigd),die niet mogen worden verward met de veiligheidsafgevaardigden bij Smals;

— de CBPL moet, onder het toezicht van de rechtbanken, kunnen beschikken over injunctie- en sanctiebevoegdheden;

— overheidsdiensten zouden beter moeten worden gecontroleerd, niet alleen door sectorcomités die te dicht bij die diensten staan (*cf*. *e-Health* en de Kruispuntbank KSZ);

[2] *Agence nationale de la sécurité des systèmes d'information* (Frankrijk)

— revenir sur des dossiers comme le numéro de registre national unique (non sectoriel) et l'usage commercial de la carte d'identité;

— mettre en évidence les solutions "PETS" (*Privacy Enhancing Technologies*) mais surtout le *Privacy impact Assessment*, obliger les entreprises et administrations à avoir une privacy policy accessible sur le Net et dans toute la mesure un accès électronique aux données;

— lancer des campagnes d'information sur les risques liés aux réseaux sociaux et certaines technologies (RFID, *etc*.);

— généraliser par loi la responsabilité des responsables de traitement pour *security breach*.

M. Dumortier (KUL) évoque pour commencer la technique de la RFID, ainsi qu'un certain nombre d'applications (voir supra). Il examine ensuite plusieurs aspects de la protection des données en matière de RFID et des éventuelles menaces ou exigences en matière de protection de la vie privée et de sécurité. Il renvoie notamment à la directive "protection des données" (DIR 1995/46/CE) et à la directive européenne (DIR 2002/58/CE), ainsi qu'à une série de principes fondamentaux en matière de protection des données et de traitement des données personnelles (cf. infra).

Les citoyens devraient en tout cas être informés, par le biais d'un logo — à l'instar des radars automatiques — de la présence d'un tag RFID. Il est essentiel, en outre, que l'utilisateur puisse disposer d'un droit de recours ou refuser d'utiliser l'application ("*withdraw*"), par le biais d'un mécanisme "*enable*/*disable*" ou d'une "*kill command*".

Solutions possibles:

— mécanismes de désactivation;

— initiatives de standardisation afin de minimiser la collecte et l'utilisation de données à caractère personnel;

— munir les "*tags*" de mots de passe;

— cryptage;

— blindage des "*tags*";

— "*privacy enhancing technologies*" (technologies renforçant la protection de la vie privée), comme la possibilité de neutraliser temporairement le *tag*.

— "*privacy-enhanced identity management solutions*".

En ce qui concerne une éventuelle réaction législative, l'orateur renvoie à une recommandation du 12 mai 2009 de la Commission européenne: "Recommandation de la commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de

— dossiers als het (niet-sectoraal) uniek rijksregisternummer en het commerciële gebruik van de identiteitskaart moeten opnieuw ter tafel komen;

— de aandacht moet worden gevestigd op PETS-oplossingen (*Privacy Enhancing Technologies*), maar vooral op *Privacy Impact Assessment*; ondernemingen en overheidsdiensten moeten hun privacybeleid kenbaar maken op het internet en altijd elektronische toegang mogelijk maken tot de gegevens;

— er moeten voorlichtingscampagnes komen over de risico's die gepaard gaan met sociale netwerken en bepaalde technologieën (RFID, enzovoort);

— er moet worden voorzien in een algemene wettelijke regeling om ook *security breach* op te nemen in het takenpakket van de verantwoordelijken voor de gegevensverwerking.

De heer Dumortier (KUL) gaat eerst in op de techniek van RFID evenals op een aantal toepassingen (zie ook reeds supra). Vervolgens gaat de spreker in op een aantal aspecten van databescherming inzake RFID en mogelijke bedreigingen en vereisten over de privacy en veiligheid. Hij verwijst onder meer naar de databeschermingsrichtlijn (RL 1995/46/EEG) en de Europese richtlijn (RL 2002/58/EG) evenals naar een aantal essentiële principes inzake databescherming en verwerking van persoonsgegevens (zie verder).

In elk geval zouden de burgers door middel van een logo — zoals voor flitscamera's — dienen te worden geïnformeerd over de aanwezigheid van een RFID-tag. Daarnaast is het essentieel dat de gebruiker een recht heeft om bezwaar te maken of de toepassing niet te gebruiken ("*withdraw*"), ofwel met een "*enable*/*disable* mechanisme" ofwel een "*kill command*".

Mogelijke oplossingen:

— deactiveringsmechnismen;

— initiatieven van standaardisering om het verzamelen en het gebruik van persoonsgegevens te minimaliseren;

— passwoorden in de "*tags*";

— encryptie;

— "*shielding*" van de "*tags*";

— "*privacy enhancing technologies*" of "privacy bevorderende technologieën" (zoals de mogelijkheid om de "*tag*" tijdelijk uit te schakelen).

— "*privacy-enhanced identity management solutions*".

Wat een mogelijke wetgevende respons betreft, verwijst spreker naar een aanbeveling van 12 mei 2009 van de Europese Commissie: "Aanbeveling van de Commissie van 12 mei 2009 over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke

protection des données dans les applications reposant sur l'identification par radiofréquence", Commission des Communautés européennes, 12 mai 2009, C(2009) 3200, disponible à l'adresse suivante:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:FR:PDF

M. Dumortier est opposé à toute initiative législative relative à la RFID. Il s'oppose fermement à l'adoption éventuelle de règles spécifiques qui s'appliqueraient à la RFID. Par contre, il est favorable à la pratique actuelle consistant à appliquer les principes de la loi du 8 décembre 1992 sur la protection de la vie privée à toute nouvelle technologie. Il appartient à la CPVP ou aux universitaires de donner des directives concernant la manière dont ces principes doivent être appliqués[3]. La protection de la vie privée est d'ailleurs une matière qui échappe de plus en plus au législateur national et qui doit être traitée au niveau du réseau même, donc sur l'internet. En ce qui concerne l'implantation éventuelle de puces RFID sous la peau humaine, l'orateur confirme que certains États américains ont élaboré une législation en la matière. L'orateur confirme également que l'évolution dans le cadre de laquelle une puce RFID serait insérée dans l'e-ID, ainsi qu'il a été annoncé par FEDICT, est inévitable et évidente eu égard à l'énorme potentiel. Il faut toutefois rester conscient des risques qui y sont liés, même si l'e-ID est suffisamment sécurisée en ce qui concerne la lecture des données qu'elle contient.

M. Pascal Poty (Agence wallonne des télécommunications) fait observer que la protection des données personnelles est un élément central de notre vie numérique: la question de la protection des données personnelles dépasse celle de la simple technologie RFID. En effet, le droit est confronté à une avalanche technologique qui s'articule autour de quatre éléments: capacité de stockage, puissance de calcul, large bande et volume de données produites. Il renvoie ensuite aux principes fondamentaux de la législation européenne et de la législation belge en matière de vie privée, ainsi qu'aux différences d'approche, à cet égard, entre l'Union européenne (cadre réglementaire et légal fort) et les États-Unis (où les forces du marché et l'autorégulation jouent un rôle primordial). Toutefois, les grands acteurs sont établis aux États-Unis. Il souligne en outre que plusieurs modifications successives ont été apportées à la législation sur la protection des données personnelles afin de tenter de l'adapter à la révolution technologique. Dans la sphère numérique, la protection des données personnelles a pris une nouvelle signification qui se décline, selon l'orateur, sous la forme de trois droits

[3] L'orateur renvoie, en l'occurrence, aux 2 avis rendus en la matière par la CPVP.

levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen", Commissie van de Europese Gemeenschappen,12 mei 2009, C(2009) 3200, beschikbaar op:

http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:200 9:122:0047:0051:NL:PDF.

De heer Dumortier is een tegenstander van wetgevende initiatieven voor RFID. Hij kant zich scherp tegen eventuele specifieke regels die van toepassing zouden zijn op RFID. Hij is wel voorstander van de huidige praktijk waarbij de principes uit de wet van 8 december 1992 op de bescherming van de persoonlijke levenssfeer worden toegepast op elke nieuwe technologie. Het komt aan de CBPL of aan academici toe om richtlijnen te geven over de toepassing van deze principes[3]. De bescherming van het privéleven is trouwens een materie die meer en meer ontsnapt aan de nationale wetgever en die zich moet afspelen op het niveau van het netwerk zelf, dus op het internet. Wat de eventuele inplanting van RFID-chips onder de menselijke huid betreft, bevestigt spreker dat bepaalde Amerikaanse staten hieromtrent wetgeving hebben ontwikkeld. Spreker bevestigt ook dat de evolutie waarbij een RFID-chip zou worden opgenomen in de e-id zoals aangekondigd door FEDICT — onvermijdelijk is en vanzelfsprekend door het enorme potentieel. Men dient zich niettemin bewust te blijven van de hieraan verbonden risico's, zelfs als de e-id voldoende beveiligd is tegen de lezing van de gegevens die ze bevat.

De heer Pascal Poty (*Agence wallonne de télécommunications*) merkt op dat de bescherming van persoonsgegevens centraal staat in ons digitale leven: de vraag naar de bescherming van persoonsgegevens overstijgt de loutere RFID-technologie. Het recht wordt immers geconfronteerd met een technologische lawine die berust op 4 pijlers: opslagcapaciteit, rekenkracht, breedband en het volume aan geproduceerde gegevens. Hij verwijst vervolgens naar de fundamentele principes van de Europese en Belgische privacywetgeving, evenals de verschillende benadering ter zake in de EU (sterke reglementaire en wetgevende omkadering) in vergelijking met de VS (hoofdrol voor de marktkrachten en autoregulering): de grote spelers zoals bijvoorbeeld Google, zijn echter gevestigd in de VS. Hij benadrukt verder dat de wetgeving op de bescherming van persoonsgegevens opeenvolgende evoluties heeft gekend om zich te proberen aan te passen aan de technologische revolutie. In de digitale omgeving geldt er een nieuwe betekenis voor de bescherming van persoonsgegevens die zich volgens spreker vertaalt in 3 onuitgegeven rechten, zoals het recht voor elke internaut om

[3] De spreker verwijst hier naar de 2 adviezen die hierover werden uitgebracht door de CPBL.

inédits, à savoir le droit de chaque internaute de gérer son propre "capital de vie privée", le droit à la protection des données personnelles au travail et le droit à l'oubli. La protection juridique est boiteuse en raison de l'absence de prise de conscience de cette problématique et d'action démocratique, d'une part, et des difficultés que suscite l'adaptation du cadre juridique aux rapides évolutions technologiques, d'autre part. Des actions possibles consisteraient à coopérer avec les grands acteurs du secteur des réseaux sociaux (comme Facebook) et à éduquer/conscientiser les internautes. Une approche alternative importante est celle de la "*privacy by design*", c'est-à-dire de la protection de la vie privée dès la conception des applications et des produits et jusqu'à leur recyclage ("e-déchets"). Cela peut passer, par exemple, par le "*opt in*" ou par l'effacement des données après un délai raisonnable afin de minimaliser la collecte et le traitement des données personnelles durant toute la vie du "produit".

En ce qui concerne les systèmes sans contact tels que la RFID, l'orateur fait notamment observer que ces services offrent souvent un grand confort aux citoyens, de sorte que leur mise en place a lieu dans un climat de large acceptation sociale et sans guère de débat démocratique. Du point de vue juridique, le problème qui se pose est de savoir comment concilier le principe juridique de l'"*opt in*" (consentement explicite, informé et révocable au cas par cas) avec la nature intrinsèquement invisible des échanges de données dans "le silence des puces". L'évolution technologique rendra les systèmes de collecte et de traitement de données invisibles et indétectables: il est essentiel de s'y préparer.

L'orateur conclut en indiquant que nous sommes définitivement passés d'un environnement technologico- juridique basé sur la protection de l'individu à un environnement basé sur la maîtrise des données. Dans ce contexte, il est essentiel d'éduquer et de sensibiliser les citoyens aux défis relatifs à la vie privée.

zijn eigen "kapitaalprivéleven" te beheersen, het recht op bescherming van persoonsgegevens op het werk en het recht op vergetelheid ("*oubli*"). De juridische bescherming loopt mank wegens een gebrek aan bewustzijn van de problematiek en van democratische actie enerzijds en anderzijds de moeilijke aanpassing van het juridische kader aan de snelle technologische evoluties. Mogelijke acties zijn de samenwerking met de grote actoren aan de sociale netwerken (zoals Facebook) en de opvoedingbewustmaking van de internauten. Een belangrijke alternatieve benadering is "*privacy by design*", namelijk de bescherming van het privéleven vanaf de conceptie van applicaties en producten tot aan hun recyclage ("e-afval"). Dit kan bijvoorbeeld gebeuren via "*opt-in*" of via de uitwissing van gegevens na een redelijke periode, teneinde tijdens de hele levensduur van het "product" de verzameling en verwerking van persoonsgegevens te minimaliseren.

In verband met de contactloze systemen zoals RFID merkt spreker onder andere op dat deze diensten vaak een groot comfort bieden aan de burger, zodat de invoering ervan gebeurt in een klimaat van ruime sociale aanvaarding en een zwak democratisch debat. Juridisch stelt zich het probleem hoe men het juridische principe van "*optin*" (expliciete, geïnformeerde, herroepbare, geval per geval-instemming) kan verzoenen met de intrinsiek onzichtbare aard van gegevensuitwisselingen in een "pervasieve CT-omgeving ("*le silence des puces*"). De technologische evolutie zal de systemen voor gegevensverzameling en -bewerking onzichtbaar en ondetecteerbaar maken: het is essentieel om zich hierop voor te bereiden.

De spreker besluit dat we definitief zijn overgegaan van een technologisch-juridische omgeving gebaseerd op de bescherming van het individu naar een omgeving gebaseerd op de beheersing van de gegevens ("*la maîtrise des données*"). In deze optiek is opvoeding en sensibilisering van burgers aangaande de privacyproblematiek essentieel.

Peter DEDECKER (N-VA)
Bert WOLLANTS (N-VA)
Steven VANDEPUT (N-VA)
Min DE RIDDER (N-VA)
Kristien VAN VAERENBERGH (N-VA)

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. vu l'importance essentielle des TIC (technologies de l'information et de la communication) pour l'innovation et la compétitivité de notre économie, ainsi que pour la fourniture d'un service moderne par les autorités ("*e-government*");

B. considérant que la RFID (*Radio Frequency Identification* — Identification par radiofréquence) est une technologie relativement récente, qui est cependant en plein essor et qui offre diverses possibilités d'accès très prometteuses;

C. considérant que la technologie est, dans beaucoup de secteurs, utilisée à des fins diverses, notamment dans les transports (système MOBIB à Bruxelles, clés de voiture équipées d'un tel système ou "transpondeur"), la navigation aérienne (traitement des bagages, "*boarding passes*"), la sécurisation du contrôle d'accès (passeports comme le passeport belge, accès à certains espaces au moyen d'une "*smart card*"), le secteur de la distribution et de la production (gestion des stocks, suivi de la production dans la chaîne logistique, procédure accélérée aux caisses, sécurisation contre le vol, *etc.*);

D. considérant qu'à côté des avantages manifestes, les applications RFID présentent également un certain nombre d'inconvénients potentiels, en l'occurrence des implications éventuelles sur la vie privée, qui ont notamment été décrites par la CPVP dans les deux avis qu'elle a rendus sur la question;

E. souligne qu'il est ressorti des auditions que les éventuelles implications de la RFID sur la vie privée peuvent être renforcées par les évolutions technologiques de plus en plus rapides du monde numérique, qui sont déterminées par l'augmentation de la capacité de stockage, la capacité de calcul, le haut débit et le volume de données produites, ainsi que par l'augmentation du nombre "d'objets intelligents" ("internet des objets");

F. constatant que l'évolution technologique rend les systèmes de collecte et de traitement de données de plus en plus invisibles et indétectables, de sorte qu'il est essentiel de s'y préparer;

G. considérant que la vie privée ne peut être considérée comme un élément supplémentaire qui est ajouté à un système (une brèche fait capoter l'ensemble du système), mais qu'elle doit être intégrée en tant que concept dans le système dès la conception (tout comme la sécurité d'ailleurs) ("*Privacy by design*");

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op het essentiële belang van ICT (Informatie- en communicatie-technologieën) voor de innovatie en het concurrentievermogen van onze economie, evenals voor een moderne dienstverlening van de overheid ("*e-government*");

B. gelet op het feit dat RFID (*Radio Frequency Identification* — Identificatie door radiogolven) een relatief recente technologie is, die echter in volle ontwikkeling is, met diverse en veelbelovende toegangsmogelijkheden;

C. overwegende dat de technologie in vele sectoren voor diverse doeleinden wordt aangewend, zoals onder meer transport (MOBIB-systeem in Brussel, autosleutels uitgerust met een dergelijk systeem of "*transponder*"); luchtvaart (verwerken van bagage, "*boarding passes*"), beveiliging toegangscontrole (paspoorten zoals de Belgische reispas; toegang tot bepaalde ruimten met een zogenaamde "*smart card*"); distributie- en productiesector (stockbeheer; volgen van productie binnen logistieke keten; snellere afrekening aan de kassa; diefstalbeveiliging;…);

D. overwegende dat naast de manifeste voordelen van RFID-toepassingen, er ook een aantal potentiële nadelen zijn, met name mogelijke privacyimplicaties, die onder meer werden beschreven door de CBPL in twee adviezen hierover;

E. wijst erop dat uit de hoorzittingen is gebleken dat mogelijke privacyimplicaties van RFID kunnen worden versterkt door de steeds snellere technologische evoluties in de digitale wereld, die worden bepaald door de toename van de opslagcapaciteit, rekenkracht, breedband en het volume aan geproduceerde gegevens en aan de toename van het aantal "intelligente objecten" ("*internet of things*");

F. vaststellende dat de technologische evolutie de systemen voor gegevensverzameling- en bewerking steeds meer onzichtbaar en ondetecteerbaar maakt, waardoor het essentieel is zich hierop voor te bereiden;

G. overwegende dat privacy niet mag worden gezien als een bijkomende laag die bovenop een systeem wordt aangebracht (één bres doet het hele systeem kapseizen), maar als concept dient geïntegreerd in het systeem vanaf de conceptie (zoals trouwens ook de veiligheid) ("*Privacy by design*");

H. considérant qu'avec l'introduction de l'eID, notre pays a fait œuvre de pionnier en Europe et est devenu la référence par excellence, ainsi qu'un exemple pour les autres pays en matière de modernisation des autorités.

I. vu l'arrêt de la Cour européenne de justice[4] qui précise: "Il s'ensuit que, lors de l'exercice de leurs missions, les autorités de contrôle doivent agir de manière objective et impartiale. À cet effet, elles doivent être à l'abri de toute influence extérieure, y compris celle, directe ou indirecte, de l'État ou des Länder, et pas seulement de l'influence des organismes contrôlés";

J. vu l'observation[5] de l'Agence des droits fondamentaux de l'Union européenne:

"*Finally, other Member states (e.g. France, Spain, Portugal, Belgium) provide for a combined procedure to nominate the officers of the national Data Protection Authority, involving the executive, the legislature and the judiciary or other organized societal groups (e.g. the Supreme Council of the Universities in Spain) at the same time. In similar cases, however, it is essential to ensure that the Government does not, in practice, control directly or indirectly the majority of the appointees, thus effectively frustrating the purpose of a pluralistic nomination procedure.*";

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. en tant qu'autorité fédérale, de prendre l'initiative d'utiliser les nouvelles technologiques, telles que la RFID, afin d'exploiter pleinement les opportunités qu'elles offrent de devenir un service public plus convivial et plus efficace, tout en excellant en tant que référence en matière de protection de la vie privée. L'autorité fédérale doit prendre la tête dans ce domaine et montrer le bon exemple tant au pays qu'à l'étranger. À cet égard, il s'agit de soutenir le déploiement d'un *tag* RFID anonyme sur l'eID;

2. de permettre également un déploiement rapide d'un éventuel tag RFID sur l'eID, y compris pour les anciennes cartes sans les remplacer, par exemple en

H. gelet op het feit dat ons land met de invoering van de eID in Europa het voortouw nam en uitgroeide tot dè referentie en een voorbeeld voor andere landen inzake modernisering van de overheid;

I. overwegende het arrest van het Europees Hof van Justitie[4] dat stelt dat "Bij de uitoefening van hun taken moeten de toezichthoudende autoriteiten bijgevolg objectief en onpartijdig handelen. Daartoe moeten zij vrij zijn van beïnvloeding van buitenaf, daaronder begrepen de — rechtstreekse of indirecte — beïnvloeding door de staat of de Länder, en niet enkel van beïnvloeding door de organen waarop zij toezicht uitoefenen";

J. overwegende de opmerking[5] van het *European Union Agency for Fundamental Rights*:

"*Finally, other Member states (e.g. France, Spain, Portugal, Belgium) provide for a combined procedure to nominate the officers of the national Data Protection Authority, involving the executive, the legislature and the judiciary or other organized societal groups (e.g. the Supreme Council of the Universities in Spain) at the same time. In similar cases, however, it is essential to ensure that the Government does not, in practice, control directly or indirectly the majority of the appointees, thus effectively frustrating the purpose of a pluralistic nomination procedure.*";

VERZOEKT DE FEDERALE REGERING:

1. als federale overheid het voortouw te nemen in het werken met nieuwe technologieën, zoals RFID, om ten volle de kansen te benutten die deze bieden om te komen tot een gebruiksvriendelijkere en efficiëntere overheid, hierbij uitblinkend als referentie inzake privacy. De federale overheid moet een koppositie innemen en het goede voorbeeld geven aan binnen- en buitenland. De uitrol van een anonieme RFID-*tag* op de eID dient in deze te worden ondersteund;

2. een snelle uitrol mogelijk te maken van een eventuele RFID-tag op de eID, ook voor oudere kaarten zonder deze te vervangen, door bijvoorbeeld stickers ter

4 Arrêt de la Cour (Grande Chambre) du 9 mars 2010, Commission européenne contre République fédérale d'Allemagne, manquement à la directive 95/46/CE Protection des personnes physiques à l'égard du traitement des données à caractère personnel et libre circulation de ces données — Article 28, paragraphe 1er, autorités nationales de contrôle — indépendance — tutelle administrative exercée sur ces autorités. Affaire C-518/07.

5 FRA — *European Union Agency for Fundamental Rights, 2010, Strengthening the fundamental rights architecture in the EU, II Data protection in the European Union: the role of National Data Protection Authorities*, ISBN: 978-92-9192-509-4, DOI: 10.2811/47216

4 Arrest van het Hof (Grote Kamer) van 9 maart 2010, Europese Commissie tegen de Bondsrepubliek Duitsland, Niet nakoming van richtlijn 95/46/EG Bescherming van natuurlijke personen bij de verwerking van persoonsgegevens en vrij verkeer van deze gegevens — artikel 28, eerste lid, nationale toezichthoudende instanties — onafhankelijkheid — overheidstoezicht op deze instanties. Zaak C – 518/07.

5 FRA — *European Union Agency for Fundamental Rights, 2010, Strengthening the fundamental rights architecture in the EU, II Data protection in the European Union: the role of the National Data Protection Authorities*, ISBN: 978-92-9192-509-4, DOI: 10.2811/47216.

proposant des autocollants. Avec une telle campagne, les citoyens pourront rapidement découvrir les possibilités de la RFID et le débat pourra être lancé afin de sensibiliser le grand public à son impact;

3. de donner suite aux recommandations de la Commission européenne du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence: cette recommandation donne aux États membres des indications sur les moyens de concevoir et d'exploiter les applications RFID de façon licite, éthique et socialement et politiquement acceptable, en respectant le droit à la vie privée et en assurant la protection des données à caractère personnel:

4. en veillant à ce que les entreprises, en collaboration avec les parties intéressées de la société civile, élaborent un cadre d'évaluation de l'impact sur la protection des données et de la vie privée;

5. d'aider la Commission européenne à déterminer quelles applications pourraient présenter un risque pour la sécurité de l'information ayant des conséquences pour le grand public. Concernant ces applications, les États membres doivent veiller à ce que les exploitants, avec les autorités compétentes nationales et les organisations de la société civile, élaborent de nouveaux systèmes ou appliquent des systèmes existants, comme la certification ou l'autoévaluation par l'exploitant, afin de démontrer que le niveau de sécurité de l'information et de protection de la vie privée est approprié aux risques évalués;

6. de veiller, conformément aux directives 95/46/CE et 2002/58/CE, à ce que les exploitants élaborent et rendent publique, pour chacune de leurs applications, une politique d'information concise, précise et aisément compréhensible;

7. de veiller à ce que les exploitants prennent des mesures pour informer les personnes de la présence de lecteurs, au moyen d'un signe européen commun élaboré par des organismes européens de normalisation avec l'aide des parties concernées. Le signe doit indiquer l'identité de l'exploitant et un point de contact auquel les personnes peuvent se procurer des informations concernant l'application;

8. au moyen d'un signe européen commun élaboré par des organismes européens de normalisation en collaboration avec les parties concernées, les exploitants

beschikking te stellen. Met dergelijke campagne kunnen alle burgers de mogelijkheden van RFID snel ontdekken en kan het debat worden aangezwengeld om een groot publiek bewust te maken van de impact;

3. de aanbevelingen van de Europese Commissie van 12 mei 2009 over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen te implementeren: deze aanbeveling verschaft de lidstaten richtsnoeren over ontwerp en werking van RFID-toepassingen op een rechtmatige, ethische, sociale en politiek aanvaardbare manier met inachtneming van het recht op privacy en met waarborging van persoonsgegevens:

4. ervoor te zorgen dat de industrie, samen met de relevante belanghebbenden uit het maatschappelijk middenveld, een kader ontwikkelen voor effectbeoordeling op het gebied van persoonlijke levenssfeer en beveiliging;

5. de Europese Commissie te steunen bij het identificeren van toepassingen die de informatiebeveiliging zouden kunnen bedreigen met gevolgen voor het grote publiek. Voor dergelijke toepassingen dienen de lidstaten ervoor te zorgen dat exploitanten, samen met de nationale bevoegde autoriteiten en maatschappelijke organisaties, nieuwe regelingen ontwikkelen of bestaande regelingen toepassen zoals certificering of zelfbeoordeling van de exploitant om aan te tonen dat er ten aanzien van de vastgestelde risico's een aangepast niveau bestaat van informatiebeveiliging en bescherming van de persoonlijke levenssfeer;

6. er overeenkomstig de richtlijnen 95/46/EG en 2002/58/EG voor te zorgen dat exploitanten een beknopt, nauwkeurig en eenvoudig te begrijpen informatiebeleid ontwikkelen en bekendmaken voor elk van hun toepassingen;

7. ervoor te zorgen dat exploitanten stappen nemen om personen op de hoogte te brengen van de aanwezigheid van lezers met een gemeenschappelijk Europees kenmerk, dat ontwikkeld is door de Europese normaliseringsorganisaties met steun van de betrokken belanghebbenden. Dit kenmerk dient de naam van de exploitant te vermelden en een contactadres waar informatie kan worden verkregen over de toepassing;

8. met een gemeenschappelijk Europees kenmerk, ontwikkeld door Europese normaliseringsorganisaties, in samenwerking met de betrokken belanghebbenden,

doivent informer les citoyens de la présence d'étiquettes placées sur les produits ou incorporées à ceux-ci;

9. les détaillants doivent désactiver ou retirer, au point de vente, les étiquettes de leur application, à moins que les consommateurs acceptent que les étiquettes restent opérationnelles. Par désactivation des étiquettes, on entend tout processus qui interrompt les interactions d'une étiquette avec son environnement et qui n'exige pas de participation active du consommateur. La désactivation ou le retrait des étiquettes par le détaillant doivent être effectués sur-le-champ et sans coût pour le consommateur. Les consommateurs doivent pouvoir vérifier que la désactivation ou le retrait sont effectifs;

10. en collaboration avec l'industrie, la Commission et d'autres parties intéressées, de prendre les mesures appropriées pour informer les pouvoirs publics et les entreprises des avantages et des risques potentiels liés à la technologie RFID et pour les y sensibiliser. Il convient d'accorder une attention particulière aux questions de sécurité de l'information et de respect de la vie privée;

11. en collaboration avec l'industrie, les associations de la société civile, la Commission et d'autres acteurs intéressés pertinents, de recenser et de fournir des exemples de bonne pratique dans la mise en œuvre d'applications RFID afin d'informer et de sensibiliser davantage le grand public. Préalablement à une plus large adoption de la technologie RFID, il y a également lieu de prendre les mesures appropriées, comme le lancement de projets pilotes à grande échelle, pour sensibiliser davantage le public à la technologie RFID et aux avantages, risques et conséquences de son utilisation;

12. de collaborer avec l'industrie, les acteurs intéressés pertinents de la société civile et la Commission afin de promouvoir et de favoriser l'intégration du principe de "sécurité et de respect de la vie privée assurés dès la conception" à un stade précoce du développement des applications RFID;

13. de veiller à ce que les applications informatiques soient, dès leur conception, développées de manière à ce qu'un minimum absolu de données à caractère personnel soient collectées ou à ce que ces données soient (automatiquement) effacées après un certain temps;

14. d'accroître l'indépendance et les compétences de la CPVP en prévoyant entre autres, un droit d'injonction et la possibilité d'infliger des amende;

dienen exploitanten burgers op de hoogte te brengen van de aanwezigheid van tags die zijn geplaatst op of zijn ingebed in producten;

9. kleinhandelaren dienen tags die op de plaats van verkoop worden gebruikt in hun toepassing te deactiveren of te verwijderen tenzij consumenten, hiervoor wel toestemming verlenen. Onder deactivering van tags wordt verstaan elk proces dat de interactie van een tag met zijn omgeving stopt waarvoor geen actieve betrokkenheid van de consument nodig is. Deactivering of verwijdering van tags door de kleinhandelaar dient onmiddellijk te gebeuren zonder dat hieraan voor de consument kosten mogen zijn verbonden. Consumenten moeten kunnen verifiëren of de deactivering of verwijdering doeltreffend is;

10. in samenwerking met de industrie, de Commissie en andere belanghebbenden passende maatregelen te nemen om overheden en ondernemingen voorlichting te verschaffen en bewust te maken van de potentiële voordelen en risico's van RFID-technologie. Bijzondere aandacht moet worden verleend aan de beveiliging van informatie en de persoonlijke levenssfeer;

11. in samenwerking met de industrie, verenigingen uit het maatschappelijk middenveld, de Commissie en andere relevante belanghebbenden, voorbeelden te verschaffen en bekend te maken van goede praktijken bij de tenuitvoerlegging van RFID-toepassingen om het grote publiek voorlichting te verschaffen en meer bewust te maken. Om deze technologie op bredere schaal in te voeren, dienen zij passende maatregelen te nemen om het publiek voor te lichten over RFID-technologie, de voordelen, risico's en gevolgen van het gebruik;

12. samen te werken met de industrie, relevante belanghebbenden uit het maatschappelijk middenveld en de Commissie om de invoering van het beginsel van ingebouwde zekerheid en privacy in een vroeg stadium van de ontwikkeling van RFID-toepassingen te steunen;

13. erop toe te zien dat informaticatoepassingen vanaf hun conceptie zó wordt ontwikkeld dat een absoluut minimum aan persoonsgegevens worden ingezameld, desnoods deze gegevens (automatisch) worden gewist na verloop van een bepaalde periode;

14. de onafhankelijkheid en de bevoegdheden van de CBPL te vergroten met onder andere een injunctierecht en de mogelijkheid om boetes op te leggen;

15. de remplacer la désignation des membres de la Commission de la protection de la vie privée par le biais de l'établissement de listes doubles de candidats présentées au Parlement par un système excluant l'ingérence du pouvoir exécutif dans la composition de la commission;

16. de fournir des efforts en vue de développer une vision interdépartementale assurant un équilibre entre l'innovation et la protection de la vie privée;

17. de mettre à profit, dans ce contexte, l'expertise belge reconnue en matière de cryptographie;

18. de veiller à ce que la protection de la vie privée figure de façon adéquate en tant que critère important dans les cahiers des charges établis dans le cadre d'adjudications publiques et à ce que ces derniers soient ouverts aux nouvelles technologies et aux solutions innovantes;

19. de veiller à ce que des préposés à la protection des données à caractère personnel (fonction dont la création remonte déjà à 1998) soient mis en place au sein des entreprises et des administrations;

20. de souligner dans ce contexte l'importance des "*Privacy Enhancing Technologies*" (technologies de protection de la vie privée) et en particulier des "*Privacy Impact Assessments*", et d'obliger les entreprises et les administrations à développer une "*privacy policy*" pouvant être consultée sur internet;

21. d'utiliser exclusivement des standards ouverts dans sa propre application et d'examiner si leur utilisation peut être imposée aux exploitants privés;

24 décembre 2012

15. de aanstelling van de Privacycommissie via de opmaak en het voorleggen aan het parlement van dubbele kandidatenlijsten te vervangen door een systeem dat inmenging van de uitvoerende macht in de samenstelling van de commissie uitsluit;

16. inspanningen te doen om te komen tot de ontwikkeling van een interdepartementale visie met een evenwicht tussen enerzijds innovatie en anderzijds privacybescherming;

17. in deze context gebruik te maken van de erkende Belgische expertise inzake cryptografie;

18. erop toe te zien dat de lastenboeken bij openbare aanbestedingen open staan voor nieuwe technologieën en innovatieve oplossingen en op passende wijze privacybescherming opnemen als een belangrijk criterium;

19. ervoor te zorgen dat de (sinds 1998 geplande) aangestelden voor de bescherming van persoonsgegevens in ondernemingen en de administraties er komen;

20. in deze context het belang van "*Privacy Enhancing Technologies*" (privacybeschermende technologieën), vooral van "*Privacy Impact Assessments*" te benadrukken en ondernemingen en administraties te verplichten om een "*privacy policy*" te ontwikkelen die kan worden geraadpleegd op het internet;

21. in haar eigen toepassing uitsluitend gebruik te maken van open standaarden en te onderzoeken in hoeverre deze kunnen worden afgedwongen bij particulieren exploitanten.

24 december 2012

Peter DEDECKER (N-VA)
Bert WOLLANTS (N-VA)
Steven VANDEPUT (N-VA)
Min DE RIDDER (N-VA)
Kristien VAN VAERENBERGH (N-VA)

Imprimerie centrale – Cette publication est imprimée exclusivement sur du papier certifié FSC
Centrale drukkerij – Deze publicatie wordt uitsluitend gedrukt op FSC gecertificeerd papier