

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

20 juli 2002

VOORSTEL VAN RESOLUTIE

**inzake het aanscherpen van de privacy
bij de implementatie van het federale
e-government**

(ingediend door de heer Peter Vanhoutte
en de dames Kristien Grauwels, Zoé Genot
en Géraldine Pelzer-Salandra)

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

20 juillet 2002

PROPOSITION DE RÉSOLUTION

**relative au renforcement de la protection de
la vie privée lors de la mise en place
de l'e-government fédéral**

(déposée par M. Peter Vanhoutte
et Mmes Kristien Grauwels, Zoé Genot
et Géraldine Pelzer-Salandra)

AGALEV-ECOLO	:	Anders gaan leven / Ecologistes Confédérés pour l'organisation de luttes originales
CD&V	:	Christen-Democratisch en Vlaams
FN	:	Front National
MR	:	Mouvement Réformateur
PS	:	Parti socialiste
cdH	:	Centre démocrate Humaniste
SP.A	:	Socialistische Partij Anders
VLAAMS BLOK	:	Vlaams Blok
VLD	:	Vlaamse Liberalen en Democraten
VU&ID	:	Volksunie&ID21

<i>Afkortingen bij de nummering van de publicaties :</i>		<i>Abréviations dans la numérotation des publications :</i>	
DOC 50 0000/000 :	Parlementair document van de 50e zittingsperiode + basisnummer en volgnummer	DOC 50 0000/000 :	Document parlementaire de la 50e législature, suivi du n° de base et du n° consécutif
QRVA :	Schriftelijke Vragen en Antwoorden	QRVA :	Questions et Réponses écrites
CRIV :	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (op wit papier, bevat ook de bijlagen)	CRIV :	Compte Rendu Intégral, avec à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (sur papier blanc, avec les annexes)
CRIV :	Voorlopige versie van het Integraal Verslag (op groen papier)	CRIV :	Version Provisoire du Compte Rendu intégral (sur papier vert)
CRABV :	Beknopt Verslag (op blauw papier)	CRABV :	Compte Rendu Analytique (sur papier bleu)
PLEN :	Plenum (witte kaft)	PLEN :	Séance plénière (couverture blanche)
COM :	Commissievergadering (beige kaft)	COM :	Réunion de commission (couverture beige)

<i>Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers</i>		<i>Publications officielles éditées par la Chambre des représentants</i>	
<i>Bestellingen :</i>		<i>Commandes :</i>	
Natieplein 2		Place de la Nation 2	
1008 Brussel		1008 Bruxelles	
Tel. : 02/ 549 81 60		Tél. : 02/ 549 81 60	
Fax : 02/549 82 74		Fax : 02/549 82 74	
www.deKamer.be		www.laChambre.be	
e-mail : publicaties@deKamer.be		e-mail : publications@laChambre.be	

TOELICHTING

DAMES EN HEREN,

Deze resolutie is een aanzet om het vertrouwen van de burgers in informatica en het e-government in het bijzonder te versterken en tegelijkertijd de privacy en veiligheid ervan te optimaliseren. De resolutie vraagt de regering bij de implementatie van het e-government en de daaraan gebonden ICT-initiatieven, meer rekening te houden met de bescherming van de privacy en stelt daartoe een reeks beleidsondersteunende maatregelen voor.

De problematiek van de bescherming van de privacy en meer in het bijzonder van persoonsgegevens is niet nieuw. Duitsland en Frankrijk werkten reeds in 1977 resp. 1978 een specifieke privacy-wetgeving uit. Nederland en België volgden in 1990 en 1993. Het tot stand komen van deze wetgevingen hing nauw samen met internationale akkoorden en richtlijnen, waaronder de Richtlijnen van de OESO inzake de bescherming van de persoonlijke levenssfeer en de internationale uitwisseling van persoonsgegevens van 23 september 1980 en het door de Raad van Europa onderhandelde Verdrag 108 van 28 januari 1981, in 1995 gevolgd door richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van persoonsgegevens. De internationale afspraken resulteerden in een aantal basisprincipes inzake gegevensbescherming, die een algemeen kader voor nationale wetgevingen vormen.

De wereldwijde technisch-wetenschappelijke ontwikkelingen en de steeds sneller verlopende verspreiding van informaticatoepassingen resulteerden in een tastbare performantieverbetering van het informatiegaringen –verwerkingsproces. Ook de federale overheid schrijft zich met projecten inzake e-government, waaronder de oprichting van nieuwe kruispuntbanken en de invoering van een elektronische identiteitskaart, in deze evolutie in. Naast de positieve aspecten van deze evolutie blijven echter de privacy-gebonden problemen onderbelicht, met name de mogelijke bedreigingen van de privacy. Door de reeds bestaande problematische machtsverhoudingen en de nieuwe trends dreigt de privacy steeds verder uitgehold te worden. Dankzij het inzetten van informaticasystemen en de haast onbeperkte mogelijkheden die vaste en mobiele netwerken, en met name het Internet bieden, wordt het aantal bewerkings-, koppelings- en selectiemogelijkheden

DEVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente résolution vise à renforcer la confiance du citoyen dans l'informatique en général, et dans l'*e-government* en particulier, tout en optimisant la confidentialité et la sécurité des données informatiques. Elle invite le gouvernement à tenir davantage compte de la protection de la vie privée lors de la mise en oeuvre de *e-government* et des initiatives TIC entreprises dans ce cadre, et propose à cet effet une série de mesures destinées à l'aider à définir la politique à mettre en oeuvre.

La problématique de la protection de la vie privée, et plus particulièrement des données à caractère personnel, n'est pas nouvelle. En 1977 et 1978 déjà, l'Allemagne et la France avaient toutes deux élaboré une législation spécifique en matière de protection de la vie privée. Les Pays-Bas et la Belgique leur avaient emboîté le pas en 1990 et en 1993. Ces législations étaient étroitement liées à divers accords internationaux et directives, notamment les lignes directrices de l'OCDE réglementant la protection de la vie privée et les flux transfrontaliers des données à caractère personnel en date du 23 septembre 1980 et la convention n°108 du Conseil de l'Europe du 28 janvier 1981, suivies, en 1995, par la directive 95/46/CE du Parlement européen et du Conseil de l'Union européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Les accords internationaux ont permis de définir une série de principes de base en matière de protection des données, qui constituent un cadre général pour les législations nationales.

L'évolution technico-scientifique à l'échelon mondial et la propagation toujours plus rapide des applications informatiques ont engendré une amélioration évidente des performances en matière de traitement et de collecte de l'information. L'autorité fédérale s'inscrit également dans cette évolution en élaborant des projets en matière d'*e-government*, parmi lesquels la mise sur pied de nouvelles banques-carrefours et l'introduction d'une carte d'identité électronique. Sous les aspects positifs de cette évolution se cachent toutefois des problèmes liés à la protection de la vie privée, à savoir les éventuelles menaces de violation de la vie privée. Les rapports de force problématiques qui se sont établis et les nouvelles tendances menacent de continuer à vider de sa substance le principe même du respect de la vie privée. Les systèmes informatiques et les possibilités quasi illimitées qu'offrent les réseaux fixes et mobiles, et notamment l'internet, ont permis d'élargir con-

beduidend opgevoerd. De individuele burger wordt hierdoor in hoge mate transparant gemaakt worden en kan steeds beter gecontroleerd worden – lees: in het oog gehouden worden.

Het is echter duidelijk dat ook de burger zelf een verantwoordelijkheid draagt bij de toenemende aantasting van zijn privacy. Door de toenemende informatisering laat de burger alsmaar meer sporen na. Het – dikwijls achteloos - gebruik van klantenkaarten, waardoor het consumptiegedrag van de individuele burger nauwgezet in kaart wordt gebracht, kan daarvoor model staan. De schier eindeloze controle-mogelijkheden die deze sporen teweeg brengen, controles in real-time én achteraf, hebben tot gevolg dat de burger zich dikwijls onbewust steeds meer gaat conformeren aan (doelgroep)normen die door deze controle-mogelijkheden worden opgedrongen. Informatica werkt in de regel machtsbevestigend en beperkt de vrijheid van het individu.

De bestaande wetgeving, de uitvoering en het toezicht op de uitvoering ervan vertonen een aantal belangrijke lacunes. Het versterken van de privacy ten overstaan van het ICT-gebeuren en meer in het bijzonder van de implementatie van het e-government, verdienen dan ook bijzondere aandacht. Tijdens het internationaal congres «*Debating privacy and ICT before and after September 11th*» (International conference on the use of personal data in criminal investigations and commerce dd. 17 januari 2002) werd op initiatief van de organisator, het Rathenau-Instituut, de 'Declaration of Amsterdam' opgesteld in antwoord op de toenemende druk en mogelijke aantastingen van de privacy die een gevolg kunnen zijn van de aanslagen van 11 september 2001. In de hiernavolgende resolutie nemen wij de krachtlijnen van deze Verklaring over.

Peter VANHOUTTE (Agalev-Ecolo)
 Kristien GRAUWELS (Agalev-Ecolo)
 Zoé GENOT (Agalev-Ecolo)
 Géraldine PELZER-SALANDRA (Agalev-Ecolo)

sidérablement les possibilités en matière de traitement, de connexion et de sélection. On fait ainsi du citoyen un être hautement transparent, ce qui permet de le contrôler de plus en plus efficacement – lisez : de le tenir à l'œil.

Il est toutefois évident que le citoyen porte également une part de responsabilité dans l'atteinte de plus en plus manifeste au respect de sa vie privée. Du fait de l'informatisation de plus en plus poussée, le citoyen laisse toujours plus de traces de ses actes. L'utilisation – souvent désinvolte – de cartes de clients, permettant d'analyser avec précision le comportement de chaque citoyen en matière de consommation, en est un parfait exemple. Les possibilités quasi illimitées de contrôle, en temps réel ou ultérieur, qu'engendrent ces traces ont pour effet que le citoyen se conforme de plus en plus, souvent inconsciemment, à des normes (fixées par groupe cible), que ces possibilités de contrôle permettent de lui imposer. L'informatique tend généralement à conforter la position des détenteurs du pouvoir et restreint la liberté de l'individu.

La législation en vigueur, son exécution et le contrôle de son exécution révèlent un certain nombre de lacunes importantes. Le renforcement de la protection de la vie privée face à l'évolution des TIC et, plus spécialement, à la mise en œuvre de l'*e-government*, mérite dès lors une attention particulière. Durant le congrès international intitulé «*Debating privacy and ICT before and after September 11th* » (International conference on the use of personal data in criminal investigations and commerce, 17 janvier 2002) a été élaborée, à l'initiative de l'organisateur, le *Rathenau-Instituut*, la «*Declaration of Amsterdam*», en réponse aux pressions de plus en plus fortes et aux violations de la vie privée qui peuvent éventuellement résulter des attentats du 11 septembre 2001. La résolution ci-après reprend les lignes directrices de cette Déclaration.

VOORSTEL VAN RESOLUTIE

DE KAMER VAN VOLKSVERTEGENWOORDIGERS,

Overwegende dat:

A. internationale samenwerking rond de bescherming van de privacy een lange geschiedenis heeft:

- dat de OESO, de Raad van Europa, de EU en anderen zich met deze materies hebben ingelaten;

- dat de belangrijkste overeenkomst vandaag de dag de EU-richtlijn inzake de bescherming van gegevens (95/46/EG) blijft;

- dat de essentiële principes van de bescherming van de privacy gedurende vele jaren onderhandeld werden;

B. de tragedie van 11 september het proces van het definiëren en harmoniseren van de internationale principes inzake privacy, niet mag onderbreken of terugschreeven;

C. de snelle ontwikkeling van ICT ook de komende jaren nieuwe thema's aan de orde zal stellen inzake de bescherming van de persoonlijke levenssfeer, in het bijzonder wanneer deze nieuwe technologieën een potentieel hebben inzake beveiliging en ordehandhaving;

- dat de federale overheid intensief werkt aan het op punt stellen van het e-government, met als voorname onderdelen de introductie van de nieuwe elektronische identiteitskaart, de invoering van een uniek nummer en het kruisen van federale databases;

- dat momenteel de laatste hand wordt gelegd aan de invoering van een nieuwe politiedatabank op basis van biometrische gegevens;

- dat de Commissie ter Bescherming van de persoonlijke levenssfeer voor de meeste van deze projecten niet of laattijdig om advies gevraagd werd;

- dat de noodzakelijke onafhankelijkheid van eventuele adviezen van de Commissie ter Bescherming van de Persoonlijke Levenssfeer niet kan worden gegarandeerd, gezien de daartoe noodzakelijke onafhankelijkheid van alle leden niet gegarandeerd blijkt;

PROPOSITION DE RÉOLUTION

LA CHAMBRE DES REPRÉSENTANTS,

Considérant

A. que la coopération internationale en matière de protection de la vie privée a une longue histoire:

- que l'OCDE, le Conseil de l'Europe, l'Union européenne et d'autres organisations se sont penchés sur cette matière ;

- qu'aujourd'hui, la directive européenne relative à la protection des données (95/46/CE) demeure la principale convention en la matière ;

- que les principes essentiels de la protection de la vie privée ont fait l'objet de négociations pendant de nombreuses années ;

B. que la tragédie du 11 septembre ne peut interrompre ni inverser le processus visant à définir et à harmoniser les principes internationaux en matière de protection de la vie privée ;

C. que le développement rapide des technologies de l'information et de la communication mettra également à l'ordre du jour, au cours des prochaines années, de nouveaux thèmes en matière de protection de la vie privée, plus particulièrement lorsque ces nouvelles technologies auront un potentiel en matière de sécurité et de maintien de l'ordre :

- que le pouvoir fédéral travaille d'arrache-pied à la mise au point de l'*e-government*, dont l'introduction de la nouvelle carte d'identité électronique, l'instauration d'un numéro unique et le croisement des banques de données fédérales seront les principaux éléments ;

- que l'on finalise actuellement la mise en place d'une nouvelle banque de données policières constituée sur la base de données biométriques

- que, pour la plupart de ces projets, la Commission de la protection de la vie privée n'a pas été consultée ou qu'elle l'a été tardivement ;

- que l'indispensable indépendance d'éventuels avis de la Commission de la protection de la vie privée ne peut être garantie, dès lors que l'indépendance de tous les membres nécessaire à cet effet n'est pas garantie ;

D. de laatste tientallen jaren de grenzen tussen de overheids-, commerciële en non-profitsectoren steeds verder vervagen;

- dat persoonsgegevens, ingezameld, verwerkt, opgeslagen en gecommuniceerd door één sector, in toenemende mate uitgewisseld worden over de traditionele grenzen heen met andere sectoren;

- dat deze ontwikkeling problemen schept inzake het afleggen van verantwoording en daarvoor noodzakelijke transparantie, en verstreckende gevolgen heeft voor het publieke vertrouwen;

E. de sociale kostprijs van gesofistikeerde bewakingssystemen, die de veiligheid van de burger dienen te verhogen, niet beperkt blijft tot het binnendringen in de persoonlijke levenssfeer;

- dat het verzamelen, verwerken, opslaan en meedelen van persoonsgegevens gedragsnormen tot stand brengt en categorieën sociale groepen standaardiseert. Dit opleggen van '*normaliteit*' begrenst in ernstige mate de persoonlijke keuze en beperkt het voor de maatschappij noodzakelijke potentieel voor verandering. Het onderwerpt individuen eveneens aan discriminatie;

- dat sommige bewakingssystemen onder bepaalde omstandigheden gerechtvaardigd kunnen zijn om de veiligheid van de burger en de orde te bevorderen. Om een voorgesteld bewakings- en registratiesysteem te legitimeren is echter een stap voor stap-analyse op basis van het voorzorgsprincipe noodzakelijk;

- dat burgers middels informatieverbreiding en opvoeding de noodzakelijke bewustwording, bekwaamheden en instrumenten aangereikt moeten krijgen om deel te nemen aan het beslissingsproces over hoger vermelde bewakingssystemen en om zichzelf tegen misbruiken te beschermen;

F. privacybescherming de effectieve implementatie vereist van de privacybeginselen door alle organisaties die persoonlijke gegevens verwerken;

- dat de meeste pogingen tot zelfregulering tot op heden symbolisch waren, slecht geïmplementeerd binnen de organisatie en/of misleidend voor het individu. Te dikwijls gaan de belangen van de gebruiker van gegevens voor op deze van het individu. De effectieve implementatie van privacybescherming, gekoppeld aan een effectief toezicht, is dan ook noodzakelijk;

D. que ces dernières décennies, les frontières entre les secteurs public, commercial et non marchand tendent de plus en plus à s'estomper;

- que les données à caractère personnel, collectées traitées, stockées et communiquées par un secteur sont de plus en plus échangées, par-delà les frontières traditionnelles, avec d'autres secteurs;

- que cette évolution crée des problèmes au niveau de la fourniture d'explications et de la transparence nécessaire pour ce faire et est lourde de conséquences pour la confiance du public;

E. que le coût social de systèmes de surveillance sophistiqués, qui sont destinés à accroître la sécurité du citoyen, ne se limite pas à une intrusion dans la vie privée;

- que la collecte, le traitement, le stockage et la communication de données à caractère personnel établissent des normes comportementales et standardisent les catégories de groupes sociaux. Cette imposition d'une '*normalité*' restreint de manière sérieuse les choix personnels et limite le potentiel de changement, qui est indispensable à la société. Elle expose également les individus aux discriminations;

- que, dans certaines circonstances, l'utilisation de certains systèmes de surveillance peut se justifier par la nécessité d'assurer la sécurité du citoyen et le maintien de l'ordre. Pour légitimer un service de surveillance et d'enregistrement qui est proposé, il est toutefois nécessaire d'effectuer une analyse graduelle, en vertu du principe de précaution;

- qu'il faut, par le biais de la diffusion d'informations et de l'éducation, conscientiser les citoyens, leur permettre d'acquérir les compétences requises et leur fournir les instruments nécessaires, de manière à ce qu'ils puissent prendre part à la prise de décisions concernant les systèmes de surveillance précités et se protéger eux-mêmes contre des abus;

F. la protection de la vie privée requiert la mise en œuvre effective des principes de confidentialité par toutes les organisations qui traitent des données à caractère personnel ;

- qu'à ce jour, la plupart des tentatives d'autorégulation étaient symboliques, mal mises en œuvre au sein de l'organisation et/ou trompeuses pour l'individu. Les intérêts de l'utilisateur des données priment trop souvent ceux de l'individu. La mise en œuvre effective de la protection de la vie privée, soumise à un contrôle effectif, est dès lors nécessaire.

G. de actuele discussies inzake privacy een schrijnend gebrek vertonen aan empirische ondersteuning en daarom afhankelijk worden gemaakt van ideologie en opportunisme. Deze empirische ondersteuning is in de meeste ons omringende landen ruim voorhanden en kan middels inbreng van de voorhanden zijnde expertise uit deze landen worden onderbouwd,

VERZOEKT DE REGERING:

1. ervoor te ijveren dat de EU-richtlijn inzake databescherming met onmiddellijke ingang in alle EU-lidstaten wordt geïmplementeerd, zoals dit in ons land reeds gebeurde en in alle EU-lidstaten ook effectief van kracht wordt;

2. er voor te ijveren dat in de kandidaat EU-lidstaten als onderdeel van de vereisten tot toetreding en als normerend element inzake mensenrechten een niveau van privacybescherming gerealiseerd wordt conform de bepaling van de Europese privacy-richtlijn;

3. er voor te ijveren dat in derde landen een 'adequaat' niveau van privacybescherming wordt gerealiseerd conform de bepalingen van de Europese privacy-richtlijn;

4. er voor te ijveren dat op EU-niveau een volwaardige privacy-commissie wordt opgericht, die ressorteert onder het Europees Parlement;

Aangaand nieuwe ICT-ontwikkelingen:

5. wanneer nieuwe ontwikkelingen inzake ICT opgenomen worden in internationale akkoorden, in een zeer vroeg stadium van de technologie en de ontwikkeling van standaarden rekening te houden, middels overleg en het vragen van een formeel advies aan de bevoegde privacy-commissie, met de privacy-implicaties van deze nieuwe technologieën;

6. het recente initiatief van het *Centre Européen de Normalisation* (CEN), gericht op een gemeenschappelijke internationale standaard, een kwaliteitsgarantie en een kwaliteitslabel, te ondersteunen;

G. les discussions actuelles en matière de vie privée témoignent d'une absence totale de soutien empirique et sont donc guidées par l'idéologie et l'opportunisme. Ce soutien empirique est largement présent dans la plupart de nos pays voisins et peut se fonder sur l'expertise existant dans ces pays,

DEMANDE AU GOUVERNEMENT :

1. de s'employer à ce que tous les États membres de l'Union européenne transposent sans délai, à l'instar de la Belgique, la directive européenne sur la protection des données, et qu'elle entre effectivement en vigueur dans tous les États membres de l'Union européenne ;

2. d'œuvrer pour que les pays candidats à l'adhésion soient tenus d'instaurer, à titre de condition d'adhésion accessoire et d'élément normatif en matière de droits de l'homme, un niveau de protection de la vie privée conforme aux dispositions de la directive européenne en matière de vie privée;

3. d'œuvrer pour que, dans les pays tiers, un niveau 'adéquat' de protection de la vie privée soit mis en place conformément aux dispositions de la directive européenne sur la protection de la vie privée ;

4. d'œuvrer en vue de la création, au niveau européen, d'une commission à part entière, consacrée à la vie privée, qui relèverait du Parlement européen.

Concernant les derniers développements en matière de Technologies de l'information et de la communication (TIC):

5. de tenir compte, lorsque les dernières innovations en matière de TIC sont inscrites dans des accords internationaux au cours des premiers stades de leur développement et du développement de normes standardisées, des implications des nouvelles technologies sur la vie privée, et ce, en organisant une concertation à ce propos et en invitant les commissions compétentes en matière de respect de la vie privée à rendre un avis formel ;

6. de soutenir l'initiative récente du *Centre européen de Normalisation* (CEN) visant à créer une norme standardisée internationale commune, une garantie de qualité et un label de qualité ;

7. de problemen inzake transparantie en verantwoording aan te pakken middels geëigende en effectieve instrumenten die de bescherming van persoonsgebonden gegevens in alle sectoren waarborgen;

Aangaande nieuwe bewakings- en registratiesystemen:

8. vooraleer een bewakings- en/of registratiesysteem in gebruik wordt genomen door de overheid, een stap voor stapanalyse te verplichten op basis van volgende elementen:

- bewakingssystemen mogen enkel geïmplementeerd worden indien zij effectief zijn, niet gemakkelijk omzeild kunnen worden en een aantoonbaar voordeel voor de veiligheid opleveren;

- bewakingssystemen mogen enkel geïmplementeerd worden indien de voordelen opwegen tegen de sociale kostprijs, met inbegrip van een eventuele aantasting van de privacy, een afname van autonomie, sociale discriminatie of het opleggen van conformiteit. Het principe van de proportionaliteit dient met andere woorden toegepast te worden;

- indien de systemen een veiligheidsvoordeel opleveren dat de sociale kostprijs verrechtvaardigt, zijn maatregelen noodzakelijk om deze kostprijs tot een minimum te herleiden;

9. vooraleer een bewakingssysteem geïmplementeerd wordt, wettelijke mechanismen met het oog op een onafhankelijk toezicht en controle op eventuele aanpassingen uit te werken;

10. de effecten – negatief en positief – van de systemen regelmatig te laten evalueren door de Commissie ter Bescherming van de Persoonlijke Levenssfeer;

Inzake het gebruik van Privacy Enhancing Technologies (PET):

11. de ontwikkeling en het gebruik van PET (*privacy enhancing technologies*) aan te moedigen om burgers minder kwetsbaar te maken voor mogelijke misbruiken van hun persoonsgebonden gegevens;

12. PET-audits te laten uitvoeren voor alle ICT-gerateerde overheidsactiviteiten, waarbij persoonsgebonden gegevens worden verwerkt, teneinde een maximaal beschermingsniveau van deze informatie te garanderen;

7. d'examiner les questions de transparence et de justification au moyen d'instruments appropriés et efficaces garantissant la protection des données à caractère personnel dans tous les secteurs ;

Concernant les nouveaux systèmes de surveillance et d'enregistrement :

8. de rendre obligatoire, avant la mise en service d'un système de surveillance et/ou d'enregistrement par un service public, la réalisation d'une analyse systématique tenant compte des éléments suivants :

- les systèmes de surveillance ne peuvent être mis en service que s'ils sont efficaces, ne peuvent pas être facilement trafiqués, et présentent un avantage démontrable pour la sécurité ;

- les systèmes de surveillance ne peuvent être mis en service que si les avantages qu'ils présentent sont à la mesure de leur coût social, lequel inclut une éventuelle atteinte à la vie privée, une réduction d'autonomie, une discrimination sociale, ou encore l'imposition d'une forme de conformité. Le principe de proportionnalité doit, en d'autres termes, être appliqué ;

- si les systèmes présentent un avantage en termes de sécurité qui justifie leur coût social, des mesures doivent être prises afin de réduire ce coût autant que possible ;

9. avant qu'un système de surveillance soit mis en œuvre, d'élaborer des mécanismes légaux en vue d'une surveillance et d'un contrôle indépendants des adaptations éventuelles ;

10. de faire procéder régulièrement par la Commission de la protection de la vie privée à l'évaluation des effets – négatifs et positifs – des systèmes ;

En ce qui concerne l'utilisation de *Privacy Enhancing Technologies (PET)* :

11. d'encourager le développement et l'utilisation de PET (*privacy enhancing technologies*), afin de rendre les citoyens moins vulnérables aux utilisations abusives éventuelles de leurs données à caractère personnel ;

12. de faire procéder à des audits PET pour toutes les activités publiques liées aux initiatives ICT et impliquant le traitement de données à caractère personnel, afin de garantir au maximum la protection de ces informations ;

13. af te zien van de invoering van een uniek identificatienummer voor alle burgers, gezien zulks de bescherming van de persoonlijke levenssfeer in het gedrang brengt en onverenigbaar is met de implementatie van PET;

14. erop toe te zien dat het inzamelen, opslaan, verwerken en communiceren van biometrische gegevens minimaal onder dezelfde strikte voorwaarden geschiedt als dat van andere persoonsgegevens;

15. een technologisch burgerschap aan te moedigen door het bewustzijn aan te scherpen van de risico's voor schendingen van de privacy en door de digitale praktijkkennis aan te scherpen middels informatiecampagnes en opvoeding;

16. het privacy-bewustzijn bij de publieke opinie aan te moedigen door te verduidelijken hoe overheden en privé-bedrijven omgaan met hun persoonlijke gegevens;

17. het begrip bij beleidsmakers aan te scherpen inzake de publieke noden en zorgen. Zulks kan onder andere gerealiseerd worden door publieke consultaties;

18. werk te maken van een effectieve implementatie van maatregelen ter bescherming van de persoonlijke levenssfeer op basis van:

- een goed gedefinieerd wettelijk kader;
- een organisatorische structuur en cultuur die de privacy op alle niveaus respecteert;
- het op punt stellen van verificatiemethodes, met inbegrip van onafhankelijke en externe audits;
- het uitvoeren van «privacy impact assessments» bij de introductie van nieuwe technologieën en/of diensten die implicaties kunnen hebben voor de privacy, met inbegrip van een assessment voor de introductie van de nieuwe elektronische identiteitskaart;
- waar zulks nuttig is, een onafhankelijke privacy-ambtenaar aan te stellen, die toeziet op de conformiteit;

Inzake research:

19. nationale en internationale researchprogramma's op te zetten en uit te bouwen om betrouwbare kwalitatieve en kwantitatieve gegevens inzake organisatie-

13. de renoncer à l'instauration d'un numéro d'identification unique pour tous les citoyens, étant donné qu'une telle mesure compromet la protection de la vie privée et est incompatible avec la mise en œuvre des PET ;

14. de veiller à ce que la collecte, le stockage, le traitement et la communication de données biométriques s'opèrent au moins dans les mêmes conditions strictes que celles prévues en ce qui concerne d'autres données à caractère personnel ;

15. d'encourager une citoyenneté technologique en faisant prendre davantage conscience des risques de violations de la vie privée et en renforçant les connaissances pratiques dans le domaine numérique au moyen de campagnes d'information et d'éducation ;

16. de conscientiser l'opinion publique aux risques de violation de sa vie privée en l'informant de la manière dont les pouvoirs publics et les entreprises privées gèrent leurs données à caractère personnel ;

17. d'affiner, chez les décideurs politiques, les conceptions en ce qui concerne les besoins et les préoccupations du public. Cela peut s'effectuer, entre autres, par le biais de consultations populaires ;

18. de veiller à la mise en œuvre effective des mesures de protection de la vie privée en partant

- d'un cadre légal bien défini ;
- d'une structure et d'une culture organisationnelles respectueuses la vie privée, à tous les niveaux ;
- de la mise au point de méthodes de vérification, y compris d'audits externes et indépendants ;
- de l'exécution de « *privacy impact assessments* » lors de l'introduction de nouvelles technologies et/ou de nouveaux services pouvant avoir des répercussions sur la vie privée, y compris d'une évaluation de l'introduction de la nouvelle carte d'identité électronique ;
- de la désignation, au besoin, d'un fonctionnaire indépendant chargé de veiller à la protection de la vie privée, ainsi que d'effectuer des contrôles de conformité ;

En matière de recherche :

19. d'élaborer et de développer des programmes de recherche nationaux et internationaux en vue de rassembler et d'analyser des données qualitatives et quan-

praktijk, technologische applicaties en innovaties, en het publieke begrip inzake privacy te verzamelen en te analyseren;

20. de onderzoeksresultaten in het besluitvormingsproces mee te nemen en toe te zien op de implementatie ervan in alle sectoren.

27 juni 2002

Peter VANHOUTTE (Agalev-Ecolo)
Kristien GRAUWELS (Agalev-Ecolo)
Zoé GENOT (Agalev-Ecolo)
Géraldine PELZER-SALANDRA (Agalev-Ecolo)

titatives fiables en ce qui concerne la pratique organisationnelle, les applications et innovations technologiques et la façon dont le public comprend la protection de la vie privée ;

20. d'intégrer les résultats des recherches dans le processus décisionnel et veiller à ce qu'ils soient appliqués dans tous les secteurs.

27 juin 2002