# EUROPEES PARLEMENT

*2004* *2009*

*Commissie burgerlijke vrijheden, justitie en binnenlandse zaken*

**2008/2160(INI)**

21.1.2009

# ONTWERPVERSLAG

met een ontwerpaanbeveling van het Europees Parlement aan de Raad betreffende de versterking van de veiligheid en van de fundamentele vrijheden op het internet
(2008/2160(INI))

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

Rapporteur: Stavros Lambrinidis

PR_INI_art114

## INHOUD

**Blz.**

ONTWERPAANBEVELING VAN HET EUROPEES PARLEMENT AAN DE RAAD .....3

ONTWERPAANBEVELING AAN DE RAAD (B6-0302/2008).....9

TOELICHTING.....11

# ONTWERPAANBEVELING VAN HET EUROPEES PARLEMENT AAN DE RAAD

**betreffende de versterking van de veiligheid en van de fundamentele vrijheden op het internet**
**(2008/2160(INI))**

*Het Europees Parlement*,

– gezien de ontwerpaanbeveling aan de Raad, ingediend door Stavros Lambrinidis namens de PSE-Fractie, betreffende de versterking van de veiligheid en van de fundamentele vrijheden op het internet (B6-0302/2008),

– gelet op het Internationaal Verdrag inzake burgerrechten en politieke rechten, het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en het Handvest van de grondrechten van de Europese Unie[1], en in het bijzonder het daarin bepaalde over de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie en de eerbiediging van het privéleven en het familie- en gezinsleven, en het recht op vrijheid en veiligheid,

– gezien Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[2], kaderbesluit van de Raad 2008/977/JBZ van 27 november 2008 inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële samenwerking in strafzaken[3], Richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie[4], het voorstel van de Commissie van 13 november 2007 voor een richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking met betrekking tot consumentenbescherming (COM(2007)0698), Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken[5] en de Conclusie van de advocaat-generaal van 14 oktober 2008 in de zaak C-301/06 Ierland / Parlement en Raad,

– gelet op Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen[6], Kaderbesluit 2001/413/JBZ van de Raad van 28 mei 2001 betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen

[1] PB C 364 van 18.12.2000, blz. 1.
[2] PB L 281 van 23.11.1995, blz. 31.
[3] PB L 350 van 30.12.2008, blz. 60.
[4] PB L 345 van 31.12.2003, blz. 90.
[5] PB 2006 L 105, blz. 54.
[6] PB L 69 van 16.3.2005, blz. 67.

dan contanten[1], Kaderbesluit 2008/919/JBZ van de Raad van 28 november 2008 tot wijziging van Kaderbesluit 2002/475/JBZ inzake terrorismebestrijding[2], de mededeling van de Commissie van 22 mei 2007 'Naar een algemeen beleid voor de bestrijding van cybercriminaliteit' (COM(2007)0267), alsmede de recente initiatieven voor de opsporing van ernstige misdaad en terrorisme (zoals het "Check the Web-project"),

– gezien de werkzaamheden die zijn aangevat binnen het kader van de Raad van Europa, de Organisatie voor economische samenwerking en ontwikkeling (OESO) en de Verenigde Naties zowel ten aanzien van de strijd tegen criminaliteit en cybercriminaliteit als ten aanzien van de bescherming van de grondrechten en fundamentele vrijheden, ook op het internet[3],

– gezien de meest recente arresten van de Europese en nationale constitutionele hoven ter zake, met name het arrest van het Duitse Bundesverfassungsgericht waarin een afzonderlijk recht op bescherming van de vertrouwelijkheid en van de integriteit van informaticasystemen wordt erkend[4],

– gelet op artikel 114, lid 3, en artikel 94 van zijn Reglement,

– gezien het verslag van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken en het advies van de Commissie cultuur en onderwijs (A6-0000/2009),

A. overwegende dat de ontwikkeling van het internet aantoont dat het zich aan het ontwikkelen is tot een onmisbaar hulpmiddel voor het bevorderen van democratische initiatieven, een nieuwe arena voor het politieke debat (bijvoorbeeld elektronisch campagne voeren, elektronisch stemmen) en een zeer belangrijk instrument op mondiaal niveau voor het uitoefenen van de vrijheid van meningsuiting (bijvoorbeeld door te bloggen) en voor het ontwikkelen van bedrijfsactiviteiten,

B. overwegende dat het internet de definitie van vrijheid van meningsuiting zoals vervat in artikel 11 van het Handvest van de grondrechten van de Europese Unie, met name in de dimensie 'ongeacht grenzen' van dit artikel, volledig invult,

C. overwegende dat transparantie, eerbiediging van de persoonlijke levenssfeer en een omgeving van vertrouwen onder internetbelanghebbenden moeten worden beschouwd als onmisbare elementen voor het opbouwen van een duurzame veiligheidsvisie op het internet,

D. overwegende dat het internet, door de vrijheid die het biedt, ook gebruikt wordt als platform voor gewelddadige en niet-democratische boodschappen, waaronder boodschappen die aanzetten tot terrorisme, en overwegende dat de dreiging van cybercriminaliteit in een bredere betekenis wereldwijd is toegenomen en een gevaar

[1] PB L 149 van 2.6.2001, blz. 1.
[2] PB L 330 van 9.12.2008, blz. 21.
[3] Bijvoorbeeld: Verdrag van de Raad van Europa inzake cybercriminaliteit van 23 november 2001; Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens.
[4] BVerfG, 1 BvR 370/07, 27.2.2008, punten 1-333.

vormt voor personen (waaronder kinderen) en netwerken,

E. overwegende dat dergelijke misdaden effectief en vastberaden moeten worden bestreden, zonder de fundamenteel vrije en open aard van het internet te wijzigen,

F. overwegende dat het in een democratische maatschappij de burgers zijn die het recht hebben dagelijks de daden en overtuigingen van hun overheden en van particuliere bedrijven die hun van diensten voorzien te observeren en te beoordelen en het niet de overheden of bedrijven zijn die het recht hebben de daden en overtuigingen van hun burgers te observeren en te beoordelen; overwegende dat de combinatie van technologisch geavanceerde technieken voor toezicht en vage wetten waarin de grenzen aan de toepassingen ervan worden voorgeschreven dit principe in toenemende mate in het gedrang brengt,

G. overwegende dat sprongsgewijze technologische ontwikkelingen het in toenemende mate mogelijk maken in het geheim en vrijwel onopgemerkt toezicht uit te oefenen op de activiteiten van burgers op het internet; overwegende dat het kale feit dat technieken voor toezicht bestaan het gebruik ervan niet vanzelfsprekend rechtvaardigt, maar dat het doorslaggevende belang van het beschermen van de grondrechten van burgers de grenzen en exacte omstandigheden moet bepalen waaronder dergelijke technieken door overheden en particuliere bedrijven gebruikt mogen worden,

H. overwegende dat men niet mag vergeten dat, waar het rechten als de vrijheid van meningsuiting of de eerbiediging van het privéleven betreft, inmenging in de uitoefening van de desbetreffende rechten alleen door overheden mag worden opgelegd als dit ‘conform de wet’ en noodzakelijk is en op proportionele wijze wordt toegepast binnen een democratische maatschappij,

I. overwegende dat vanwege de mondiale, open en participatieve aard van het internet, het internet als regel uitgaat van vrijheid, maar dat dit niet de noodzaak uitsluit na te denken (op nationaal en internationaal niveau, in een openbare en privéomgeving) over hoe de fundamentele vrijheden van internetgebruikers en hun veiligheid worden gerespecteerd en beschermd,

J. overwegende dat digibetisme het nieuwe analfabetisme van de eenentwintigste eeuw zal zijn; overwegende dat het ervoor zorgen dat alle burgers toegang hebben tot het internet daarom gelijkwaardig is aan het ervoor zorgen dat alle burgers toegang hebben tot onderwijs, en overwegende dat dergelijke toegang niet als strafmaatregel mag worden ontzegd door overheden of particuliere bedrijven; overwegende dat het belangrijk is iets te doen aan nieuwe kwesties zoals netwerkneutraliteit, interoperabiliteit, mondiale bereikbaarheid van alle internetknooppunten, en het gebruik van open formaten en standaarden,

K. overwegende dat de juiste balans moet worden behouden tussen het hergebruik van overheidsinformatie, hetgeen ongekende mogelijkheden biedt voor creatieve en culturele experimenten en uitwisseling, en de bescherming van intellectuele-eigendomsrechten,

1. richt de volgende aanbevelingen tot de Raad:

***Volledige en veilige toegang tot het internet voor iedereen***

a) deelnemen aan inspanningen om van het internet een belangrijk hulpmiddel te maken voor de *empowerment* van gebruikers, een omgeving die de ontwikkeling van 'bottom up' praktijken en e-democratie mogelijk maakt, terwijl er tegelijkertijd op wordt toegezien dat er wezenlijke voorzorgsmaatregelen worden genomen aangezien er zich in deze omgeving nieuwe vormen van controle en censuur kunnen ontwikkelen; de vrijheid en bescherming van het privéleven die de gebruikers op het internet ervaren moet echt zijn en geen illusie,

b) erkennen dat het internet een buitengewone mogelijkheid kan zijn om actief burgerschap te vergroten en dat, in dit opzicht, toegang tot netwerken en inhoud een van de belangrijkste elementen is; aanbevelen dat deze kwestie verder wordt ontwikkeld op basis van de aanname dat iedereen het recht heeft deel te nemen aan de informatiemaatschappij en dat instellingen en belanghebbenden op alle niveaus een algemene verantwoordelijkheid hebben voor het meewerken aan deze ontwikkeling,[1] waarmee de beide nieuwe uitdagingen van digibetisme en democratische uitsluiting in het elektronische tijdperk te lijf worden gegaan[2],

c) samen met andere relevante actoren ervoor zorgen dat veiligheid, vrijheid van meningsuiting en eerbiediging van de persoonlijke levenssfeer, evenals openheid op het internet, niet als concurrerende doelen worden aangepakt, maar gelijktijdig worden verwezenlijkt binnen een totaalvisie die een adequaat antwoord vormt op al deze vereisten,

***Sterke gerichtheid op het bestrijden van cybercriminaliteit***

d) het voorzitterschap van de Raad en de Commissie ertoe uitnodigen na te denken over een brede strategie om cybercriminaliteit te bestrijden, waaronder begrepen de manieren waarop het probleem van "identiteitsdiefstal" op EU-niveau kan worden aangepakt,

e) een debat aanmoedigen over de noodzakelijke samenwerking tussen particuliere en openbare actoren op dit gebied en over de uitbreiding van de samenwerking tussen instanties voor wetshandhaving,

f) het werk dat is aangevat in het kader van het "Check the Web"-project voortzetten en acties gericht op het verbeteren van de verspreiding van informatie over cybercriminaliteit bevorderen, zoals de recente initiatieven voor het opzetten van nationale waarschuwingsplatforms en een Europees waarschuwingsplatform voor het melden van misdrijven die op het internet worden gepleegd, op voorwaarde dat de noodzakelijke voorzorgsmaatregelen zijn genomen,

[1] Zie de Griekse grondwet en artikel 5A daarvan.

[2] In het document '*Internet - a critical resource for all*' van de Raad van Europa van 17 september 2008 wordt ook benadrukt dat het zekerstellen en bevorderen van rechtvaardigheid en deelname met betrekking tot het internet een essentiële stap is voor de vooruitgang van rechtvaardigheid en deelname in de totale maatschappij.

g) programma's bevorderen voor het beschermen van kinderen en het onderwijzen van hun ouders, zoals vastgelegd in EU-wetgeving met betrekking tot de nieuwe elektronische gevaren, en voorzien in een effectbeoordeling van bestaande programma's tot dusverre,

h) overgaan tot het aannemen van de richtlijn inzake strafmaatregelen gericht op het handhaven van intellectuele-eigendomsrechten en tegelijkertijd, in het kader van dat doel, tot het verbieden van het systematisch uitoefenen van controle en toezicht op alle activiteiten van gebruikers op het internet en erop toezien dat de straffen proportioneel zijn aan de gepleegde schendingen; binnen deze context ook de vrijheid van meningsuiting en vereniging van individuele gebruikers eerbiedigen en de stimulansen bestrijden voor cyberschendingen van intellectuele-eigendomsrechten, waaronder bepaalde excessieve toegangsbeperkingen die door de houders van intellectuele-eigendomsrechten zelf worden opgelegd,

i) erop toezien dat de uiting van controversiële politieke overtuigingen via het internet, onder andere met betrekking tot terrorisme, gevrijwaard is van strafrechtelijke vervolging,

***Constante aandacht voor de absolute bescherming en betere bevordering van fundamentele vrijheden op het internet***

j) in overweging nemen dat "digitale identiteit" in toenemende mate een integraal onderdeel wordt van wie wij zijn en in dit opzicht adequate en effectieve bescherming verdient tegen inmenging door zowel particuliere als overheidsactoren; voldoende belang hechten aan de betekenis van anonimiteit, pseudonimiteit en de beheersing van informatiestromen voor privacy en het feit dat gebruikers moeten worden voorzien van de middelen om deze efficiënt te beschermen,

k) het gevaar erkennen van vormen van internettoezicht en -controle die mede gericht zijn op het volgen van alle 'digitale' stappen van een individu met als doel een profiel van de gebruiker te verstrekken en 'scores' toe te wijzen; duidelijk maken dat dergelijke technieken altijd zouden moeten worden beoordeeld in termen van hun noodzaak en hun proportionaliteit ten opzichte van de doelen die men ermee wil bereiken; tevens de noodzaak benadrukken van een groter bewustzijn en van de geïnformeerde toestemming van gebruikers met betrekking tot hun internetactiviteiten (bijvoorbeeld in het geval van sociale netwerken),

l) onderzoeken en vastleggen welke grenzen er zijn aan de 'toestemming' die door overheden of particuliere bedrijven kan worden gevraagd of afgedwongen van bezoekers om hun privacy deels op te geven, aangezien er een duidelijke disbalans is met betrekking tot onderhandelingspositie en kennis tussen individuele gebruikers en de desbetreffende instellingen,

m) de gevallen waarin een particulier internetbedrijf verplicht kan worden gegevens aan overheden bekend te maken, strikt beperken en definiëren,

n) censuur van overheidswege op de inhoud die gezocht kan worden op internetsites veroordelen, in het bijzonder indien dergelijke beperkingen een '*chilling effect'*

kunnen hebben op politieke uitingen, waardoor mensen ervan worden weerhouden dergelijke uitingen te doen,

o) de lidstaten verzoeken erop toe te zien dat de vrijheid van meningsuiting niet onderworpen wordt aan arbitraire beperkingen uit de publieke en/of private sfeer en dat alle wetgevings- of bestuurlijke maatregelen worden voorkomen die een *'chilling effect'* kunnen hebben op individuen,

p) de aandacht vestigen op het feit dat de ontwikkeling van het 'internet van dingen' niet voorbij mag gaan aan de bescherming van gegevens en van de rechten van burgers,

q) de bevordering van het "*privacy by design*"-principe aanmoedigen, dat ervan uitgaat dat privacy- en gegevensbeschermingsvereisten zo vroeg mogelijk in de levenscyclus van nieuwe technologische ontwikkelingen geïntroduceerd moeten worden,

***Internationale verbintenissen***

r) alle internetactoren ertoe aansporen actief deel te nemen aan het proces voor het Handvest van grondrechten inzake internet ('Internet Bill of Rights') dat momenteel aan de gang is en dat voortbouwt op bestaande fundamentele rechten en hun handhaving en de erkenning van nieuwe grondslagen bevordert; in dit opzicht zou de dynamische coalitie voor het handvest van grondrechten inzake internet een voortrekkersrol moeten spelen,

s) ervoor zorgen dat, in deze context, een procesgericht initiatief van veel belanghebbenden op meer niveaus en een mix tussen mondiale en lokale initiatieven in overweging worden genomen teneinde de rechten van internetgebruikers nader te omschrijven en te beschermen en de rechtmatigheid en aanvaarding en de verantwoordingsplicht over het proces zeker te stellen,

t) de EU aanmoedigen actief deel te nemen aan verschillende internationale fora die zich bezighouden met mondiale en gelokaliseerde aspecten van het internet, zoals het Internet Governance Forum (IGF),

u) samen met alle relevante EU-actoren deelnemen aan de totstandkoming van een Europees IGF dat de balans opmaakt van de ervaring die is opgedaan door nationale IGF's, als regionaal kernpunt fungeert en Europabrede kwesties, standpunten en zorgen efficiënter doorgeeft in de toekomstige internationale IGF's;

-o0o-

2. verzoekt zijn Voorzitter deze aanbeveling te doen toekomen aan de Raad en, ter informatie, aan de Commissie.

11.6.2008

## ONTWERPAANBEVELING AAN DE RAAD (B6-0302/2008)

ingediend overeenkomstig artikel 114, lid 1, van het Reglement

door Stavros Lambrinidis

over de versterking van de veiligheid en van de fundamentele vrijheden op het internet

*Het Europees Parlement*,

– gelet op het Europese Verdrag tot bescherming van de rechten van de mens en het Handvest van de grondrechten, in het bijzonder de artikelen daarvan over de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie en de eerbiediging van het privéleven en het familie- en gezinsleven,

– gezien de recente initiatieven voor de opsporing van ernstige misdaad en terrorisme (het "Check the Web"-project) en het recente voorstel tot wijziging van Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding, alsmede het voorstel tot herziening van Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie,

– gezien de werkzaamheden die zijn aangevat binnen de Raad van Europa, de Organisatie voor economische samenwerking en ontwikkeling (OESO) en de Verenigde Naties zowel ten aanzien van de strijd tegen criminaliteit en cybercriminaliteit als ten aanzien van de bescherming van de grondrechten en fundamentele vrijheden, ook op het internet,

– gezien de meest recente arresten van de Europese en nationale constitutionele hoven ter zake, met name het arrest van het Duitse Bundesverfassungsgericht waarin een afzonderlijk recht op bescherming van de vertrouwelijkheid en van de integriteit van informaticasystemen wordt erkend,

– gelet op artikel 114, lid 1, van zijn Reglement,

A. overwegende dat het internet in de wereld een essentieel instrument is geworden voor de ontwikkeling van de vrijheid van meningsuiting en de ontplooiing van economische activiteiten; in dit verband overwegende dat het van cruciaal belang is ervoor te zorgen dat de strijd tegen de misdaad en tegen misbruik door de overheid en particulieren het potentieel van dit instrument niet aan banden legt,

B. overwegende dat het verschijnsel internet vanwege de mondiale dimensie, de snelle ontwikkeling en de technische kenmerken ervan moeilijk in het kader van nationaal recht alleen kan worden geregeld en dat initiatieven nodig zijn, vooral op internationaal niveau, om de rechten van het individu te beschermen, zowel zijn recht op veiligheid als het recht op bescherming van zijn vrijheid en het recht op bescherming van zijn persoonlijke levenssfeer,

1. beveelt de Raad het volgende aan:

a) geleidelijk harmoniseren van de nationale wetgevingen binnen de EU inzake de eisen in verband met de bescherming van de grondrechten op het internet,

b) intensiveren van de dialoog tussen de nationale en de Europese wetgevers, alsmede tussen de nationale en Europese rechtsstelsels,

c) bevorderen van de dialoog tussen alle betrokkenen bij het internet, met name de internetexploitanten en de gebruikers,

d) bevorderen van het sluiten van de nodige overeenkomsten op internationaal niveau, zowel op bilateraal (met name trans-Atlantisch) als op multilateraal vlak (initiatieven van de Raad van Europa, de OESO en de VN);

2. verzoekt zijn Voorzitter deze aanbeveling te doen toekomen aan de Raad en, ter informatie, aan de Commissie.

# TOELICHTING

## Grondrechten op het internet - verbeterd én bedreigd

Wij leven in een tijdperk waarin iedereen, van de overheid tot de politie, van particuliere bedrijven tot criminelen, een zo ruim mogelijk toegang tot onze elektronische privégegevens wil hebben. Met name het internet levert voorheen ongekende details over ons privéleven op; één enkele klik op een website biedt toegang tot gegevens die mogelijk kunnen worden gebruikt of misbruikt door verkopers, geheime diensten of "identiteitsdieven".

Bescherming van het **grondrecht op bescherming van de privésfeer** op internet is dan ook een van de meest dringende taken die de wetgever moet aanpakken, en tevens een van de lastigste ethische, wettelijke, technologische en politieke uitdagingen waarmee onze samenleving ooit is geconfronteerd.

Het is duidelijk dat het internet een instrument kan vormen dat onze grondrechten uitbreidt, dat ons van onbegrensde informatie voorziet en ons in contact brengt met mensen en gemeenschappen over de hele wereld. Minder aandacht wordt geschonken aan het feit dat het internet tegelijkertijd ook een grote bedreiging van onze grondrechten inhoudt, doordat de gebruiker aan in zijn nadeel werkende controle wordt onderworpen, en doordat het door criminelen en terroristen wordt ingezet. En het is allerminst duidelijk hoe het internet zodanig kan worden gereguleerd dat iedereen van de voordelen ervan profiteert, terwijl de zeer reële en ernstige gevaren van misbruik worden beperkt. De zaak wordt nog verder gecompliceerd door de aard van het internet zelf - een decentraal, door gebruikers aangestuurd netwerk, waarop geen enkele regering controle kan uitoefenen en dat vrijwel alle grenzen passeert.

Dit verslag heeft dan ook tot doel te belichten hoe de grondrechten van het individu in een online-omgeving het best kunnen worden beschermd en bevorderd. Essentiële elementen van het antwoord op deze vraag zijn onder meer:

- Participatie van alle belanghebbenden;
- Actie op verschillende niveaus, met gebruikmaking van bestaande nationale, regionale en internationale instrumenten en observatie hoe deze in de dagelijkse wetgevingspraktijk worden toegepast;
- Uitwisseling van beste praktijken, en
- Ingaan op de behoeften en problemen van verschillende types internetgebruikers en van uiteenlopende (en zich voortdurend verder ontwikkelende) soorten online-activiteiten.

Het vinden van een adequaat evenwicht tussen privacy en veiligheid vormt de kern van ons streven. Het zal een kwestie zijn van constante oplettendheid en herijking, zodat de wetgeving gelijke tred houdt met de onstuitbare opmars van de technologie. Alle veiligheidsaspecten moeten zorgvuldig tegen het licht worden gehouden, van nationale veiligheidsvraagstukken tot de veiligheid en betrouwbaarheid van onze netwerken, en de persoonlijke veiligheid van

individuele gebruikers die hun gegevens online doorgeven. Als het waarborgen van een veiliger internet een legitiem doel van onze samenleving is, moeten wij het gebruik van toezicht- en controletechnieken die onze grondrechten bedreigen, onder de loep nemen en aan banden leggen - met name wanneer er twijfels rijzen omtrent noodzaak, proportionaliteit en efficiency van deze technieken. Flexibiliteit, aanpassingsvermogen en verantwoordingsplicht moeten de kenmerken vormen van de wetgeving en de programma's die wij ontwikkelen, zodat wij de ontwikkeling van de technologie steeds een stap voor blijven.

**Het internet kan bepaalde grondrechten, zoals de vrijheid van meningsuiting, van politieke activiteit en van vereniging, zeer bevorderen**, maar het kan deze even gemakkelijk ondermijnen. Een recent voorbeeld van dit debat was het wetgevingsinitiatief voor controle op de meningsuiting op het internet om terroristische aanvallen te voorkomen. Dit is een klassiek voorbeeld van wetgeving die - tenzij zeer nauwkeurig toegesneden op het eigenlijke doel - de deur openzet naar grootschalige controle, waardoor de politieke meningsuiting van het individu, de kern van een democratische samenleving, gemuilkorfd wordt.

Het vinden van een juist evenwicht tussen dit soort kwesties is van cruciaal belang. Het lijdt geen twijfel dat het internet criminelen heeft voorzien van een machtig instrumentarium, en het spreekt vanzelf dat terroristen moet worden belet het internet te gebruiken om aanvallen te plannen en uit te voeren. Daarnaast eist de samenleving terecht dat verspreiders en gebruikers van kinderporno op het internet worden tegengehouden. Dergelijke criminelen vormen een tastbare bedreiging, waardoor de burger minder terughoudend is om van de politie grootschalige controle op het internet te eisen - het internet, dat uit de aard der zaak "niet-tastbaar" is. Wij moeten ons verzetten tegen deze tendens. Onze wetten moeten de misdaad afdoende kunnen bestrijden, maar zij mogen niet excessief zijn. Het internet is door zijn ongestructureerde en ongrijpbare aard juist gevoelig voor excessen. Zo zouden weinig mensen bijvoorbeeld accepteren dat de politie of bedrijven elke verzonden brief via het postkantoor zouden mogen openen om de inhoud ervan te controleren. Eenzelfde oplettendheid is vereist als het om de bescherming van de inhoud van elektronische communicatie gaat.

Maar het muilkorven van de vrije meningsuiting en het schenden van de privacy gebeurt niet alleen door overheden bij de strijd tegen criminelen, maar ook door particuliere internetbedrijven bij de jacht naar winst. De meest recente tendens als dit aan het licht komt - en dat is meestal pas als bedrijven op heterdaad zijn betrapt bij het zonder toestemming verzamelen, opslaan en gebruiken van onze gegevens - is dat de gebruiker om **instemming** met het gebruik van zijn gegevens wordt gevraagd (hetzij als keuze voor, hetzij als keuze tegen deze mogelijkheid).

Wat zijn de grenzen van een dergelijke **instemming**? Deze vraag betreft zowel hoeveel gegevens een bedrijf een gebruiker kan verzoeken mee te delen, als hoeveel van zijn privacy en grondrechten een gebruiker mag worden verzocht op te geven in ruil voor bepaalde internetdiensten of -privileges.

De antwoorden op deze vragen zijn niet eenvoudig. Op een ander terrein, nl. arbeidswetgeving, is onze samenleving overeengekomen dat er grenzen zijn aan de zeggenschap van de burger over zijn privéleven. Zo bepalen arbeidswetten en collectieve arbeidsovereenkomsten in de meeste lidstaten bijvoorbeeld de maximale werktijd, het

minimumloon en andere arbeidsrechten, die afzonderlijke werknemers niet "weg kunnen onderhandelen" met hun werkgever. Hier is een simpele reden voor: er wordt van uitgegaan dat er geen machtsevenwicht bestaat tussen werkgever en werknemer, en dat er niet op voet van gelijkheid "instemming" kan worden gegeven of gevraagd. Een andere reden is dat wij ook hebben besloten dat er geen nivellering op het laagste peil mag komen wat arbeidsrechten aangaat, hetgeen zou kunnen gebeuren indien individuele werknemers zou worden toegestaan of als zij zouden worden gedwongen in onderhandelingen van sommige van hun rechten af te zien.

Van een vergelijkbaar machts- en kennisvacuüm is sprake op het internet: macht van bedrijven en overheden, kennis en belangen leggen veel meer gewicht in de schaal dan de individuele gebruiker, net als het gevaar van "goedkopere" (en dus aantrekkelijkere) internetdiensten in ruil voor een geringere bescherming van de privacy. Uw rapporteur is ervan overtuigd dat de volgende strijd in het debat over veiligheid en privacy op het internet zal gaan over de grenzen van de "instemming" die overheden en particuliere bedrijven proberen te krijgen.

Deze kwestie moet ons nauw aan het hart liggen, want in het Europa van vandaag zal "Big Brother" zich niet voordoen in de vorm van een of ander autoritair regime, maar komt hij - vooropgesteld dat hij komt - heimelijk en met onze "instemming".

Tot slot zijn **het recht op onderwijs en het recht op internettoegang** twee bijkomende rechten, die het op zich al waard zijn te worden bevorderd, maar die in de context van strijd tegen internetcriminaliteit eveneens onder vuur kunnen komen te liggen. Digibetisme wordt het nieuwe analfabetisme van de 21ste eeuw. Zoals elk kind vandaag de dag recht heeft op onderwijs, en elke volwassene op permanente opleiding, zo zou elk individu zijn leven lang recht moet hebben op toegang tot computers en tot internet. Regeringen zouden een dergelijk recht zelfs in de meest verafgelegen regio's en voor de armste burgers moeten waarborgen; daarnaast mag het weigeren van toegang niet gebruikt worden om overtredingen van burgers te "bestraffen". Mensen uit alle geledingen van de samenleving, uit alle regio's en culturen, moeten over de mogelijkheid beschikken om te profiteren van de ruime keuze aan diensten op het internet. Op deze manier kunnen zij werken aan hun persoonlijke ontwikkeling en relaties aangaan op het gebied van onderwijs of beroep dan wel in de privésfeer, en kunnen zij in de ruimste mate die de technologie en de wet toestaan gebruik maken van economische kansen.