Colloquium

DE IMPACT VAN DE NIEUWE TECHNOLOGIEËN OP ONZE PRIVACY EN DE GEGEVENSBESCHERMING: WAT STAAT ER OP HET SPEL?

BELGISCHE SENAAT - 17 OKTOBER 2016

Handelingen

De impact van de nieuwe technologieën op onze privacy en de gegevensbescherming: wat staat er op het spel?

Belgische Senaat - maandag 17 oktober 2016

Inhoudsopgave

Programma

Moderator
Eddy Caekelberghs, RTBF-journalist

13.30 u. **Verwelkoming**
Christine Defraigne, Voorzitster van de Senaat

13.45 u. **Inleiding**
Paul De Hert, Codirecteur van de onderzoeksgroep 'Law, Science, Technology & Society' van de VUB

De persoonlijke levenssfeer en de opkomst van nieuwe technologieën

14.00 u. **Het standpunt van de bedrijven**
Marc Lambotte, CEO van Agoria

14.15 u. **Het standpunt van de Europese Unie**
Giovanni Buttarelli, Hoogleraar in de rechten en de theologie (Université Libre de Bruxelles – Université de Mons)

14.30 u. **De persoonlijke levenssfeer en de opkomst van nieuwe technologieën**
Elise Degrave, Doctor in de rechten, gespecialiseerd in e-government en de bescherming van de persoonlijke levenssfeer (UNamur)

De bescherming van de persoonlijke levenssfeer op het vlak van veiligheid en openbaar leven

14.45 u. **Veiligheid in de praktijk**
Guy Rapaille, Voorzitter van het Comité I

15.00 u. **Gegevensbescherming**
Amid Faljaoui, Directeur van de tijdschriften Trends Tendances, Le Vif-L'Express, strategisch adviseur van de 'Cercle de Wallonie' en columnist bij de RTBF

15.15 u. **Persoonlijke levenssfeer en openbaar leven in België**
Els Kindt, Postdoctoraal onderzoeker aan de KU Leuven (Centre for IT and IP law-iMinds), associate professor eLaw Universiteit Leiden

15.30 u. **Koffiepauze**

Bescherming van persoonsgegevens en traceerbaarheid

15.45 u. **Het verzamelen en uitwisselen van gegevens**
Danielle Jacobs, General Manager van BELTUG

16.00 u. **Gevallen waarin persoonsgegevens niet of onvoldoende beschermd worden**
Matthias Dobbelaere-Welvaert, Oprichter en managing partner van 'deJuristen/lesJuristes'

16.15 u. **Het standpunt van de samenleving over het gevoel van traceerbaarheid**
Yves Poullet, Rector van de UNamur en hoogleraar aan de ULg

Politiek debat

16.30 u. **Debat in aanwezigheid van de heer Philippe De Backer, staatssecretaris voor Bestrijding van de sociale fraude, Privacy en Noordzee, en van de vertegenwoordigers van de verschillende partijen**

Besluit

17.30 u. **Louis Michel,** Minister van Staat en Europarlementslid

17.45 **Drink**

De impact van de nieuwe technologieën op onze privacy en de gegevensbescherming: wat staat er op het spel?

Verwelkoming

Mevrouw Christine Defraigne. – Mijnheer de voorzitter, mijnheer de minister van Staat, mijnheer de staatssecretaris, waarde collega's, dames en heren, ik ben verheugd u te ontvangen in het halfrond van onze Hoge Vergadering om een onderwerp te bespreken dat zeer actueel en fundamenteel is voor de toekomst van onze samenlevingsmodellen, namelijk de impact van de huidige digitale revolutie op onze democratische waarden en grondwettelijke rechten.

Als reflectiekamer hield de Senaat altijd de vinger aan de pols wanneer erg complexe maatschappelijke problemen behandeld moesten worden, in het bijzonder wanneer een juist evenwicht moest worden gevonden tussen de verschillende grondrechten; de uitoefening ervan kan immers tot conflicten leiden.

Het thema waarover wij vandaag debatteren, ligt overigens in het verlengde van de ideeën en aanbevelingen van de werkgroep 'Informatica en vrijheden', die in 2011 binnen onze commissie voor de Justitie werd opgericht. Ik groet de toenmalige voorzitter van die commissie, die hier aanwezig is.

De hoorzittingen van die werkgroep vestigden de aandacht op een essentiële ontwikkeling, namelijk het ontstaan van een nieuw economisch model: de uitwisseling van 'diensten tegen persoonlijke gegevens' in plaats van wat vroeger de uitwisseling van 'diensten tegen geld' was. Een slogan die aan Tim Cook, de CEO van Apple, wordt toegeschreven, luidt immers 'Als u schijnbaar niks betaalt, dan bent u het product.'

In deze tijden kan eenieders gedrag volledig getraceerd worden dankzij de met internet verbonden toestellen - draagbare telefoons en computers, gps of de iWatch van Apple. De webapplicaties roven vlot onze gegevens en bespieden systematisch ons doen en laten. Google, Facebook, Instagram en dergelijke bespioneren ons. De meest gangbare techniek is het gebruik van de beruchte cookies die ons gedrag op internet registreren. Die technieken, die voor marketingdoeleinden worden opgezet, zouden ook gebruikt kunnen worden om te discrimineren of om overgezonden

informatie te wijzigen. Ook cloudcomputing, waarbij gegevens tegen een lage kostprijs kunnen worden opgeslagen dankzij programma's die op de computer van iemand anders staan, kan betekenen dat iemand minder controle heeft over mogelijk gevoelige informatie die hem aanbelangt.

Men moet dus vaststellen dat iedereen die online is voortdurend nieuwe gegevens verstrekt. In zekere zin is iedereen een soort Klein Duimpje die, deze keer weliswaar onbewust, steentjes laat vallen waardoor hij kan worden teruggevonden. De internetpagina's die worden geraadpleegd, de weblinks die worden doorgestuurd, de persoonlijke informatie die op sociale media wordt verspreid, de meningen die worden gedeeld, maar ook verplaatsingen, aankopen en interesses zijn allemaal sporen die de betrokkene vaak argeloos achterlaat. Al onze gegevens worden door steeds intelligentere programma's samengebracht.

Alles of nagenoeg alles in ons bestaan wordt voortaan gemakkelijker gemaakt, maar wordt ook gestuurd door algoritmes die almachtig zijn geworden. Dankzij de analyse van de massa's gegevens is het specifiek mogelijk om met enige zekerheid – er is zelfs geen sprake meer van waarschijnlijkheid – op het gedrag en de behoeften te anticiperen.

De ontwikkeling van de analyse van massa's data moet gepaard gaan met het stellen van vragen op het gebied van de bescherming van de privacy. De maatschappelijke aanpassingen, bijvoorbeeld, volgen die ontwikkelingen niet en het is niet zeker dat iedereen de impact van zijn gedrag op de bescherming van de privacy begrijpt en onder controle heeft.

Het geheugen van het internet is immers zowel een rijkdom als een gevaar. Eén van de punten waarbij we lang hebben stilgestaan tijdens de werkzaamheden van de werkgroep 'Informatica en vrijheden' was precies het zogenaamde recht op digitale vergetelheid, dat het Hof van Cassatie in zijn arrest van 29 april 2016 heeft beschouwd als een bestanddeel van het recht op eerbiediging van het privéleven. Dat recht op digitale vergetelheid werd al op 13 mei 2014 door het Hof van Justitie van de Europese Unie bekrachtigd, in een zaak waarin een Spaanse burger het tegen Google opnam. David tegen Goliath. Driemaal raden wie gewonnen heeft.

Het is onder andere aan de hand van dergelijke beslissingen van de nationale en Europese rechtscolleges dat de juridische omlijning van de bescherming van persoonsgegevens op het internet tot stand komt. Op

nationaal vlak denk ik bijvoorbeeld, in verband met profilering, aan de beslissing betreffende Facebook, die de voorzitter van de rechtbank van eerste aanleg van Brussel nam, maar die jammer genoeg enkele maanden geleden in hoger beroep werd herroepen. Het gevolg is dat bij de huidige stand van zaken de Belgische burger, die aan massale schendingen van zijn persoonlijke levenssfeer is blootgesteld, momenteel door hoven en rechtbanken niet tegen dergelijke inbreuken kan worden beschermd ten opzichte van buitenlandse actoren.

Tevens heeft het Hof van Justitie van de Europese Unie zich steeds vaker duidelijk moeten uitspreken ten gunste van de rechten van de belanghebbenden, bijvoorbeeld in het arrest-Schrems, waarin het Hof duidelijk bevestigd heeft dat iedere nationale overheid het recht heeft om na te gaan of een transfer van persoonsgegevens vanuit haar lidstaat naar een derde land beantwoordt aan de vereisten voor een afdoend beschermingsniveau.

Wanneer echter de nationale veiligheid op het spel staat, kan het gebruik van vertrouwelijke informatie in procedures onvermijdelijk worden. Dat is het thema van het tweede deel van ons colloquium.

Het is een hele opgave om het Wetboek van Strafvordering aan te passen aan de technologische evolutie. Een wetsontwerp is momenteel in behandeling in de Kamer van volksvertegenwoordigers. Het probeert een antwoord te bieden op de vraag van het gerecht naar een actualisering van de middelen om bewijzen te kunnen vergaren in computersystemen. Bij het schrijven van de tekst werd rekening gehouden met het noodzakelijke evenwicht tussen het onthullen van de waarheid, enerzijds, en de rechten van de verdediging en het beschermen van de private levenssfeer, anderzijds.

Maar ook op Europees vlak komen de maatregelen in een stroomversnelling. Dit brengt mij tot het derde deel van het colloquium, dat handelt over de bescherming van persoonsgegevens. Sinds 4 mei 2016, na vier jaar bespreking, is de nieuwe Europese verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens eindelijk een feit.

In feite waren de huidige teksten, die al meer dan twintig jaar oud zijn, niet meer aangepast aan de nieuwste ontwikkelingen op het gebied van informatietechnologie en evenmin aan de context van globalisering

waarin persoonsgegevens tegenwoordig zowel binnen als buiten de Unie worden uitgewisseld.

De nieuwe verordening neemt alle beginselen en regels die tegenwoordig van kracht zijn, over en maakt ze vaak dwingender. Er worden heel wat nieuwe rechten voor de betrokkenen toegevoegd en nieuwe verplichtingen voor de ondernemingen die gegevens verwerken. De nationale toezichthoudende autoriteiten, zoals de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer, krijgen ruimere bevoegdheden. Ze zullen administratieve boetes kunnen opleggen die tot 4% van de totale wereldwijde jaaromzet van het voorgaande boekjaar kunnen bedragen.

We moeten vaststellen dat 2016 een boeiend jaar was met allerhande wetgevende vernieuwingen. Zoals ik heb gezegd, holt het recht in ethische of bio-ethische aangelegenheden altijd achter de geneeskunde aan. Hier holt het recht achter de technologische innovatie aan.

Mijnheer de voorzitter, waarde collega's, mijnheer de minister, dames en heren, in het licht van deze digitale explosie en de potentiële gevaren ervan is het opbouwen van een klimaat van vertrouwen bij de gebruikers van onlinediensten absoluut fundamenteel. Onderwijs, bewustmaking en verantwoordelijkheid van alle bevoegde overheden en van het maatschappelijk middenveld is een must.

Het is van belang dat de norm de bescherming van de persoonlijke levenssfeer boven alle andere overwegingen plaatst, weliswaar met behoud van het essentiële evenwicht met de andere fundamentele vrijheden, waaronder de vrijheid van meningsuiting.

Als individuen proberen we het recht op ons privéleven en op ons privéterrein te beschermen. We zullen proberen de juiste benaderingswijzen te vinden, maar ook de juiste manier van handelen. De Belgische Senaat heeft zich altijd opgeworpen als een forum met voldoende ervaring om een diepgaande discussie over maatschappelijke uitdagingen aan te vatten. Ongetwijfeld zal ook dit colloquium door kwalitatief hoogstaand werk een aanzienlijke bijdrage leveren tot de huidige gedachtewisseling.

Ik geef het woord aan Eddy Caekelberghs, die de rol van moderator zal vervullen.

De heer Eddy Caekelberghs. – De eerste spreker deze middag is de heer Paul De Hert. Hij is specialist in 'Law, Science, Technology & Society', in strafrecht en in privacy. Het spreekt vanzelf dat de meeste knelpunten van deze namiddag in die gebieden zijn terug te vinden.

Inleiding

De heer Paul De Hert *(in het Frans)*. – Het thema van dit colloquium boeit mij enorm en ik merk dat dit gevoel wordt gedeeld. Ik wil twee zaken aankaarten in verband met de privacy: de onrust en het optimisme. Dat dit thema mensen boeit, wijst erop dat er ook reden is tot optimisme.

(Verder in het Nederlands) Ik hou van het beeld van de 'jardins secrets'. Het is erg mooi. Ik heb ook een tuin. Het gaat niet alleen over wat in die tuin gebeurt, maar ook over wie ik in die tuin uitnodig en over de mensen zonder tuin, over de mogelijkheid om overal een tuin te kunnen hebben in bepaalde omstandigheden.

(Verder in het Frans) Het privéleven is veelzijdig. Het gaat om het recht op intimiteit en ook om het recht om zich met anderen te verbinden, zelfs in het openbaar.

(Verder in het Nederlands) Dat is zo bijzonder aan het recht op privacy. Het is complex en vaag, maar het is er en we herkennen het allemaal. Als Belgische samenleving hebben we een gedeeld begrip van de notie 'privéleven'. Ik heb het moeilijker met het begrip 'inquiétude', maar ik heb het minder moeilijk met optimisme. Als ik ergens gerust in ben, dan is het dat de vragen over het privéleven, die we ons allemaal stellen, gedeelde vragen zijn. Ik merk ook bijvoorbeeld dat bij alle politieke partijen veel belang wordt gehecht aan de bescherming van het privéleven als waarde en dat er alleszins geen opbod is tegen die waarde.

(Verder in het Frans) Ik heb privacy altijd beschouwd als een fundamenteel begrip in onze maatschappij. Het is een waarde die in de Grondwet is opgenomen, weliswaar na enige tijd, maar we hadden al de vrijheid en volgens mij is privacy een aspect van de vrijheid. Ze is ook opgenomen in het Europees Handvest van de grondrechten. Er zijn twee artikelen aan gewijd, het ene over het privéleven, met daarin begrepen de

intimiteit en de 'geheime tuin', en het andere over de bescherming van persoonsgegevens.

In Europa werd duidelijk het onderscheid tussen beide gemaakt, wat ik een goede strategie vind, want de vraag of iets al dan niet binnen de sfeer van de intimiteit valt, is niet de juiste weg om de problemen die zich nu stellen op te lossen.

(Verder in het Nederlands) Onze 'rijke' aanpak in Europa is heel verstandig. We concentreren ons niet alleen op de slaapkamer, op het huiselijk geluk, maar ook op het vermogen om ons te kunnen ontplooien als individu in de samenleving van vandaag, ook al is ze geconnecteerd, ook al zijn er overal sporen. Dat is ook de zienswijze van het Europees Hof voor de Rechten van de Mens: geen definitie van het privéleven, maar een breed begrip om vandaag de vrijheid in deze samenleving te kunnen denken en mogelijk te maken. Voor mij is het praten over 'vie privée, protection des données' een manier om op een interessante manier te praten over vrijheid.

(Verder in het Frans) De waarden die daartegenover staan zijn economische belangen en veiligheid. Ze zijn minder bekend en minder beschermd. Het recht om zich economisch in te dekken staat niet in de Grondwet. Toch is het aanvoelen dat die belangen ook van grote betekenis zijn en dat er moet gezocht worden naar een evenwicht tussen die waarden.

Het verbaast me dat er steeds gewag gemaakt wordt van het einde of de verdwijning van de privacy. Het is nochtans een waarde die een goede bescherming geniet in onze grondwettelijke teksten, terwijl dat voor de tegenovergestelde belangen veel minder het geval is. Als jurist is er dus geen reden tot pessimisme. Dat is geen punt; de privacy is een goed verankerde waarde, die overal erkend wordt.

(Verder in het Nederlands) U had het over *cloudcomputing*, over cookies, over het geconnecteerde individu dat sporen, '*traces*', nalaat. U hebt over de kracht van algoritmes gesproken, over het eroderende vertrouwen in onze menselijke relaties. Dat zijn bezorgdheden die we absoluut ernstig moeten nemen. Het is ook van belang dat we al die bezorgdheden stuk voor stuk ernstig nemen. Wat ik vandaag dus niet wil, is dat mensen van de veiligheidsdiensten en van de politie met de vinger wijzen naar Facebook en dergelijke, en dat mensen vanuit de privésector met de vinger

wijzen naar de overheid. Dat is geen interessant debat. Ik stel vast dat het veel te veel op die manier wordt gevoerd. Het wordt een soort pingpongspel: 'Het zijn wij niet, het zijn de anderen'.

(Verder in het Frans) Daar doen we niet aan mee. We beschouwen elk fenomeen als iets wat onze volledige aandacht verdient en overwegen alle bezorgdheden die te maken hebben met onze grondrechten. Ik vraag dus aan de mensen van de overheidssector om het niet over Facebook te hebben en aan de mensen uit de privésector om zich niet te beklagen over de beperkingen van het recht op privacy die overheidsinstellingen opleggen.

Wat staat hier vandaag op het programma? Een eerste panel zal het fenomeen zelf in kaart brengen, een tweede zal zich buigen over de problemen die kunnen ontstaan vanuit het overheidsoptreden en het derde panelgesprek zal gaan over de traceerbaarheid en is zowel van toepassing op de overheidssector als op de privésector. Maar ik vermoed dat we het vooral zullen hebben over onze Amerikaanse 'vrienden'.

(Verder in het Nederlands) Ik ben heel blij dat er dan een politiek debat komt. Ik hou heel erg van die politieke debatten. Meestal komen we dan tot de vaststelling dat er in ons land misschien ruzie wordt gemaakt over belastingen, maar over het privéleven eigenlijk niet. Politici, mannen en vrouwen, beseffen als geen ander hoe belangrijk het is om niet over alles te tweeten en om nog eens op restaurant te kunnen gaan met toekomstige partners, zonder dat de hele wereld het weet. In zekere zin is de waarde van de privacy goed geborgen bij onze politieke vertegenwoordigers, die ook bepaalde verwachtingen over die privacy hebben. Ik zeg altijd tegen de mensen: 'Het gaat zeer goed met het privéleven. We hebben zelfs een staatssecretaris voor het privéleven.' Dan begint iedereen te lachen, maar de vaststelling is pertinent.

(Verder in het Frans) In de regering zijn debatten gevoerd over verschillende aspecten van het privéleven. Vroeger verliep de discussie vooral meerderheid tegen oppositie. De meerderheid is nu verplicht om zich te buigen over die aspecten van het privéleven, die vaak in hoofdzaak gaan over beginselen van goed bestuur. In feite gaat het erom goed na te denken over wat men doet en te onderzoeken hoe een doel kan worden bereikt zonder al te veel schadelijke gevolgen of problemen op het gebied van de privacy.

(Verder in het Nederlands) Het is dus goed dat we een staatssecretaris hebben en dat de structuren er zijn. Kamer en Senaat hebben de afgelopen vijftig jaar interessante debatten gevoerd over het privéleven, over alle grenzen heen. Ik verwijs onder meer naar het debat over de telefoontap, een maatregel die na jarenlange reflectie werd ingevoerd. Voor sommigen te laat, volgens mij na rijp debat. Waarom is er reden tot optimisme? Het feit dat ik hier de introductie mag doen is natuurlijk persoonlijk een aangename ervaring, maar ik zie vooral rijpheid in onze samenleving, waar 's avonds de gordijnen worden gesloten, terwijl men even ten noorden van ons die reflex nog niet heeft. Dat zal wel komen als ze daar ontdekken hoe belangrijk het privéleven is. Ons land heeft op het vlak van privacy een enorme knowhow opgebouwd. Ik zie ook positieve ontwikkelingen op meerdere terreinen.

(Verder in het Frans) Het recht om vergeten te worden is een belangrijk recht dat zowel op Europees als op Belgisch niveau erkend wordt. Mensen moeten hun kinderen niet verbieden om op het internet te surfen. Integendeel, ze moeten hen daartoe aanmoedigen, want ze zijn goed beschermd. Het vergeetrecht – of het recht op vergetelheid – helpt kinderen om zich in dit verband te ontwikkelen. Dit aspect moet niet benaderd worden vanuit de angst voor technologie.

In België zijn er verschillende wetten die betrekking hebben op de bescherming van de privacy. We zijn verwend. Bij twee Europese gerechtshoven is er al heel wat rechtspraak over. We zullen het straks over de verordening ter zake hebben, die van zeer groot belang is. We hebben ook een instantie die hierop toezicht houdt. Als we dit vergelijken met de arbeidersstrijd of milieukwesties, beseffen we dat er voor die materies lang niet zoveel controle-instanties zijn als voor de bescherming van het privéleven. We hebben een Privacycommissie die de burger gratis kan bijstaan om tegen Goliath te strijden! Die dienst wordt door de Staat georganiseerd en betaald en werkt bovendien op geheel autonome wijze. Is dat geen mooi voorbeeld van creativiteit?

Er is dus een verordening, er zijn nieuwe rechten en verplichtingen en een Privacycommissie met verreikende bevoegdheden.

(Verder in het Nederlands) Ik ben zeer blij met de grote opkomst en kijk dan ook uit naar het debat dat hier vandaag zal worden gevoerd.

In artikel 16 van het Verdrag betreffende de werking van de Europese Unie staat iets heel vreemds, namelijk dat alles wat de bescherming van persoonsgegevens aangaat, in principe in aanmerking komt voor Europese wetgeving. Dat is een consensusartikel. Europa voelde namelijk aan dat men Europees moet denken in de strijd met de technologiegiganten en in de strijd met de andere supermachten, die op het vlak van het privéleven geen vertrouwen inboezemen. De subsidiariteitsgedachte achter de Europese Unie werd opzijgeschoven voor een volledig mandaat aan de Europese Unie voor de reglementering op het vlak van de bescherming van persoonsgegevens. Dat is een verstandige keuze, op voorwaarde dat men op nationaal vlak niet in slaap valt omdat de Europese Commissie het zal regelen.

Welnu, we vallen niet in slaap, we zijn alert.

De heer Eddy Caekelberghs *(in het Frans).* – Het eerste deel van onze werkzaamheden betreft de persoonlijke levenssfeer en de opkomst van nieuwe technologieën. Het eerste onderdeel gaat over het standpunt van de bedrijven. De CEO van Agoria, de heer Marc Lambotte, heeft niet alleen de zware opdracht het standpunt van de bedrijven toe te lichten, maar ook onverwacht de baas van Google te vervangen, die was gevraagd om deel te nemen aan dit colloquium. Aangezien de baas van Google meestal dienst doet als *punching ball*, neem ik aan dat de heer Lambotte alvorens naar hier te komen een sporttraining achter de rug heeft om zich voor te bereiden op alle vragen die we hem zouden kunnen stellen!

Het woord is aan de heer Lambotte.

De persoonlijke levenssfeer en de opkomst van nieuwe technologieën

Het standpunt van de bedrijven

De heer Marc Lambotte. – Ik zal een niet-technisch verhaal brengen, een verhaal oude stijl. Vroeger was er een eenvoudige manier om onze privacy te garanderen: het volstond om de gordijnen dicht te doen.

(Verder in het Frans) Degenen die nog in een oud kantoor werken, een kantoor met een deur, weten dat het volstaat om ze te sluiten om in alle rust te kunnen praten. De wereld is echter veranderd. We spreken over privacy. Is dat nog iets reëels of is het een illusie geworden?

(Verder in het Nederlands) Toen ik vele jaren geleden, na een verblijf in Engeland, naar België terugkwam, stonden we net aan het begin van de opmars van de gsm. Niemand stelde zich daarbij vragen over de privacy. Na een tijdje werd duidelijk dat de operatoren, met een beetje moeite, konden achterhalen waar iemand zich op een bepaald moment bevond. Toen werd als excuus gegeven: 'Het is niet erg, we geven die informatie alleen aan de politie'.

(Verder in het Frans) Vandaag hebben we allemaal een smartphone en we geven hem graag de toestemming ons op elk moment te volgen en deze informatie door te geven aan privébedrijven. De meeste mensen vinden dat normaal.

Als ik 's avonds mijn Samsung Smart TV aanzet, kan ik me afvragen wat mijn televisie doet terwijl ik kijk. Ziet hij mij? Hoort hij mij? U weet allemaal dat het antwoord 'ja' is. Weerhoudt mij dat om televisie te kijken? Neen, ik richt de kleine camera naar een andere kant, maar dat is een andere kwestie.

(Verder in het Nederlands) Wie leest mijn emails? Wie leest mijn sms'jes? Wie weet dat ik hier ben? Wie weet wat ik aan u vertel? Wie weet wat er op deze pc staat? Indien u zich het eerste scherm van de slides herinnert, kan ik u met 99 procent zekerheid zeggen dat deze pc 'extremely hackable' is. Hij draait immers op een zeer oude Windowsversie waarvoor geen securityupdates meer beschikbaar zijn. En we bevinden ons in de Senaat, dames en heren! Ik hoop dat niemand ooit op het slechte

idee komt om dit onding op het internet aan te sluiten, want dan moeten we echt niet komen huilen. Op calimeroreflexen kom ik straks nog terug.

Eigenlijk gaat het hier om een zeer eenvoudig probleem. Dit hele debat kan samengevat worden in twee eenvoudige vragen: wie mag welke informatie hebben en wie mag er wat mee doen? Daar stopt het probleem. We moeten het niet moeilijker maken. Dit is de kern van de zaak, al de rest is techniciteit. Ik geef een voorbeeld: vind ik het erg dat de Staatsveiligheid mijn telefoontjes afluistert of mijn sms'jes leest? Mijn persoonlijke mening is dat het mij totaal niet kan schelen, afhankelijk van wat ze ermee doen. Hier is het tweede deel van de vraag belangrijk: wat mogen ze ermee doen? Als het erom gaat uw en mijn veiligheid te garanderen, heb ik daar echt geen probleem mee. Sommigen onder ons zouden evenwel van mening zijn dat het een heel andere zaak wordt indien hun sms'jes aan hun partner zouden worden doorgegeven. Dan wordt het gevoeliger. Net daarom is die tweede vraag zo belangrijk. Het verhaal verandert helemaal indien een willekeurige verzekeraar informatie zou verzamelen over mijn DNA, over mijn genoom, met het oog op de bepaling van mijn verzekeringspremie en om te weten of ik al dan niet verzekerbaar ben. In dat geval zullen wij al veel vlugger zeggen dat zoiets niet kan.

(Verder in het Frans) Het is dus een keuze.

De nieuwe munt heet Privacy. Ik betaal niet in euro voor het gebruik van de Googlebrowser, mijn favoriete toegang tot het internet, maar ik betaal met die nieuwe munt en ik lever een beetje privacy in.

Men vraagt uiteraard onze instemming met de lange en saaie lijst van voorwaarden voor het gebruik van de software. De overgrote meerderheid van de gebruikers gaat akkoord zonder de voorwaarden te hebben gelezen. En daar situeert zich het probleem. Beslissen is iets anders dan bewust beslissen.

(Verder in het Nederlands) Ik ben van opleiding onderwijzer en lesgevers verstaan één kunst: zij moeten zeer complexe dingen kunnen uitleggen op een heel eenvoudige manier. Ik kan u verzekeren dat ik de lange teksten die door Google zijn opgesteld in voor iedereen heel verstaanbare woorden, kan resumeren. Dat is zeer gemakkelijk: als u mijn product gebruikt, heb ik het recht om alles wat u met mijn product op het internet doet, op te slaan, te analyseren en te verkopen. Dat is alles.

(Verder in het Frans) Dat is eenvoudig gezegd. Al de rest is blabla waarmee juristen hun kost verdienen.

Ik heb kort samengevat waar het om gaat.

(Verder in het Nederlands) Wij gaan er dus van uit dat wij vertrouwen kunnen hebben. We kijken naar anderen, in dit geval de overheid, om ervoor te zorgen dat ons privéleven wordt beschermd. Dat is een calimeroreflex: ik heb een probleem en de anderen moeten het oplossen. Zo werkt het niet. Ik heb een probleem met deze pc en iemand anders zou het moeten oplossen? Men mag niet alleen naar de overheid kijken.

Vanuit Agoria onderschrijven wij alle op de slide vermelde principes: de bescherming van de persoonsgegevens, die al dateert van 1992; de Europese verordening waarover zoveel te doen is geweest en die een antwoord is op een veranderende wereld, namelijk een wereld waar we met sociale media bezig zijn; en een aantal basisprincipes voor de herziening van de privacywetgeving.

Laten we kijken naar een aantal zaken waarvoor we aandacht moeten hebben. Ik zal het nu niet te veel hebben over de kostprijs voor de bedrijven – dat komt later aan bod – maar er moet wel een zeker evenwicht zijn.

We weten allemaal dat een computer die heel veel werkt, weinig in panne valt of uitgeschakeld staat, geld kost: 99,95% uptime, zoals dat heet, heeft een prijs, 99,99% heeft een veel hogere prijs en 99,999% is zo goed als onbetaalbaar. Wat is nodig, waar ligt het evenwicht? Vandaag gaat het niet alleen over persoonsgegevens. We bevinden ons in een digitale transformatie en dat betekent dat er overal big data, overal gegevens zijn, voortdurend en in enorme hoeveelheden.

(Verder in het Frans) Laten we het daarover eens zijn, men kan zich ertegen verzetten, men kan ertegen zijn, maar het is de realiteit: het is onmogelijk de technologische vooruitgang tegen te houden. We moeten ermee leven.

(Verder in het Nederlands) Rond bewustwording wil ik u toch wel iets vertellen. Voor de bedrijven die lid zijn bij ons, hebben we een grote bewustmakingscampagne opgezet, omdat bedrijven daar heel erg mee bezig zijn. Ze vragen zich af hoe ze die gegevens moeten beschermen. Ze zijn ook een beetje bang, want er komen allerlei regeltjes op hen af. Dan

is hun vraag: 'Agoria, hoe kunnen jullie mij helpen?' De hoeveelheid vragen die wij op dit moment over de verordening krijgen, is zeer hoog. Dat is ook normaal, want in mei 2018 moet iedereen klaar zijn. Men stelt zich dus de vraag: 'Wat moet ik doen, wat moet ik klaar hebben?'

(Verder in het Frans) Eerst sensibiliseren, vervolgens informeren en tot slot begeleiden.

Ik ben fier het nieuwe Agorialogo te kunnen tonen. Het wordt voorafgegaan door een punt. De punt staat symbool voor het einde van een zin, maar wij hebben de punt voor onze naam gezet, want waar de anderen stoppen, gaat Agoria door. Is het niet mooi?

(Verder in het Nederlands) We gaan dan verder, we gaan begeleiden. Waarom? Omdat we dat punt willen waarmaken en zo doen we dat. Probeert u maar eens met de blote hand een spijker in een plank te krijgen. Dat gaat niet zo goed, daar hebben wij gereedschap voor uitgevonden.

(Verder in het Frans) We hebben een instrument ontwikkeld om de bedrijven te begeleiden. We helpen hen hun risico's te herkennen en tonen hen hoe ze die risico's kunnen verkleinen. We helpen hen zodat ze weten wat ze moeten doen – en eventueel veranderen – bij de ontwikkeling en bij het gebruik van de technologie als een bondgenoot. De technologie is immers geen vijand, maar een bondgenoot die bedrijven helpt hun doestellingen te bereiken op vlak van transparantie, om hun gegevens te beheersen enzovoort. Dat lijkt dus tegenstrijdig.

In de toekomst zullen we blijven samenwerken met de Privacycommissie met slechts één doel voor ogen.

(Verder in het Nederlands) Het doel is privacybescherming op een pragmatische, correct onderbouwde manier te realiseren. Zodat ze betaalbaar blijft. Zodat we niet meer moeten uitgeven dan nodig is, ook in een wereld van hightech.

Dit is een beeld van een toilet in Gent. Weet u waar dat toilet zich bevindt? U moet het eens gaan bezoeken. Het bevindt zich in het restaurant The Belga Queen. U komt daar aan en misschien voelt u zich daar niet zo op uw 'gemak'. Het is nogal doorzichtig. Ga er eens naartoe en u zult merken dat op het moment dat de deur dichtgaat, de ramen ondoorzichtig worden. Ook dat is technologie. Ik gebruik deze boutade om er u

opmerkzaam op te maken dat wat een probleem kan lijken te zijn, ook opgelost kan worden door technologie.

Mijn laatste slide is dezelfde als mijn eerste. Wij moeten af en toe de gordijnen terug dicht kunnen doen. Wij hebben recht op privacy en wij moeten kunnen kiezen wanneer we privacy willen, zowel in ons privéleven als in ons bedrijfsleven. Laten we dat doen zonder de bedrijven op overdreven kosten te jagen.

Ik wil nog één waarschuwing uiten: de fundamentalisten die zeggen dat technologie een gevaar is voor het privéleven, hebben natuurlijk gelijk. Als ik geen gsm had, dan zou men mijn gesprekken ook niet kunnen afluisteren. Dat is logisch. Bovenal kan technologie hier onze vriend zijn. Dankzij technologie is het mogelijk om van privacy geen binair verhaal te maken. Dankzij technologie kunnen wij bepalen wie welke informatie mag hebben en dan moeten we alleen nog maar afdekken wat zij ermee mogen doen. Technologie is geen ja/neen-verhaal en dat is dus het foute debat. Het juiste debat moet gaan over wie welke informatie mag hebben en wat ze ermee mogen doen. Dat gaat veel verder dan pure technologie.

De heer Eddy Caekelberghs. – Tijdens het debat zullen we de gelegenheid hebben om vragen te stellen.

Mijnheer Lambotte, u hebt mijn belangstelling gewekt met deze *privacy currency unit*. Voor onze privacy zullen we in elk geval moeten betalen.

(Verder in het Frans) Aangezien we het over technologie hebben, stel ik voor ze te gebruiken bij de volgende uiteenzetting door de heer Giovanni Buttarelli, die sinds december 2014 de Europese toezichthouder voor gegevensbescherming is. De heer Buttarelli was voordien adjunct-toezichthouder. Hij heeft bovendien veel ervaring als Italiaanse autoriteit op het gebied van de bescherming van gegevens en is lid van de Italiaanse magistratuur. Om precies te zijn, hij is cassatierechter. De heer Buttarelli zal ons een kort overzicht geven van de Europese wetgeving ter zake.

Het standpunt van de Europese Unie

De heer Giovanni Buttarelli *(in het Engels).* – Vooreerst dank voor de uitnodiging om vandaag met u te spreken.

Als Europese toezichthouder voor gegevensbescherming hebben we de mogelijkheid te interageren met de beleidsmakers binnen en buiten Europa. De cultuur en de politiek verschillen van land tot land, maar België heeft het belang van de privacy en de bescherming ervan heel goed begrepen. Het heeft voor de eerste keer sinds zijn bestaan een lid van de regering speciaal belast met de bescherming van het privéleven met betrekking tot persoonsgegevens. België is zonder twijfel de eerste EU-lidstaat die dat heeft gedaan. Ik had het genoegen onlangs de heer De Backer te ontmoeten. We hebben van gedachten gewisseld over de grote uitdagingen waarmee onze digitale maatschappij wordt geconfronteerd. Ik ben ervan overtuigd dat we andere gelegenheden zullen hebben om die gedachtewisseling voort te zetten. We hadden het over de manier waarop het nieuw Europees juridisch kader voor de bescherming van gegevens zal worden toegepast.

Voorts heeft België het belang van de bescherming van het privéleven goed begrepen omdat het veel ervaring heeft met online diensten, in het bijzonder de elektronische identiteitskaart, de automatische uitwisseling van gegevens in de sociale zekerheid, eHealth en Taxonweb. België is trouwens in vele opzichten een land dat nauw betrokken is bij nieuwe elektronische technologieën. Er wordt actief geïnvesteerd in online overheidsdiensten en de verschillende sectorale comités garanderen dat er niet wordt binnengedrongen in het privéleven van de burgers. België beschermt ook degenen die datatechnologie gebruiken. De Commissie voor de bescherming van de persoonlijke levenssfeer is trouwens één van de belangrijkste actoren in de Werkgroep Artikel 29 voor de bescherming van persoonsgegevens. Ze deinst er niet voor terug grote internationale ondernemingen aan te vallen als ze meent dat de individuele rechten zijn geschonden, zoals we gezien hebben met Facebook.

Persoonlijk ben ik al meer dan twintig jaar actief in de sector van het toezicht op de bescherming van gegevens. Vaak wordt de bescherming van gegevens beschouwd als iets technisch, abstracts, buiten het politieke debat. Ik ben ervan overtuigd dat het nieuwe reglement voor de bescherming van gegevens en de richtlijn ter zake voor de strafrechtspraak een

doeltreffend antwoord is op problemen die ontstaan door technologieën die verband houden met big data en persoonsgegevens.

Hoe het ook zij, de wet heeft ook beperkingen. Noch de richtlijn van 1995, noch de nieuwe algemene verordening gegevensbescherming zullen beletten dat het toezicht het belangrijkste element wordt voor de werking van het internet. De wet kan nooit het tempo van de technologische evolutie volgen. Dat is de reden waarom het ethische aspect mij bijzonder interesseert. In september 2015 publiceerde ik hierover een artikel waarin ik het belang van de menselijke waardigheid ten opzichte van technologieën als artificiële intelligentie, intelligente huizen, *connected cars* enzovoort benadruk.

In december vorig jaar hebben we een raadgevend ethisch comité opgericht om de verbanden tussen de mensenrechten, de technologie en de markten en de ondernemingsmodellen voor de eenentwintigste eeuw vanuit ethisch oogpunt beter te begrijpen. Het accent wordt gelegd op de consequenties voor het recht op de bescherming van gegevens in een digitale omgeving.

Ethiek, de opvatting of iets slecht is of goed, is universeler dan het westerse begrip van bescherming van gegevens. Ethiek gaat verder dan de wet. Ethiek roept veel vragen op. Is het bijvoorbeeld mogelijk dat een onderneming die inlichtingen behandelt de letter van de wet naleeft en zich daarbij niet ethisch gedraagt? Hoe een dergelijke kwestie analyseren? Zijn de regulerende overheden in staat deze vraag te ontleden? Voor mij zijn big data het perfecte voorbeeld van dit probleem. Het is het fenomeen waarbij men met heel krachtige computers gegevens uit uiteenlopende bronnen verzamelt en analyseert, daaruit conclusies trekt over het (menselijke) gedrag en het beïnvloedt.

Big data zijn een voorbeeld van de wijze waarop persoonsgegevens de handelingen en de technologieën op de markt en in de publieke sfeer een bepaalde richting kunnen geven. Artificiële intelligentie, *virtual reality* en robotica staan voor de deur en worden over enkele jaren werkelijkheid. Deze technologieën leiden tot diepgaande vragen op het vlak van mensenrechten, maar brengen er ons ook toe ons af te vragen wat ‘mens zijn’ betekent.

Men moet weer verder gaan in het onderzoek naar de ethische component van onze digitale samenleving. Big data kunnen bijdragen tot

onmiskenbare voordelen voor de samenleving, maar de vraag is te weten wie er voordeel uit deze vooruitgang zal halen. De samenleving in het algemeen of alleen enkele individuen of bedrijven?

Alles wat betrekking heeft op de behandeling van gegevens heeft een impact op het privéleven. In een *big data*-omgeving kunnen onschuldige gegevens uit verschillende bronnen verzameld worden en een heel precies beeld geven van de gedragingen van mensen. De persoonsgegevens over het gedrag van mensen zijn vandaag koopwaar en een belangrijke commerciële troef.

In mijn recent opiniestuk over digitale ethiek leg ik de nadruk op vier punten: gegevens- en privacybescherming zijn belangrijke instrumenten om de menselijke waardigheid te beschermen; deze rechten zijn opgenomen in de Europese verdragen en het Handvest van de grondrechten van de Europese Unie; ze geven de mens het recht zijn persoonlijkheid te ontwikkelen en een zelfstandig leven te leiden, te innoveren, en andere vrijheden en rechten uit te oefenen. Men moet er leidende principes van maken voor het gebruik van het internet.

Ten tweede, onze rechten en waarden mogen niet door de technologie worden bepaald. Men moet rekening houden met hun impact op de waardigheid, op de individuele vrijheden en op de werking van de democratie.

Ten derde, zoals ik daarstraks zei, volstaat het in de huidige digitale omgeving niet zich aan te passen aan de wet. Men moet ook rekening houden met de ethische dimensie.

Ten vierde hebben big data eveneens een weerslag op het vlak van de techniek, maar er zijn ook de filosofische, legale en morele consequenties. Deze laatste moeten deel uitmaken van onze reflectie over de digitale maatschappij.

De adviesgroep ethiek werkt dit jaar intensief aan de klassieke benadering van de reglementering van gegevens en toetst die aan de nieuwste technologieën. De adviesgroep buigt zich over enkele essentiële vragen.

Ten eerste, wat betekent privacy in een samenleving die gekenmerkt wordt door een massale uitwisseling van gegevens? We weten dat de visie op privacy aan het veranderen is om de eenvoudige reden dat vele mensen heel veel persoonlijke informatie uitwisselen op de sociale

media; maar niet iedereen wil gegevens overdragen. Ze zijn daarin selectief. We moeten in deze context dus echt onze definitie van het privéleven herzien.

Ten tweede, in welke mate zal de ethiek de ontwikkeling van nieuwe technologieën beïnvloeden? Voor mij is er geen binaire indeling van innovatie en ethiek. Integendeel, de ethische overwegingen moeten de innovatie sturen. Als we ons van bij het begin inschrijven in een ethische benadering bij de ontwikkeling van alle belangrijke innovaties, zullen we de vooruitgang aanmoedigen en garanderen we een samenleving die berust op menselijke waarden.

Ten derde, is ethiek een alternatief voor wetten of is het complementair? Ik ben ervan overtuigd dat de verantwoordelijke organisaties zich laten leiden door ethiek. Het volstaat niet dat een bedrijf zich aanpast aan de wet.

Voor mij is de technologie in termen van waarden niet neutraal. De technologie is het resultaat van de menselijke vindingrijkheid en de waarden die de ingenieurs inspireren. Spijtig genoeg werd het internet gedomineerd door wetenschappers en briljante technici die niet noodzakelijk hebben nagedacht over de fundamentele waarden, zoals de menselijke waardigheid, de privacy en de vrijheid van meningsuiting. Het doel van de adviesgroep is dat te veranderen en een groep juridische experts en ingenieurs bijeen te brengen.

Ik hoop dat dit zal bijdragen tot een duurzame ontwikkeling op lange termijn en tot de competitiviteit van de digitale eenheidsmarkt in de Europese Unie. Ik beëindig mijn uiteenzetting met deze uitdaging, die hoop ik een aanleiding zal zijn voor het openen van het debat.

Ik vind het spijtig dat ik vandaag niet fysiek aanwezig kon zijn. Ik weet dat u een vruchtbare en onderbouwde discussie zult hebben, want België heeft goed begrepen wat er op het spel staat. Ik wens u een geslaagde, zeer vruchtbare bijeenkomst, en hoop in de toekomst fysiek aanwezig te kunnen zijn.

De heer Eddy Caekelberghs *(in het Frans).* – Ik denk dat we de essentie van de uiteenzetting van de heer Buttarelli hebben begrepen.

Ik geef nu het woord aan mevrouw Elise Degrave, die bronnen en beginselen van het recht, internetbeheer en e-government doceert aan de rechtenfaculteit van Namen. De overgang is ideaal, want de heer Buttarelli heeft zopas het Belgische e-government en de toepassingen ervan lof toegezwaaid.

De persoonlijke levenssfeer en de opkomst van nieuwe technologieën

Mevrouw Elise Degrave *(in het Frans).* – Ik stel voor om nu, na de bescherming van de privacy vanuit het standpunt van de bedrijven en de bescherming van de privacy op het niveau van de Europese Unie, de bescherming van de privacy van de burgers ten overstaan van de Staat en meer in het bijzonder ten overstaan van de administratie, die steeds meer geautomatiseerd wordt, te onderzoeken. In dat opzicht rijst de volgende cruciale vraag: hoe kan men ervoor zorgen dat de burger, die geconfronteerd wordt met een administratie die meer en meer steunt op moeilijk te begrijpen informatica, vat krijgt op de administratie, deze begrijpt en controleert en hoe kan men vermijden te vervallen in een duistere, kafkaiaanse administratie?

Laat ons eerst de balans opmaken van de omwentelingen die de administratie doormaakt, zowel wat haar structuur als haar werking betreft. Gedurende lange tijd was de administratie volgens een silostructuur opgebouwd; de ministeries waren van elkaar gescheiden en verzamelden elk langs hun kant de gegevens die nodig zijn om de dossiers van de burgers te behandelen. Met de opkomst van het internet groeide het besef dat het misschien niet noodzakelijk is dezelfde gegevens meerdere malen aan de burgers te vragen en dat de betrokken afdelingen deze gegevens zouden kunnen uitwisselen. Er werd over nagedacht en dit leidde tot een structuurwijziging van de administratie, die voortaan als een netwerk werd georganiseerd. Daartoe heeft men de administraties met gemeenschappelijke kenmerken geïdentificeerd; de administraties die de sociale zekerheid beheren, werden gegroepeerd, net als de fiscale administraties of zij die zich met voertuigen bezig houden. Op deze grondslag heeft men sectorale netwerken gecreëerd, zoals het sectorale netwerk van de sociale zekerheid. In het centrum van het netwerk heeft men een kruispuntbank opgericht, dat wil zeggen een instelling belast met de behandeling en de doorvoer van gegevens binnen het netwerk. Het belangrijkste kenmerk

van dit model is inderdaad dat de gegevens niet in de kruispuntbank worden gecentraliseerd omdat dit grote gevaren met zich mee zou brengen in geval van piraterij. Men heeft eerder gekozen voor het verspreiden van de gegevens over het gehele netwerk. Zo heeft men bijvoorbeeld beslist dat de Dienst voor Pensioenen de gegevens inzake pensioenen zou behandelen terwijl het Rijksregister zich met de burgerlijke gegevens zou bezig houden. Zodoende neemt een administratie contact op met de kruispuntbank als ze gegevens nodig heeft waarover ze niet beschikt. De kruispuntbank haalt de gegevens op bij de administratie die ze opgeslagen heeft en geeft ze door aan de verzoekende administratie. Het voordeel van deze procedure is dat de gegevens veel betrouwbaarder worden. Deze worden immers één keer opgeslagen in het netwerk en vallen onder de verantwoordelijkheid van een administratie die moet toezien op hun juistheid en hun updating.

In concreto houdt deze procedure een administratieve vereenvoudiging in; eertijds was een burger gehouden tot het meermaals doorgeven van dezelfde gegevens aan verschillende administraties, terwijl hij vandaag in principe deze gegevens slechts één keer meedeelt aan het sectorale netwerk, dat de gegevens doorstuurt.

De vraag die sinds enkele jaren wordt gesteld, is of een administratie verplicht is de in het netwerk beschikbare informatie op te zoeken, dan wel of ze louter over de mogelijkheid beschikt om dat te doen.

Meerdere wetten en decreten bepalen dat de administraties verplicht zijn de gegevens in het netwerk te gaan opzoeken zonder zich opnieuw tot de burger te richten. Dat wordt de onrechtstreekse gegevensverzameling genoemd. Als de gegevens beschikbaar zijn, dient de administratie ze dus zelf te gaan opzoeken. Dit impliceert een belangrijke cultuurwijziging in de administratie. Deze wijziging begint zich langzamerhand door te zetten, maar is nog niet volledig ingeburgerd. Wanneer de administratie bepaalde gegevens nodig heeft, moet ze eerst aan de kruispuntbank vragen of deze beschikbaar zijn.

Dit vergemakkelijkt de administratieve vereenvoudiging aanzienlijk. Laat ons een voorbeeld nemen: een burger die een sociale uitkering van het OCMW wenste te verkrijgen, werd gevraagd een aantal documenten voor te leggen met het oog op de samenstelling van zijn dossier. De burger was er niet in geslaagd een document voor te leggen in verband met de uitbetaling van kinderbijslag enkele jaren voordien en het OCMW

besliste dat er sprake was van een gebrek aan samenwerking vanwege de burger en dat zijn dossier onvolledig was. Bijgevolg werd zijn aanvraag tot een uitkering geweigerd. De zaak werd voor het Arbeidshof in Brussel gebracht, waar een rechter zetelde, die reeds zeer goed op de hoogte was van e-government en administratieve vereenvoudiging. Deze rechter stelde vast dat het gevraagde document beschikbaar was in het sectoraal netwerk en dat het OCMW verplicht was het document zelf op te zoeken. Het OCMW werd bijgevolg veroordeeld tot het betalen van de sociale uitkering.

Wanneer de burger het recht heeft te weigeren een opnieuw gevraagd document voor te leggen en de administratie voor haar verantwoordelijkheden kan stellen, rijst van meet af aan de vraag waar zijn gegevens zich bevinden. De burger moet er zeker van zijn dat zijn gegevens in het netwerk zijn opgenomen en dat hij de administratie voor haar verantwoordelijkheid kan stellen. Op dat vlak zijn de zaken momenteel zeer ingewikkeld. Toen er nog geen sprake was van de nieuwe technologieën, wist de burger min of meer waar zijn gegevens zich bevonden; vroeg men hem om fiscale gegevens, dan richtte hij zich tot de fiscus.

Vandaag zijn de omstandigheden volledig ondoorzichtig geworden. De gegevens zijn verspreid, de administraties weten zelf niet goed waar de gegevens zich bevinden aangezien ze zich tot de kruispuntbank moeten wenden om de gegevens te bekomen; er bestaat bijgevolg een reëel probleem van transparantie wat de werking van de administratie betreft.

Hoe kan de burger vandaag toegang krijgen tot zijn gegevens? Er bestaan een aantal hulpmiddelen, waarvan er sommige zeer archaïsch zijn. Ik denk bijvoorbeeld aan de toegang tot de gegevens verzameld in de Kruispuntbank van de Sociale Zekerheid (KSZ). Indien u wenst te weten welke gegevens die u aanbelangen zich in het netwerk van de sociale zekerheid bevinden, dient u zich tot de KSZ te wenden door het handmatig invullen van een bijzonder langdradig document, een fotokopie te nemen van uw identiteitskaart, het geheel te posten en een geschreven antwoord af te wachten. Dezelfde procedure wordt voorgeschreven door de Privacycommissie: indien u zich wil wenden tot welke administratie dan ook om te vernemen wat ze over u weet, moet u een modelbrief invullen, aankruisen wat de reden is van uw verzoek, een fotokopie nemen van uw identiteitskaart, het geheel verzenden langs de post en het antwoord afwachten. Dit is vrij cynisch: men krijgt de indruk dat de e-administratie op dit ogenblik vooral ten gunste van de administratie werkt. Enorme

middelen worden ter beschikking van de administratie gesteld om ze tijd en geld te doen winnen en om ze efficiënt te doen functioneren. Maar tegelijkertijd moet de burger volstrekt archaïsche hulpmiddelen gebruiken, wat sommigen tot de uitspraak brengt dat de administratie zich met een limousine voortbeweegt terwijl de burger te voet gaat.

Gelukkig bestaat er een hulpmiddel, waarover men wonderlijk genoeg weinig spreekt: het Rijksregister. Op de website van het Rijksregister bevindt zich een rubriek 'Mijn dossier', waarmee men toegang krijgt tot zijn dossier in het Rijksregister door zich te identificeren met zijn identiteitskaart.

Het is een zeer gebruiksvriendelijk hulpmiddel. Het moeilijkste is het terugvinden van de pincode van de identiteitskaart, die men alsnog bij de gemeente kan bekomen. Als u erin slaagt in te loggen, krijgt u toegang tot uw gegevens bij het Rijksregister, maar u kunt ook klikken op een interessant tabblad 'Historiek van de raadplegingen', dat u in staat stelt na te gaan welke instellingen uw gegevens hebben geraadpleegd. Gedurende lange tijd kon men tevens het nummer zien van de beambte die de gegevens had opgevraagd, maar deze mogelijkheid werd geschrapt omdat de Privacycommissie van oordeel was dat dit inging tegen de privacy van de beambte.

Hoe dan ook beschikt men over de mogelijkheid zich te richten tot de instelling die de gegevens heeft opgevraagd om te vernemen waarom zij werden geraadpleegd.

Toen ik aan mijn proefschrift werkte, heb ik mijn onderzoek geconcretiseerd door te proberen na te gaan hoe dit in zijn werk ging. Ik merkte dat een beambte van mijn gemeente 's avonds, om 21 uur, mijn foto had opgevraagd. Na onderzoek bleek dat hij de foto jammer genoeg slechts één keer had geraadpleegd. Ten overstaan van deze spijtige vaststelling zijn er twee opties mogelijk: ofwel was ik zijn type niet, ofwel heeft hij de foto geïnstalleerd als schermbeveiliger. Ik wenste te weten of ik een geheime bewonderaar had en wie hij was. Ik richtte mij tot de gemeente, die mij niet kon antwoorden. Zij stuurde mijn vraag naar de politie, die op haar beurt de vraag naar de burgerlijke stand stuurde. Aangezien niemand mij kon antwoorden, nam ik de beslissing om nog dieper te graven naar de effectiviteit van de wettelijk voorziene maar moeilijk te concretiseren rechten.

Ik heb een anekdote aangehaald, maar soms kan het verder gaan dan de illegale raadpleging van gegevens. Zo plaatst de Privacycommissie na elke Miss België-verkiezing een speciale markering op het Rijksregisternummer van de net verkozen Miss, aangezien men bij sommigen, en in het bijzonder bij politieagenten een zeker enthousiasme had vastgesteld. Zij gingen onmiddellijk de gegevens van de charmante juffrouw raadplegen – het Rijksregister als Facebook van de administratie!

Enkele jaren geleden had de zeer aantrekkelijke Miss België Turkse wortels; politieagenten hadden niet alleen haar gegevens geraadpleegd, maar ook die van haar ouders, die zich in een onwettige situatie bevonden. Deze informatie werd doorgespeeld aan de pers. Het leidde tot een schandaal, met drie ontslagen bij de politie tot gevolg. De betrokkenen zwoeren met de hand op het hart dat ze de jonge dame geen schade hadden willen berokkenen.

Het gebeurt ook geregeld dat politieagenten een knappe jongedame in haar auto bekijken, het kenteken noteren en terug op hun werkplek inloggen op de DIV, het gsm-nummer van de juffrouw terugvinden en haar lastig vallen op haar gsm.

Het is dus van groot belang te weten wie de gegevens heeft kunnen raadplegen, om de misbruiken aan te klagen maar ook om een zeer concrete controle in te stellen. Deze controle moet de raadpleging voorafgaan, om het enthousiasme van de beambten te temperen. Zo kan men ook de reëel gepleegde misbruiken identificeren.

Ik ben van mening dat het zeer belangrijk is – en ik richt een kordate oproep tot de wetgever – om het hulpmiddel van het Rijksregister uit te breiden tot alle administraties en dus een internetportaalsite ‘mijn administratie.be’ te creëren. De burger zou kunnen inloggen met zijn identiteitskaart en zou in de vorm van kleine venstertjes bijvoorbeeld alle gegevensbanken die informatie over hem bevatten, zien verschijnen. Hij zou erop kunnen klikken, de links met andere administraties zien verschijnen – waar zijn gegevens naartoe werden gestuurd en wie ze heeft geraadpleegd. Ik denk dat men op deze manier tot de werkelijk actieve openbaarheid van de administratie zou kunnen komen, wat de transparantie van de persoonlijke gegevens van de burger betreft. Dit zou het deze laatste mogelijk maken opnieuw meer greep te krijgen op de administratie.

Ik zou willen eindigen met een kleine opmerking over het gebruik van de elektronische identiteitskaart, in het bijzonder wat de commerciële doeleinden betreft. Zoals iedereen weet, bevat deze kaart een chip. Daarop bevinden zich gegevens, onzichtbaar voor het blote oog: de nationaliteit, adelbrieven voor degenen die ze bezitten of andere, meer delicate gegevens zoals de bijzondere kenmerken. Elkeen kan immers op zijn identiteitskaart laten noteren dat hij slechtziend is of het statuut van verlengde minderjarigheid heeft. Wat vandaag vragen oproept, zijn de uitgebreide mogelijkheden van het commerciële gebruik van de kaart.

Zo stelt Media Markt bijvoorbeeld aan zijn klanten voor om het kasticket, dat geldt als een garantiebewijs, op te nemen in hun gegevensbestand. Op die manier kan de klant bij latere problemen met het aangeschafte product onmiddellijk van de garantie genieten in de winkel, zonder het bewijs thuis te moeten opzoeken. Dit systeem wordt voorgesteld aan de klant die bereid is zijn elektronische identiteitskaart door de daartoe voorziene lezer te schuiven en op die manier zijn gegevens te laten opladen in het gegevensbestand van Media Markt.

Een ander geval dat de jongste tijd opgang maakt, is het gebruik van de identiteitskaart als getrouwheidskaart. Hoe gaat dit in zijn werk? U gaat naar een winkel, bij een handelaar die zich heeft aangesloten bij het systeem. Hij vraagt of u een getrouwheidskaart wenst. Is dat het geval, dan dient u uw identiteitskaart door de lezer te schuiven. De gegevens van uw identiteitskaart worden dan gekopieerd op de computer van de handelaar, maar tevens opgenomen in de gegevensbank van de firma die deze tool, *Freedelity* genaamd, heeft ontwikkeld. Heel concreet is deze firma bezig met het kopiëren van het Rijksregister, aangezien zij er prat op gaat over de gegevens van meerdere miljoenen consumenten te beschikken. In haar gegevensbank heeft deze firma dus meerdere miljoenen elektronische identiteitskaarten opgeslagen. Ook worden alle gemaakte aankopen, het ogenblik en de plaats ervan op de lijst gezet. Dit laat toe een zeer gedetailleerd profiel van elke consument op te stellen. De achterliggende doelstelling is overduidelijk de gerichte en directe marketing. Op die manier zult u reclame ontvangen die aan uw profiel is gelinkt. We kunnen er ook voor vrezen dat deze profielen duur worden verkocht aan andere marketingvennootschappen. Dit alles kent immers zijn prijs.

We kunnen al dan niet akkoord gaan met dit systeem. Sommigen zullen zeggen dat het hen niets kan schelen, als het hen al interesseert. Dat neemt niet weg dat men moet instemmen met kennis van zaken. De kwestie is

echter verre van duidelijk. Als u uw identiteitskaart door de lezer schuift, zegt niemand u wat er staat te gebeuren. Mocht dit wel het geval zijn, dan zouden veel klanten argwanend zijn. Op een desbetreffende vraag heeft de Privacycommissie geantwoord dat de identiteitskaart gebruikt mag worden in het kader van de klantgetrouwheid, op voorwaarde dat de toestemming van de klant vrij en geïnformeerd is. Er stelt zich echter een probleem op deze twee punten. Gaat het werkelijk over een vrije toestemming? Normaliter ontvangt u een waardebon van 10 euro als u het voorgestelde systeem aanvaardt. Men kan zich afvragen of dit geen commerciële druk op de klant inhoudt. Overigens is er nergens sprake van *informed consent*, aangezien de klant absoluut niet wordt ingelicht over de eindbestemming van zijn gegevens en het gebruik dat ervan zal worden gemaakt.

Ik richt bijgevolg een krachtige oproep aan de wetgever. Het is dringend zaak een einde te stellen aan deze juridische vaagheid en hierin klaarheid te scheppen. Momenteel verduidelijken de wet noch de koninklijke besluiten inzake de bevolkingsregisters het gebruik van de identiteitskaart voor commerciële doeleinden.

De heer Eddy Caekelberghs *(in het Frans)*. – Dank u mevrouw, voor deze zeer interessante inleiding, vooral voor de zeer concrete voorbeelden die het ons mogelijk maken een reeks zaken te verifiëren en de wetgever alvast aan het werk te zetten.

(Verder in het Nederlands) Het tweede punt van onze werkzaamheden betreft de bescherming van de persoonlijke levenssfeer op het vlak van veiligheid en openbaar leven.

(Verder in het Frans) Ik geef nu het woord aan de heer Guy Rapaille, voorzitter van het Comité I.

Hij zal het hebben over de concrete praktijk van de veiligheid, in elk geval over het verschil tussen het terrein en de theoretische opties.

De bescherming van de persoonlijke levenssfeer op het vlak van veiligheid en openbaar leven

Veiligheid in de praktijk

De heer Guy Rapaille *(in het Frans).* – Vooreerst wens ik de voorzitter van de Senaat, mevrouw Defraigne, te danken omdat ze me uitgenodigd heeft om als voorzitter van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in dit colloquium het woord te nemen. Ik weet dat mevrouw Defraigne altijd belangstelling heeft gehad voor de inlichtingendiensten; ze was immers gedurende enkele jaren lid van de begeleidingscommissie van de Senaat.

Het is niet mogelijk om de onthullingen van Edward Snowden van mei-juni 2013 ter zijde te schuiven als men de bescherming beoogt van gegevens, dus de bescherming van de privacy van burgers tegenover de nieuwe technologieën in het domein van de inlichtingen. De wereld is zich bewust van de kwetsbaarheid van de communicatiesystemen, want een inlichtingendienst, de NSA, heeft in samenwerking met een Britse inlichtingendienst, op grote schaal metadata van telefoonverkeer en metadata van elektronisch verkeer onderschept.

In werkelijkheid hebben onderzoeken aangetoond dat er andere acties zijn, maar ik beperk me tot de massale datacaptatie. De onthullingen veroorzaakten een schokgolf. De Commissie Burgerlijke Vrijheden van het Europees Parlement is in september 2013 een onderzoek gestart. De conclusies zijn aangenomen door het Europees Parlement in maart 2014. De conclusies waren – ik wik mijn woorden – heel kritisch over het massaal onderscheppen van persoonsgegevens. België is niet achtergebleven. De opvolgingscommissie van de Senaat heeft het Comité gevraagd verschillende onderzoeken te voeren naar de onthullingen van Edward Snowden en de positie van de Belgische inlichtingendiensten. De meeste onderzoeken werden in de loop van 2014 afgerond. Onze jaarrapporten zijn op dat punt volledig en kunnen worden geraadpleegd.

In het kader van dit colloquium moet één onderzoek onze aandacht krijgen. Het Comité heeft een deskundige, mevrouw Annemie Schaus, professor aan de rechtsfaculteit van de ULB, een onderzoek laten voeren naar de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van personen,

organisaties, ondernemingen of instanties die in België gevestigd zijn of die enige link hebben met België, te onderscheppen en te gebruiken. Het zal niemand verwonderen dat de conclusies van dit onderzoek eenduidig zijn. De systemen voor het massaal onderscheppen van persoonsgegevens zijn in strijd met artikel 8 van het Europees Verdrag van de Rechten van de Mens en andere Europese en internationale bepalingen. Ze schenden tevens de Belgische soevereiniteit.

Tegelijkertijd woedde er een ander debat in de Verenigde Staten. De grote providers, Facebook en Yahoo, weigerden de NSA hun codeersleutels mee te delen, sleutels die de bescherming van de communicatie van de gebruikers en de media garanderen. Momenteel is bij mijn weten het probleem nog altijd niet opgelost.

De Europese Unie is zich bewust geworden van een fundamenteel verschil tussen de Verenigde Staten en Europa wat de privacy betreft. In de Verenigde Staten zijn volgens een vroegere beslissing van het Hooggerechtshof, die nooit ter discussie werd gesteld, de metagegevens niet in het begrip privacy vervat. Alleen de inhoud van de communicatie of uitwisseling is beschermd. In Europa begint de privacy met de metagegevens. Dat is een fundamenteel verschil.

Deze situatie, beknopt geschetst, voerde de boventoon tot januari 2015. De aanslagen van januari 2015 in Parijs op het hoofdkantoor van *Charlie Hebdo* en op het warenhuis Hyper Cacher, de operatie in Verviers van 15 januari, de aanslagen van 13 november in Parijs en die van 22 maart jongstleden in Brussel brachten hevige beroering teweeg bij de gezagsdragers, de media en de burgers. Momenteel heeft de behoefte aan veiligheid blijkbaar de bovenhand op de bezorgdheid om de bescherming van de privacy.

Ik kom terug op de Belgische situatie, zonder echter de internationale context te negeren. Het is evident dat de inlichtingendiensten een invloed hebben op de privacy van de burgers, maar het doel is precies de veiligheid van diezelfde burgers te verzekeren. Hoe kunnen we die twee waarden, de privacy en de bescherming van gegevens, enerzijds, en de veiligheid, anderzijds, met elkaar verzoenen? Er is de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Deze werd grondig gewijzigd door de wet van 4 februari 2010, die in onze wetgeving indringende methodes heeft ingevoerd voor de privacy, evenwel met garanties.

Men moet in gedachten houden dat de wet van 30 november 1998 uitzonderingen omvat op de algemene regels van de verschillende wetten met betrekking tot de privacy om het de inlichtingendiensten mogelijk te maken hun wettelijke opdrachten te vervullen.

Het is onmogelijk om in enkele minuten een volledige inventaris te geven van de uitzonderingen en garanties. Ik zal me beperken tot het naar voren brengen van de mogelijkheden voor het onderscheppen van metagegevens en telefoontaps. Ik begin met het probleem van het binnendringen in informaticasystemen.

We moesten wachten tot 2010 alvorens de inlichtingendiensten de methodes konden gebruiken die tot dan door de wetgever al te veel beschouwd werden als het indringen in de privacy.

De wet maakt een onderscheid naargelang de graad van binnendringing, de zogenaamde specifieke methodes en de buitengewone methodes. De methodes om metagegevens te onderscheppen zijn specifiek. De methodes voor telefoontap of indringen in informaticasystemen zijn buitengewoon.

Het toezicht door de administratieve commissie, samengesteld uit drie magistraten, en door het Comité, is uiteraard veel strenger en intensiever voor de buitengewone methodes.

Er is controle, want de betrokken persoon moet vanzelfsprekend niet op de hoogte worden gebracht dat hij het voorwerp uitmaakt van een onderzoek.

De dubbele controle is een noodzakelijke garantie voor de naleving van het recht en het Europees Verdrag voor de Rechten van de Mens.

Het Belgische systeem, dat misschien een beetje zwaar en ingewikkeld is voor de inlichtingendiensten, werd bekrachtigd door het Grondwettelijk Hof in een arrest van 22 september 2011, maar het is fundamenteel voor onze bespiegeling te onthouden dat de Belgische wet alleen maar gerichte methodes toelaat, met uitzondering van methodes voor massaverzameling.

Voordat een procedure kan worden toegepast, moeten de inlichtingendiensten over voldoende aanwijzingen beschikken dat een persoon, een

plaats of een organisatie een reële of potentiële bedreiging vormt voor de Staat of de burgers.

Rekening houdend met het bijzondere karakter van de opdrachten van de inlichtingendiensten, kan ik zeggen dat het Belgische systeem voldoende garanties biedt voor de burger. Ik verwijs in dit verband naar het arrest van het Grondwettelijk Hof.

Andere onderzoeken op Europees of internationaal niveau gaan in dezelfde richting, maar ik zou toch niet willen dat men denkt dat ik naïef ben en dat alles opperbest is.

Er is een evolutie. Die is het resultaat van de huidige terrorismedreiging, maar ook van de steeds geavanceerdere en verfijndere technologieën.

Er werden wetten goedgekeurd of ze zullen dat binnenkort worden. Zo werd de wet op de werking van de politie gewijzigd om een nieuwe gegevensbank met betrekking tot de FTF (*Foreign Terrorist Fighters*) en degenen die uit Syrië teruggekeerd zijn naar België, te kunnen oprichten. Ook hier heeft de wetgever controles toegelaten, want het lijkt met het oog op de veiligheid nogal evident dat personen die op deze lijst of gegevensbank voorkomen, hierover niet persoonlijk ingelicht worden. De controle werd toegewezen aan het controleorgaan op de politiële informatie, evenals aan het Vast Comité I.

Momenteel is de nieuwe wet betreffende de PNR, het Europees Passagiersnamen Register, in behandeling en ze moet de komende maanden in werking treden. Ook hier heeft de wetgever in een controle voorzien door het Vast Comité I. Deze wet, door sommigen gewenst en door anderen gevreesd, maakt deel uit van discussies waarover ik nu niet zal uitweiden.

Met de nieuwe bevoegdheden – twee heb ik er al vermeld – behoudt het Vast Comité de positie die het sinds lang inneemt: de noodzaak aan bescherming van onze burgers en het naleven van de rechten die aan dezelfde burgers zijn toegekend, in een democratische samenleving met elkaar verzoenen.

Het probleem van de versleuteling van communicatiesystemen blijft, maar er is onlangs een nieuw element bijgekomen, althans in de media: niet alleen Jan Modaal gebruikt de sociale media of *WhatsApp*, maar

ook terroristen gebruiken deze kanalen om te communiceren en boodschappen te sturen. De politie- en inlichtingendiensten zijn momenteel doof en blind ten opzichte van deze technologie. Anders gezegd, ze hebben niet de instrumenten om de versleuteling te kraken. Hoe kunnen ze hun opdracht om de burgers te beschermen, uitvoeren als ze op dit punt machteloos zijn?

De pers maakte vorige week gewag van het feit dat de NSA en Yahoo een akkoord zouden hebben voor de gedeeltelijke opheffing van de versleuteling. De onthulling van dit akkoord veroorzaakte een storm van protest op het web. Het lijkt me logisch dat er binnen een redelijke termijn hierover grondig wordt nagedacht. Volgens mij en volgens het Comité mag de rode lijn niet worden overschreden: alleen gerichte procedures, met uitsluiting van massaprocedures, mogen worden toegestaan, conform het Europees Verdrag voor de Rechten van de Mens en de jurisprudentie van Straatsburg. Maar er is a priori een probleem: hoe exact bepalen wat een gerichte onderschepping is ten opzichte van een massa onderschepping? Dat is niet zo eenvoudig als het lijkt.

Momenteel is in de Kamercommissie Justitie een wetsontwerp tot wijziging van de wet van 30 november 1998 ingediend om de positie van de inlichtingendiensten te verbeteren. Het Comité I heeft op vraag van de ministers advies uitgebracht. Het blijft trouw aan zijn principes: akkoord met de noodzakelijke evoluties, maar met respect voor de rechten en de vrijheden van een democratische samenleving. Het is nu aan het parlement om zijn rol te spelen.

Tot slot, de Belgische wetgeving heeft volgens mij een evenwicht tot stand gebracht tussen de uitoefening van de opdrachten van de inlichtingendiensten en de bescherming van de privacy. Men kan altijd discussiëren, maar ik denk dat we er globaal kunnen mee instemmen. De huidige uitdagingen, het terrorisme en de technologische vooruitgang zullen hoogstwaarschijnlijk dit evenwicht ontwrichten. Het Vast Comité heeft altijd geprobeerd de efficiëntie van de diensten en het naleven van de wet met elkaar te verzoenen. Het zal altijd opmerkzaam blijven voor deze twee aspecten, in het kader van de nieuwe bepalingen, die al zijn goedgekeurd of heel binnenkort zullen worden goedgekeurd, en die dus weldra in werking zullen treden.

Wij moeten echter bijzonder waakzaam blijven voor de evoluties die voortvloeien uit de technologie zelf en die het werk van de inlichtingendiensten steeds ingewikkelder maken.

De heer Eddy Caekelberghs *(in het Frans).* – Ik dank de heer Rapaille.

Ik heb nog een reeks vragen. Wat met de gegevens in de toekomst op het *dark web*? Wat met systemen zoals Telegram, waarvan de laatste tijd veel sprake is? Wat met de effectieve onafhankelijkheid tussen een reeks grote buitenlandse veiligheids- of inlichtingenagentschappen, en degenen die er toegang toe verlenen, die aan onze wil om wetten te maken ontsnappen? En er zullen nog ontelbare vragen op ons afkomen.

Ik weet niet of onze volgende spreker het woord zal nemen in zijn hoedanigheid van journalist, als lid van de Union des classes moyennes of als spreker van de Solvay Business School. Hij heeft zoveel petten dat hij de problematiek van de bescherming van gegevens vanuit verschillende invalshoeken kan benaderen.

Gegevensbescherming

De heer Amid Faljaoui *(in het Frans).* – Ik dank u voor deze vriendelijke inleiding.

Ik word geacht te spreken over de afschaffing van cashgeld, maar u hoeft niet bang te zijn als u nog bankbiljetten of muntstukken op zak hebt. In het kwartier dat me is toegemeten, zou ik graag het verband leggen tussen de afschaffing van cash geld, de digitale revolutie en de problematiek van gegevens die hier ter sprake kwam.

Op dit ogenblik bevindt de afschaffing van het cashgeld zich nog maar in het stadium van de besprekingen, maar de mensen die het bespreken, zijn wel zeer prominente figuren op dat gebied. Sommigen vinden dat cashgeld moet afgeschaft worden omdat het achterhaald is, een ‘barbaars overblijfsel’ om de uitdrukking van Keynes te gebruiken, en onder degenen die dat voorstaan, zijn er nogal wat die met autoriteit spreken. Eén van hen is de voormalige economisch adviseur van Bill Clinton, Lawrence Summers, die niet kon aanblijven als president van Harvard vanwege zijn vrouwonvriendelijke uitspraken. Verder is er nog Kenneth Rogoff,

één van de belangrijkste economen in Amerika en zelfs op wereldvlak, want hij komt in aanmerking voor de Nobelprijs. Hij was hoofdeconoom van het IMF. Ook directeurs van centrale banken en van klassieke handelsbanken zijn voorstander van de afschaffing van het contant geld.

De argumenten die in dat verband naar voren worden geschoven, zijn met name dat cashgeld een oud concept is, dat de opslag ervan geld kost en dat het veiligheidsproblemen oplevert. U kent het politieke discours dat geleid heeft tot de afschaffing van het bankbiljet van 500 euro door de Europese Centrale Bank. Lawrence Summers was bijvoorbeeld ook voorstander van de afschaffing van het biljet van 100 dollar. Er zijn ook besprekingen aan de gang over de mogelijke afschaffing van het biljet van 1000 Zwitserse frank.

Om alvast de afschaffing van grote coupures te rechtvaardigen, wordt vaak aangevoerd dat ze gebruikt kunnen worden voor fiscale fraude, prostitutie en terrorisme. De vorige spreker heeft hier al een en ander over gezegd. Bedenk dat een bedrag van een miljoen euro, in biljetten van 500 euro, niet meer plaats inneemt dan een melkkarton van 1 liter. Het argument is niet helemaal sluitend, want ook de wegen en de openbare straatverlichting worden door terroristen gebruikt en daarom worden ze nog niet verboden. De Parijse terrorist die een kalasjnikov had gekocht, deed dat via Cetelem, dus via elektronische weg. Sommige belangrijke elementen moeten we voor ogen blijven houden.

Anderen beroepen zich op de digitale revolutie om de afschaffing van het cashgeld te bepleiten, dat als verouderd en overbodig kan worden beschouwd. Ik zie onder de aanwezigen enkele studenten die me doen denken aan het recente initiatief van Tomorrowland: de bezoekers van dat festival kregen thuis een armbandje toegestuurd waarmee ze overal binnen konden en alles konden betalen.

Met dat bandje hadden ze geen cashgeld en zelfs geen bankkaart meer nodig.

Vandaag wordt dit dus besproken en het is nog maar een intentie, maar over enkele jaren zal het misschien normaal zijn, omdat mensen eraan gewend raken niet langer met bankbiljetten te betalen. Ik vind dat contante betalingen mogelijk moeten blijven, zo niet verliezen we de garantie van vertrouwelijkheid en vrijheid.

Waarom dromen bankiers en centrale bankiers van een cashloze maatschappij? Onze landen zijn al jarenlang in crisis en sinds de kredietcrisis van 2007 is de toestand alleen maar verslechterd. De centrale banken hebben reddingsoperaties moeten uitvoeren. Het economisch beleid berust op twee pijlers: het monetair beleid en het begrotingsbeleid. Om de regeringen in moeilijkheden bij te staan, zijn de centrale bankiers tussenbeide gekomen om de rentetarieven op een extreem laag peil te houden. Het doel was om de economie aan te zwengelen, door in te werken op drie traditionele spelers, te beginnen met de gezinnen. Die moesten aangemoedigd worden om te consumeren en geld uit te geven, en dus om niet te sparen, zodat de economische machine weer volop zou draaien. Aan de tweede groep spelers, de ondernemers, werd voorgehouden dat ze zonder uitstel hun investeringsprojecten moesten realiseren. En de derde groep zijn de staten, die in ademnood kwamen vanwege hun grote schuldenberg. Dankzij de lage rente kunnen ze hun schuld verlichten en zichzelf wat marge geven om langetermijnhervormingen door te voeren. Deze strategie heeft evenwel niet de verwachte resultaten opgeleverd: de groei is zwak, de werkloosheidsgraad blijft hoog en de particulieren, die weinig vertrouwen hebben in de toekomst, sparen nog meer, terwijl de rentetarieven zo laag zijn. Bij de ondernemers is de toestand al niet veel beter: de rentetarieven mogen dan wel laag zijn, als het orderboekje niet vol staat, zullen ze niet investeren. De staten hebben weliswaar meer manoeuvreerruimte, maar de keerzijde is ook dat hun hervormingsplannen afgeremd kunnen worden omdat ze meer tijd hebben. Toen François Mitterrand met zijn uitspraak ‘Il faut laisser du temps au temps’ zei dat men voor de dingen de tijd moest nemen, antwoordde Jacques Chirac daarop dat men zo ook wel dreigt zijn tijd te verliezen. De vraag is in welke van die twee scenario’s we vandaag verkeren.

Het lagerentebeleid werkt dus niet of in elk geval niet optimaal.

Economen vragen zich af waar het momenteel op vastloopt. Het loopt vast omdat de rentetarieven niet onder de 0% kunnen zakken, want dan zouden alle spaarders hun geld van de bank halen om het om het even waar onder te brengen, behalve bij een bank.

Maar stel u voor dat er geen contant geld meer is: dan kan er wel een negatieve rente worden toegepast, aangezien de spaarders geen andere keuze hebben dan hun geld op de bank te laten staan. Dat vinden de centrale bankiers dus een prima idee, want in tegenstelling tot wat men zou kunnen denken, zijn ze uiteindelijk niet zeer liberaal, omdat ze denken

dat miljarden beslissingen kunnen gestuurd worden vanuit economische modellen, maar dat wordt nooit bewaarheid. Ook de bankiers houden van dat idee omdat ze beseffen dat iedereen zo wel een bankrekening moet hebben.

Maar ook de mensen achter de digitale revolutie zijn daar opgetogen over. Ze kunnen een boodschap uitsturen die 'cool' en 'jong' oogt – enkel oude knarren zijn anti-GAFA – en tegelijk, door sommige van hun gedragingen, nog hebzuchtiger uit de hoek komen dan sommige bankiers van Wall Street.

Dat zijn dus de gevaren van de afschaffing van het cashgeld, onder het voorwendsel van de digitale revolutie of in de toekomst misschien onder het voorwendsel van de noodzaak om een meer efficiënt economisch beleid te voeren dan het beleid dat we tot nog toe hebben gevoerd. Dat is het soort arglistige betogen die we vandaag te horen krijgen, ook al zijn er stilaan schuchtere pogingen om daar via petities tegen in te gaan, zoals in Zwitserland of in Frankrijk.

Ik wou deze reflectie met u delen. Ik vind ze interessant omdat ik contant geld beschouw als een uitdrukking van onze vrijheid, als een mogelijkheid om vertrouwelijkheid te bewaren. Ik zal niet ontkennen dat er mensen zijn die misbruik maken van contant geld of er de wet mee ontduiken, ik zeg alleen maar dat het een optie moet zijn die mogelijk blijft, zo lang mogelijk nog.

De heer Eddy Caekelberghs *(in het Frans).* – Dank u voor deze zeer interessante schets van een aantal mogelijke hinderpalen voor onze vrijheid in de moderne technologie.

(Verder in het Nederlands) Het woord is nu aan Els Kindt, postdoctoraal onderzoeker aan de KU Leuven en *associate professor* aan de Universiteit van Leiden, over de persoonlijke levenssfeer in het openbaar leven in België.

Persoonlijke levenssfeer en openbaar leven in België

Mevrouw Els Kindt. – Meer dan ooit is een debat wenselijk over de invloed van nieuwe technologieën met privacyimpact op onze samenleving. Die technologieën maken immers identificatie en een zeer gedetailleerd profiel van elke burger mogelijk. Het is derhalve cruciaal dat er een visie en beleid worden ontwikkeld over de mogelijkheden van deze nieuwe technologieën, maar ook over wat wenselijk en toelaatbaar is in onze samenleving.

Ik zal achtereenvolgens aanstippen waarom de plaatsing en het gebruik van nieuwe technologieën in het openbaar leven en op openbare plaatsen mogelijk problematisch zijn; waarom dit de veiligheid niet noodzakelijk ten goede komt; dat er belangrijke neveneffecten zijn; en wat de mogelijke oplossingen zijn.

Enkele jaren geleden werd er gedebatteerd over het gebruik van bewakingscamera's op openbare plaatsen. Dat mondde uit in de Belgische camerawet van 2007, die herhaaldelijk werd uitgebreid, onder meer voor het gebruik van mobiele camera's, inzetbaar op niet-permanente wijze. Op dit ogenblik worden er op Vlaamse gewest- en snelwegen massaal NPR-camera's – camera's met automatische nummerplaatherkenning – geïnstalleerd. Begin 2016 waren dat er al ruim 500. Ik verwijs naar antwoorden op parlementaire vragen van onder anderen de heren Van Rompuy en Van Grieken. Daaraan moeten nog de ANPN-camera's toegevoegd worden, die deels door lokale overheden en deels door het Gewest gefinancierd worden. Steden en gemeenten plaatsen deze camera's op hun invalswegen. Het veralgemeende gebruik van ANPR-camera's – *automatic number plate recognition* - , zoals elke andere technologie-infrastructuur, die *by default* op publieke plaatsen massaal persoonsgegevens, dus informatie over personen inzamelen, moet met de nodige bedachtzaamheid bekeken worden. Aanvankelijk werden de ANPR-camera's vooral geplaatst om overdreven snelheid tegen te gaan – de zogenaamde trajectcontroles – of voor het monitoren van verkeersstromen. Eenmaal de technologie en de infrastructuur geplaatst zijn, bestaat er een groot risico dat die technologie, die infrastructuur, wordt aangewend voor andere doeleinden. Wat zijn de voorwaarden van gebruik van deze informatie, ingezameld door de bestaande ANPR-camera's voor politiële en opsporingsdoeleinden, bijvoorbeeld omtrent toegang tot die gegevens?

Ik geef een ander voorbeeld: een meerderheid van de Belgen heeft en gebruikt een slimme telefoon die voor communicatiedoeleinden en voor plaatsgebonden, gepersonaliseerde diensten vaak permanent in verbinding staat met gsm-masten, wifi-antennes en gps-satellieten. Lokalisatiegegevens van de gebruiker worden zodoende continu geregistreerd en doorgestuurd.

Onze steden zullen in toenemende mate uitgerust worden met slimme infrastructuur, al dan niet verborgen in verkeerslichten of parkeergarages, die massaal locatiegegevens van de slimmetelefoongebruikers op de openbare plaatsen wenst te gebruiken. Door wie zullen deze hoogstpersoonlijke gegevens gebruikt worden en waarvoor? Heel vaak beweert men dat die locatiegegevens anoniem zijn omdat er bijvoorbeeld geen naam wordt vermeld. Onze mobiliteitspatronen zijn echter uniek. In een studie van 2013 is reeds ontegensprekelijk aangetoond dat op basis van slechts vier lokalisatiepunten van een persoon, men in meer dan 95% van de gevallen de identiteit van die persoon kan achterhalen. Dit gebeurt op basis van bijkomende informatie die massaal verspreid wordt, bijvoorbeeld op sociale media.

Anonieme locatiegegevens opslaan en gebruiken kan dus niet. Een zelfde wijziging van gebruik, bijvoorbeeld het gebruik van de locatiegegevens, niet meer voor communicatie en voor diensten, maar voor openbareordedoeleinden of voor politie- en opsporingsdoeleinden kan zich dus ook in deze *smart cities* voordoen.

Er zijn nog talrijke andere voorbeelden van de inzet van nieuwe technologieën in het openbare leven of op publieke plaatsen, bijvoorbeeld de verwachte toename van drones. Ik zou het nog kunnen hebben over nieuwe vormen van openbaar leven, namelijk wat zich afspeelt op publieke websites, blogs en sociale netwerken. Ook voor al die technologie-infrastructuren is er een risico dat het technologieplatform, waarop vaak een groot en onoverzichtelijk aantal actoren actief zijn, de informatie die initieel bedoeld was voor het leggen van contacten of vrije meningsuiting, eveneens wordt gebruikt voor andere doeleinden, zoals het systematisch monitoren van bezoeken, bijvoorbeeld door websiteanalysetools, of cookies, maar ook voor opsporing.

Die voorbeelden tonen aan dat eenmaal een technologie-infrastructuur voor de inzameling van persoonsgegevens voor een bepaald doeleinde aanwezig is, die infrastructuur, omdat ze nu eenmaal voorhanden en

geïnstalleerd is, vaak en nadien wordt gebruikt en ingezet voor totaal andere doeleinden en door totaal andere overheden. Dit is een eerste probleem. In het vakjargon gebruiken we de term *function creep*: wijziging, opschuiving van functies. Dat dergelijke *function creep* op til is voor ANPR-systemen, is duidelijk. In Nederland bijvoorbeeld is een belangrijke discussie aan de gang voor de Hoge Raad, vergelijkbaar met ons Hof van Cassatie, over de bevoegdheid van belastingdiensten voor het verzamelen van kentekens voor de controle van belastingaangiftes. In zijn conclusie stelde de advocaat-generaal dat het systematisch vastleggen van kentekens inderdaad een inbreuk op de privacy van weggebruikers vormt.

Een tweede effect van het gebruik van nieuwe technologie en infrastructuur is dat er talrijke betrokken partijen zijn, zodat niet steeds duidelijk is wie – welke private partij of overheid – over welke gegevens beschikt, zeker indien daaromtrent nog geen betreffende wetgeving is, ook omdat die technologie erg complex en steeds gesofisticeerder is. Ik geef twee voorbeelden in de sfeer van camera's op openbare plaatsen. Momenteel zijn er zes verschillende types ANPR-camera's, elk met andere functies en opdrachten, geplaatst door andere actoren: hoe transparant is dat voor de burger? Ook de gewone bewakingscamera's worden in snel tempo erg geavanceerd. De camera's worden namelijk uitgerust met allerlei softwarefuncties die automatische identificatie, bijvoorbeeld op basis van gezichtsherkenning, mogelijk maken, door vergelijking met databanken met foto's, zelfs in real time. Die fotocollecties worden in grote getale aangemaakt, bijvoorbeeld op sociale media. Dit is helemaal anders dan de 'gewone' bewakingscamera's, waar beelden in publieke ruimtes worden opgenomen en na de feiten voornamelijk nog manueel worden geanalyseerd. Men werkt overigens aan internationale standaarden, zoals de ISO-standaard 301371 voor het gebruik van biometrie en closed-circuit television (CCTV), opdat automatische identificatie meer veralgemeend over verschillende camerasystemen zou kunnen worden gebruikt. Biometrische identificatie, zeg maar automatische identificatie, zal namelijk standaard worden. Het is absoluut essentieel dat de wetgever over de invoering van elke nieuwe technologie met privacyimpact nadenkt, debatteert, begrijpt hoe die technologie werkt en op mogelijke ongewenste gevolgen anticipeert.

Ik kom derhalve bij mijn tweede punt. Kenmerkend aan deze en andere recente nieuwe informatietechnologieën, is dat ze zorgen voor

massale inzameling en voor de mogelijkheid tot samenvoeging van persoonsgegevens.

Locatiegegevens bijvoorbeeld, eenmaal in verband en in context geplaatst, vertellen ontelbaar meer dan een enkel geïsoleerd gegeven. Het punt is dat de infrastructuur zoals ANPR of de infrastructuur in een smart city, die systematisch verplaatsingen registreert, bovendien de samenvoeging van deze persoonsinformatie mogelijk maakt. Locatiegegevens in het algemeen kunnen ontegensprekelijk vele verplaatsingen met een uitgesproken privékarakter kenbaar maken, zoals het bezoek aan een psychiater, een plastisch chirurg, een abortuskliniek.

Ik citeer Sotomayor in een zeer belangrijk arrest van de Verenigde Staten vs. Jones: 'De wetenschap dat informatie macht verstrekt, bestaat reeds lang. De neiging om massaal informatie te garen is evenmin nieuw en is van alle tijden. De schaal waarop dit vandaag echter mogelijk wordt gemaakt door vaak permanente structuren is wel nieuw. Deze technologieën en massale inzameling van persoonsgegevens komen de veiligheid niet noodzakelijk ten goede.'

'L'art de la police est de ne pas voir ce qu'il est inutile qu'elle voie', wist Napoleon I reeds in zijn brief van 24 mei 1800 aan Fouché.

Bij opsporing heeft men met andere woorden de focus op relevante informatie nodig, niet een permanente systematische registratie van persoonsgegevens van alle burgers.

In een democratische staat, in tegenstelling met een politiestaat, is de politie aangewezen en beperkt in de inzameling van persoonsgegevens die noodzakelijk zijn, dus niet alleen nuttig zijn en dit voor de voorkoming van een reëel gevaar of bestrijding van een specifiek misdrijf, tenzij anders wettelijk geregeld.

Het is duidelijk dat wetgevend werk heel belangrijk zal zijn. Elke wet die ingrijpt in het privéleven of het recht op gegevensbescherming moet worden getoetst aan de principes van legitiem of algemeen belang. Maar aangezien het doel de middelen niet heiligt, moet ook aandacht worden besteed aan de evenredigheid van inmenging, geschiktheid voor het nagestreefde rechtmatige doel en de strikte noodzakelijkheid van een inmenging.

Een massale persoonsgegevensinzameling heeft belangrijke effecten op een maatschappij en haar burgers.

Het Hof van Justitie stelde in 2014 in de zaak aangespannen door een Ierse digitale burgerrechtenbeweging tegen de verplichte opslag van telecommunicatiegegevens, weliswaar opgelegd door de richtlijn gegevensbewaring, als volgt in verband met telecomgegevens maar zeker vergelijkbaar met camera- of smart city-gegevens: 'Uit deze gegevens in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die ze uitoefenen, hun sociale relaties en de sociale kringen waarin ze verkeren zodat deze bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden.'

Een dergelijke samenleving, waar er angst bestaat om op te vallen en er geen ruimte of vrijheid meer is voor andere stemmen en gedrag die de samenleving verder kunnen doen evolueren – soms tegen de heersende klasse of beter weten in – is ten dode opgeschreven.

De massale inzameling van ANPR-informatie door ontelbare gewone bewakingscamera's, mobiele politiecamera's en camera's die enkel de gegevens van burgers op de openbare weg en publieke plaatsen op grote schaal en in detail registreren, kunnen leiden tot dergelijke samenlevingen.

Het Europees Hof voor de Rechten van de Mens is duidelijk: bescherming van de persoonlijke levenssfeer kan ook ingeroepen worden op openbare plaatsen. Het onderscheid tussen private en publieke plaatsen is in dit opzicht niet relevant. Een van de belangrijkste aspecten is de nood en de mogelijkheid om ongehinderd relaties met elkaar te kunnen aanknopen, professioneel, maar ook persoonlijk.

In mijn derde punt wil ik de aandacht vestigen op een drietal oplossingen.

Gegevensverwerkingstechnologie is niet bij voorbaat goed of slecht. Het is de inzet van de technologie die moet worden afgewogen. Daarom is het essentieel dat een impactanalyse wordt uitgevoerd voordat nieuwe gegevensverwerkingstechnologie wordt ingezet, met name een analyse van de impact op de fundamentele rechten van privacy en gegevensbescherming. Dat is logisch. Vanaf 25 mei 2018 zal het trouwens verplicht

zijn voor elke verantwoordelijke. Ik verwijs naar artikel 35 van de algemene verordening.

De systematische monitoring op grote schaal van voor het publiek toegankelijke plaatsen wordt dienaangaande expliciet in de verordening genoemd.

Technologie en de verwerking van persoonsgegevens moeten ten dienste staan van de mens en niet andersom. De mens mag niet het object zijn van technologische tests.

Beleidsmakers in steden die experimenteerden met slimme omgevingen zonder rekening te houden met de burger, worden afgestraft. Dat was bijvoorbeeld het geval in Barcelona.

Politici die menen dat technologie, zoals camerabewaking, electoraal voordeel kunnen opleveren omdat ze de bevolking op die manier willen aantonen dat ze actie ondernemen, komen van een kale reis terug.

De impactanalyse zal complex zijn en beleidsmakers zullen zich moeten laten adviseren op een objectief wetenschappelijke manier, zoals in andere landen zoals Nederland, door een wetenschappelijke raad voor het regeringsbeleid of een Rathenau Instituut. Dat is een noodzaak.

Een tweede oplossing is dat men enkel technologie inzet waar privacy en gegevensbescherming verzekerd zijn van bij het ontwerp van de oplossing tot bij de implementatie ervan. Dat is overigens een andere en nieuwe verplichting en verantwoordelijkheid in overeenstemming met artikel 25 van het reglement.

Publieke overheden zullen zelfs in openbare aanbestedingen leveranciers moeten vragen om technologie te leveren die *data protection by design and by default* kunnen garanderen. Dat kan bijvoorbeeld door een beperking van de inzameling van gegevens, pseudonimisering enzovoort.

Ten slotte is het van het allergrootste belang dat we zorg dragen voor het recht om niet te allen tijde op publieke plaatsen herkend en geïdentificeerd te worden. Dat gevaar bestaat wel degelijk, nu bewakingscamera's in toenemende mate zouden worden uitgerust met gelaatsherkenningstechnologie of indien deze technologie voor iedereen vrij beschikbaar en gemakkelijk bruikbaar zou zijn, bijvoorbeeld op sociale netwerken.

Ik kom tot mijn besluit. Technologieën op openbare plaatsen die infrastructuren scheppen om permanent informatie in te zamelen en op te slaan, dragen het risico in zich dat ze vroeg of laat voor andere doeleinden worden aangewend.

In elk geval is het van het allergrootste belang dat we niet in een bewakingsmaatschappij terechtkomen. Daarom moeten we deze technologieën, in het bijzonder degene die op publieke plaatsen worden gebruikt, aan gegevensanalyse onderwerpen en van in het begin de nodige bescherming inbouwen.

De heer Eddy Caekelberghs *(in het Frans).* – We beginnen nu aan het derde deel van ons colloquium over de bescherming van de persoonlijke gegevens en de traceerbaarheid.

Ik geef het woord aan mevrouw Danielle Jacobs, die het zal hebben over het verzamelen en uitwisselen van gegevens.

Bescherming van persoonsgegevens en traceerbaarheid

Het verzamelen en uitwisselen van gegevens

Mevrouw Danielle Jacobs. – BELTUG is een vereniging van de Belgische 'technology leaders', zeg maar IT-verantwoordelijken van middelgrote en grote bedrijven en overheidsinstellingen. De input die ik vandaag ga geven, komt echt uit het bedrijfsleven. Het probleem is soms dat als er op politiek niveau gesproken wordt over de privacy en de bedrijven, men heel vaak denkt aan Google, Facebook, enz. en dat men vergeet dat elke kleine KMO tot de grootste multinational, elke gemeente tot de grootste overheidsinstelling, allemaal dezelfde wetgeving moeten respecteren.

Het is dan ook heel belangrijk dat die wetgeving duidelijk is en dat die ook nageleefd kan worden. Een bijkomende moeilijkheid is bijvoorbeeld het feit dat ze zo internationaal mogelijk is, zoals mijnheer De Hert daarstraks heeft aangegeven.

Het publiek van waar mijn input komt, zijn mensen uit de IT-afdeling van banken, warenhuizen, industrie, enz. Om te weten aan welke onderwerpen we bij BELTUG best werken, vragen wij in juli aan alle leden waarvan zij wakker liggen, en maken wij hun prioriteiten tot de onze. Er is zoveel dat gelinkt is met privacy. Nemen we bijvoorbeeld het *mobile management*. Men wil mensen mobiel laten werken, maar men wil natuurlijk niet dat als iemand het bedrijf verlaat, de privéfoto's van die persoon gedeletet worden zonder dat die persoon dat weet. Men wil veilige mobiele communicatie en men wil de toegang tot bedrijfsinformatie niet zomaar ontsluiten. Aan *mobile management* hangt dus een heel privacyonderdeel vast. Als je kijkt naar clouds: meer en meer bedrijven gaan informatie opslaan bij IT-leveranciers in de 'cloud', dus in datacentra of bij een IT-provider. Ook daar is de privacy belangrijk, want uiteindelijk blijft het bedrijf verantwoordelijk voor de kwaliteit en het niet-lekken van gegevens. Dat is in die relatie dus een belangrijk aspect.

Ik ga niet alle andere elementen aanhalen, maar ik wil maar aantonen dat heel veel van de zaken waar IT-afdelingen nu van wakker liggen, met privacy te maken hebben. Als je kijkt wat de hoogste prioriteit is, zowel bij de overheid als in de privésector, dan is dat de *compliance* met de

Europese verordening. Die IT-mensen moeten immers een aantal nieuwe dingen doen om ervoor te zorgen dat de werking van hun organisatie in overeenstemming is met de regelgeving. De wetgeving telt een tachtigtal pagina's en vele bepalingen zijn niet zo duidelijk dat ze meteen zeer concreet kunnen geïmplementeerd worden binnen het bedrijf. Vandaar dat zij met heel veel vragen zitten.

Wat doen wij dan om te helpen? Ik verwijs hier ook naar de presentatie van de heer Lambotte van Agoria daarnet, omdat wij met Agoria willen samenwerken, maar ook met andere federaties. Wij krijgen veel vragen van mensen die de privacyregelgeving zeer belangrijk vinden en die de gegevens van hun klanten en werknemers goed willen beschermen. Ze riskeren trouwens een boete tot 4% van de wereldwijde omzet als die gegevens op straat liggen. Wij hebben al een aantal workshops gedaan. Je ziet dat mensen met heel veel concrete vragen zitten, waar geen antwoord op is omdat het een juridische tekst is die voor interpretatie vatbaar is en die zeker niet klaar is voor concrete implementatie in de IT-afdelingen.

Wat we doen is al die vragen verzamelen, op papier zetten en bespreken met de privacycommissie. We willen vermijden dat elk bedrijf afzonderlijk opnieuw het warm water moet uitvinden en zelf naar interpretaties op zoek moet gaan, die misschien achteraf niet de juiste blijken te zijn. We verzamelen de vragen met de bedoeling antwoorden te kunnen bieden. Veel blijft nog vaag en ik hoop dat er veel op internationaal vlak, in de working party 29, verder wordt gedefinieerd.

Ik geef een aantal voorbeelden van problemen waarmee bedrijven, van de kleinste KMO tot de grootste multinational, geconfronteerd kunnen worden. Er dient bijvoorbeeld te worden nagegaan welke informatie beschikbaar is en hoe die verwerkt wordt. Een bedrijf, en zeker een groot bedrijf, heeft niet één database. Tal van bedrijven, en steeds meer kleinere bedrijven, bezitten zoveel applicaties en beschikken over zoveel informatie, die al dan niet geïntegreerd is. Men dient dus heel goed te weten over welke informatie men beschikt, niet enkel op de fysieke computer, maar ook in de 'public cloud'. Er zijn heel veel bedrijven waar mensen belangrijke informatie op tools plaatsen zoals Dropbox of iCloud. Ook die gegevens moeten beschermd worden. Als bedrijf zal men zeer zorgvuldig moeten omspringen met deze gegevens, wat eigenlijk een goede zaak is.

Denk hierbij niet enkel aan de databases, maar ook aan ongestructureerde informatie, zoals bepaalde dossiers, Worddocumenten die gegevens over werknemers bevatten. Het is van groot belang met deze inventarisatie te beginnen. Mensen moeten de informatiestromen goed in kaart brengen en deze goed documenteren. Denk ook aan bedrijven die het HR-management uitbesteden aan andere bedrijven zoals SD Worx, bijvoorbeeld. Ook die informatie moet onder controle gebracht worden.

De relatie met de IT-leverancier wordt aan een stresstest onderworpen, want als bedrijf blijf je verantwoordelijk voor de informatie die aan de leverancier wordt bezorgd. Tevens wil je er zeker van zijn dat er met die informatie zorgvuldig wordt omgesprongen. Dat kan gaan om contractuele aspecten, maar we krijgen ook veel vragen in verband met het opstellen van een 'vendors assessment': welke vragen moeten we aan die mensen stellen, hoe kunnen we er gerust in zijn dat de informatie die wij uitbesteden, veilig is. Uiteindelijk blijft het bedrijf immers verantwoordelijk. Denk aan de kleine KMO die de lokale pc-winkel inschakelt om installaties te verrichten en waarbij die laatste in geval van een probleem van op afstand het toestel kan overnemen. Iedereen wordt met die moeilijkheden geconfronteerd.

Daarnet werd het nieuwe begrip 'privacy by design' door mevrouw Kindt al aangehaald. In de Data Protection Regulation staat het als volgt verwoord: 'Future products, applications and services must take privacy requirements into account'. Dit is een mooi principe, maar hoe wordt dat concreet ingevuld? Wat wordt verstaan onder 'future applications'? Zijn dat nieuwe softwareontwikkelingen of belangrijke updates? Hoever moeten we hierin gaan? Dit blijven op dit ogenblik onbeantwoorde vragen, waar we samen antwoorden voor zoeken.

We zijn er al in geslaagd de materie te demystifiëren en bedrijven gerust te stellen door ze uit leggen dat het niet gaat over bepaalde technische maatregelen, maar vooral over het in kaart brengen, bij elk nieuw project, welke informatie er wordt bijgehouden, hoelang en wie daarvoor verantwoordelijk is. Hoe kunnen we dit verwezenlijken? Er is een groot internationaal luik, maar we moeten in België beginnen. Het overleg met de Privacycommissie loopt goed: de door ons gestelde vragen werden met de commissie besproken en ze werden ook schriftelijk beantwoord. De bedoeling is dat we stilaan de zaken die nu uitgeklaard zijn, kunnen meedelen aan de bedrijven, zoals de oplossingen voor de kwesties 'right to be forgotten' of 'privacy by design', bijvoorbeeld.

Stap voor stap willen we de bedrijven zoveel mogelijk concrete informatie geven, zodat ze met hun IT-implementatie aan de slag kunnen. Anderhalf jaar is echt niet lang voor dit soort werk.

De internationale dimensie is zeer belangrijk. Wij hopen dat de verschillende Privacycommissies zoveel mogelijk hun interpretaties op elkaar kunnen afstemmen. Wanneer we in de Belgische economie, die per definitie zeer internationaal is, ook voor de KMO's, iets anders moeten doen dan in Duitsland, in Nederland, dan is dat zeer moeilijk werkbaar. We willen daar heel graag onze schouders onder zetten om de bedrijven van klein tot groot daarin vooruit te helpen. Ik hoop dat dit voor iedereen het geval is.

De heer Eddy Caekelberghs. – Dan bekijken we nu een aantal gevallen waarin persoonsgegevens niet of onvoldoende beschermd worden met de heer Matthias Dobbelaere-Welvaert, oprichter en managing partner van deJuristen/lesJuristes.

Gevallen waarin persoonsgegevens niet of onvoldoende beschermd worden

De heer Matthias Dobbelaere-Welvaert. – Er werd mij gevraagd om kort de impact te bespreken van persoonsgegevens die niet of onvoldoende worden beschermd.

We moeten ons realiseren dat we in België zijn. De privacywet is in België van oudsher heel strikt en formeel geregeld. Het is een moeilijke opdracht om gevallen te vinden waarvoor er geen bescherming is.

Indien ik deze toespraak in de Verenigde Staten of in een andere Europese lidstaat zou moeten geven, weliswaar voor de hervorming in werking treedt, dan zou het verhaal wellicht anders zijn.

Dat betekent niet dat er geen gegevens zijn die de dans van de bescherming zullen ontspringen. Ik vermeld in dat verband de IP-adressen. Een IP-adres is een adres – een serie van nummers – dat verwijst naar een gebruiker of naar een device. Dat kan een printer op wifi zijn, een slimme koelkast, maar ook de persoon zelf die aan de computer zit.

Tegenstanders zeggen dat een IP-adres niet kan worden gelijkgesteld met persoonsgegevens, omdat een dynamisch IP-adres veranderlijk is, het is geen constante. Dat klopt. Toch heeft advocaat-generaal Sánchez-Bordona heel duidelijk gesteld dat IP-adressen wel persoonsgegevens zijn, in zoverre dat bijkomende informatie ook in handen is van derden, zoals internetleveranciers.

Nog veel belangrijker: in de nieuwe verordening staat uitdrukkelijk en is expliciet opgenomen dat online-identificatoren, zoals een IP-adres, vanaf nu gewoon ook officieel worden erkend als persoonsgegevens. De discussie lijkt hiermee dan ook beëindigd, maar men moet nuanceren dat niet elk IP-adres altijd naar een persoon zal verwijzen. Er blijven slimme koelkasten bestaan en er blijven ook bibliotheken bestaan waar men op internet kan surfen en waar het surfverkeer niet onmiddellijk naar een bepaalde persoon leidt.

Ik geef u twee concrete gevallen met betrekking tot de nummerplaat. Er zijn nog steeds juristen in hun oude retoriek die beweren dat de nummerplaat geen beschermd persoonsgegeven is. Volgens hen kunnen nummerplaten immers niet onmiddellijk door een andere persoon worden geïdentificeerd. Noch in de oude privacywetgeving, noch in de nieuwe verordening staat een voorwaarde dat personen direct in staat zouden moeten kunnen zijn om de identiteit van iemand anders te achterhalen. Men moet inderdaad via de DIV of via een andere publieke instantie werken, maar dat belet niet dat het gaat om een beschermd persoonsgegeven.

Daarbij moeten we opmerken dat een heel zorgwekkende evolutie plaatsvindt met dashcamfilmpjes. De meeste mensen herinneren zich de BMW-rijder op de autosnelweg, die met zijn filmpje veel ophef heeft veroorzaakt. Elke dag worden op Twitter en Facebook mensen met nummerplaat online gegooid, soms omdat het gaat om Luxemburgse platen waarbij wordt gedacht aan mogelijke belastingontduiking, soms omdat het om slechte chauffeurs gaat. In elk geval moet het duidelijk zijn dat de nummerplaat te allen tijde een beschermd persoonsgegeven is. Misschien moeten we daar wat meer duiding rond geven.

De discussie over de aansprakelijkheid voor data blijft bestaan. In het geval van IP-adressen is dat zeker het geval als die bijkomende informatie bij een derde zit. Dat is een technisch-juridische kwestie die wellicht door de rechterlijke macht zal moeten worden beslecht.

Als we de problematiek verruimen, dan zien we vooral een zorgwekkende stroom van gegevens vertrekken vanuit de Europese Unie naar lidstaten of landen die niet dezelfde adequate bescherming bieden als in België of in de Europese Unie.

Zo was er maanden geleden heel veel ophef over de gegevensuitwisseling van Europese burgers met de Verenigde Staten. Het Hof van Justitie heeft duidelijk geoordeeld dat dit niet aanvaardbaar is. De Europese wetgever heeft in allerijl moeten remediëren en heeft dat heel 'marketinggewijs' het *Privacy Shield* genoemd, met een heel mooi logo.

Een van die critici is Max Schrems, een van de bekendste privacyvoorvechters, die onder andere ook enkele jaren geleden Facebook een hak heeft gezet. Hij noemde het nieuwe verdrag letterlijk 'tien lagen lippenstift op een varken'. Wie die tekst juridisch onder de loep neemt, kan moeilijk anders dan hem gelijk geven. Volgens die tekst zou massasurveillance door de Verenigde Staten niet meer mogelijk zijn, maar tegelijkertijd staat in de documenten dat bulkdata wel nog verwerkt kunnen worden, voor maar liefst zes verschillende vormen van cybercrime, maar ook voor de algemene bepaling ter bestrijding van terrorisme. We weten dat de instanties belast met privacy in de Verenigde Staten, iets minder scrupules hebben dan die in Europa.

Een tweede punt is dat Belgen nu terecht kunnen bij hun lokale privacycommissie om een klacht in te dienen. Daarbij rijzen twee vragen. Eerst en vooral: zal de privacycommissie – ze is er nog niet – operationeel krachtig genoeg zijn om die vragen te beantwoorden? In het verleden is gebleken dat efficiëntie niet altijd het sterkste punt was, maar daar komen we nog op terug. Ten tweede, zal een Belg hoe dan ook een klacht indienen bij de privacycommissie, zeker als hij niet weet wat er met zijn gegevensstroom gaat gebeuren? Niet elke burger is zo goed op de hoogte van alle privacyregels. De toekomst zal dus moeten uitwijzen hoe dat nieuwe *privacy shield*, of dat nieuwe verdrag, er concreet zal uitzien. Ik vrees dat het werk zal moeten worden overgedaan.

Een andere problematiek is die van het moederbedrijf en de dochter- en zusterbedrijven. Moederbedrijven zijn vaak enorm grote concerns die over een massa aan data beschikken dankzij hun dochters en zusters. Nu rijst de vraag wie die gegevens verwerkt, waar ze worden opgeslagen. Worden ze hoe dan ook gedeeld, en als ze gedeeld worden, wie in dat bedrijf heeft allemaal toegang tot die data? Wat gaan ze ermee doen?

Ik hoop dat de privacycommissie in haar nieuwe verantwoordelijkheid niet alleen aandacht heeft voor de gemiddelde KMO, maar dat ze ook de massaconcerns en de moederbedrijven gaat voorlichten en in zekere zin ook gaat aanpakken. Op dit moment is het zeer ondoorzichtig hoe moederbedrijven omgaan met *intercompany data*.

Ik kom tot een laatste voorbeeld, een van de laatste legale online zwendelpraktijken die nog bestaan, namelijk datamarketing. Een daarvan is het opkopen van databanken. Databanken met particuliere e-mailadressen worden voor grof geld verkocht aan commerciële aanbieders, zodat zij commerciële e-mails kunnen sturen. Dat gebeurt zogezegd met personen die hun toestemming hebben gegeven. De meeste mensen krijgen niet graag commerciële mail in hun inbox. De vraag rijst dan ook waarom die praktijk van het legaal opkopen voor grof geld van databanken anno 2016-2017 nog mogelijk is.

Ik zal nu even dieper ingaan op *data minimisation*. Het is een mooi woord voor het minimale aan data. *Big data* zijn geen nieuw fenomeen. Het is het inzamelen van zoveel mogelijk gegevens binnen een bedrijf om ervoor te zorgen dat er statistieken of commerciële oplossingen worden afgeleid uit die data, met andere woorden, *big data* zijn een bulk van data. Dat levert wellicht heel interessante pistes op voor marketeers, maar aan de andere kant hebben we het *less is more*-principe, de *data minimisation* die niet alleen zou moeten gelden voor commerciële bedrijven, maar misschien ook wel voor overheden, want overheden bezitten ook een enorme hoeveelheid aan data. Het zou wellicht aangewezen zijn om ook daar het *less is more*-principe toe te passen.

Zowel commerciële bedrijven als de overheid hebben voortaan sowieso geen keuze meer, want in de nieuwe verordening staat letterlijk: 'het strikte volstrekte minimum, relevant en noodzakelijk'. Daarvan verschilt onze oude privacywetgeving overigens heel weinig.

Ik wil met u meedenken over hoe we privacy door de gemiddelde ondernemer willen laten percipiëren. De Privacycommissie krijgt in een nieuwe verordening een heel grote macht. Macht gaat samen met verantwoordelijkheid. Het is misschien terecht een punt van kritiek te leveren op de efficiëntie van de Privacycommissie gedurende de jongste jaren. Nemen we als voorbeeld de cookiewetgeving. De Belgische Privacycommissie heeft er twee tot drie jaar over gedaan om een definitief advies te formuleren, opdat online marketeers, online ondernemers en

webontwikkelaars zouden weten wat ze met hun website moesten doen om in orde te zijn. De Nederlandse tegenpool van de Privacycommissie had na drie dagen het bindend advies klaar, in heel begrijpelijke mensentaal. We moeten wellicht ook opletten met de huidige tendens van de Privacycommissie. Facebook aanpakken heeft bij sommige mensen wellicht heel wat mediapunten opgeleverd, maar men moet zich afvragen wat het in de praktijk heeft opgeleverd. Wanneer men nu naar Facebook surft, zal men iets merken van die maatregelen, maar slechts heel weinig.

Ik ben wellicht niet de enige privacyjurist die zich afvraagt of die hoge advocatenkosten, rechtzaakkosten, mankracht en personeel niet beter hadden kunnen worden gebruikt voor de voorlichting van onze Belgische KMO's en bedrijven.

Het belang van de privacy moet correct en duidelijk worden overgebracht naar de ondernemer. Men dient zich bewust te worden van de impact die persoonlijke gegevens hebben op ondernemers, maar ook op de maatschappij en men moet beseffen dat de vergetelheid niet meer bestaat in deze online samenleving. We werken alle dagen voor ondernemers, die weliswaar bezorgd zijn, maar ze moeten de situatie correct kunnen inschatten.

De slotvraag is: willen we de ondernemers verplichtingen opleggen, hen bestraffen, hen belasten met rechtszaken of willen we de ondernemers positieve incentives geven, hen informeren over het belang van privacy, zodat privacy niet alleen in het wetgevend kader komt, maar ook hoog op de prioriteitenlijst van elke organisatie staat. Iedereen die hier aanwezig is, weet dat een rechtsregel pas waarde heeft als degene aan wie hij geadresseerd is, ook inziet waarom die rechtsregel bestaat. Als die voorwaarde vervuld is, komen we tot het resultaat dat men met de nieuwe verordening wil bereiken.

De heer Eddy Caekelberghs *(in het Frans).* – Voordat we overgaan tot het debat, stel ik voor dat we naar de uiteenzetting van de heer Poullet luisteren, de rector van de Universiteit van Namen en professor aan de ULg. Hij heeft twaalf jaar ervaring in de Commissie voor de bescherming van de persoonlijke levenssfeer en kan daar dus zijn bedenkingen over naar voren brengen.

In dat verband verwijs ik naar *Petits entretiens de la vie privée*, een boek met bijdragen van verschillende experts, gepubliceerd door de *Presses universitaires de Namur*. Er zijn hier enkele folders te uwer beschikking.

Het standpunt van de samenleving over het gevoel van traceerbaarheid

De heer Yves Poullet *(in het Frans)*. – Na dit wetenschappelijke gedeelte van het colloquium, leg ik u enkele overwegingen voor over de maatschappelijke aanvaardbaarheid van onze informatiemaatschappij en van de informatietechnologie.

Dat doe ik rond vijf punten:

- ten eerste, de aard: de verwerkte gegevens;
- ten tweede, het hoe: de wijze van gegevensverzameling en opslag;
- ten derde, het wie: de actoren;
- ten vierde, waarom de gegevens worden verzameld en bewerkt;
- ten vijfde, met welke gevolgen, de inzet, het debat en de vraag: is de privacy het geschikte concept om de belangrijke vraag van de maatschappelijke aanvaardbaarheid van de gegevensverwerking te benaderen?

Tot slot zal ik enkele conclusies formuleren.

Over het eerste punt, de aard van de verwerkte gegevens, wil ik enkele overwegingen met u delen.

De eerste overweging is dat er steeds meer triviale gegevens verwerkt worden. Doorgaans zeggen we dat het gevaar zit bij gevoelige gegevens, maar de vraag is nu veel ruimer omdat het in de meeste gevallen om de verwerking van triviale gegevens gaat, zoals de inhoud van uw boodschappenkarretje of uw aanwezigheid op verschillende plaatsen, maar die afzonderlijk of samen genomen uw persoonlijkheid onthullen.

De Franse *Commission nationale d'informatique et des libertés* publiceerde onlangs een Engelse studie die aantoont dat Spotify gegevens registreert. We kunnen aannemen dat die gaan over de muziek die beluisterd werd. Daarnaast worden ook de duur en het afgelegde parcours bij Spotify geregistreerd. Er wordt uiteraard ook geregistreerd waar en

wanneer u die muziek hebt beluisterd en dat is al meer van belang. Als al deze triviale gegevens worden samengelegd, kan de persoonlijkheid van de Spotifyabonnee zeer nauwkeurig worden weergegeven.

Mijn tweede overweging is dan dat de informatieverwerking steeds verder zal gaan op het gebied van de analyse van de persoonlijkheid. Ik denk aan wat *affective computing* wordt genoemd: een poging om op basis van gegevens die door het lichaam worden vrijgegeven een aantal elementen te verwerken die een uitdrukking zijn van de persoonlijkheid. We hebben de gelegenheid gehad een project te volgen van de Europese Commissie waarbij de bewegingen van het gezicht worden geanalyseerd. Gelaatsuitdrukkingen vertalen immers op uiterst precieze wijze de gevoelens van een persoon tijdens een conversatie of een winkelbezoek, bijvoorbeeld. Een applicatie daarvan is hoe die informatie kan gebruikt worden bij een sollicitatiegesprek met die persoon.

Ik wil daar nog een derde overweging aan toevoegen. Die gaat over de metadata, de gegevens die, volgens de Raad van Europa, worden toegevoegd door de persoon die een dienst ter beschikking stelt. Die referentiegegevens kunnen bestaan uit een IP-adres, maar – en dat ligt in de lijn van mijn vorige overweging – steeds vaker gaat het om het identificatienummer van een *Radio-frequency identification*-tag (RFID), de chip die u bij zich draagt.

Zijn die referentiegegevens persoonlijke gegevens? De bedrijven zullen dit ontkennen omdat ze uw naam, adres en andere gebruikelijke identificatiegegevens niet kunnen vinden. Laten we een voorbeeld nemen. In de Verenigde Staten werd er een experiment uitgevoerd door distributiereus WalMart. Een klant wandelt rond in een winkel met een uurwerk dat hem gratis werd aangeboden door WalMart. Dat uurwerk bevat een RFID-tag. Telkens de klant zich in de winkel verplaatst, wordt vrij precies gelokaliseerd waar hij zich bevindt en wordt geregistreerd welke goederen hij in de winkelwagen plaatst, die aan zijn RFID-nummer is gelinkt. Zijn dat persoonlijke gegevens? WalMart beweert van niet, omdat ze op basis van dat nummer de identiteit van die persoon niet kunnen achterhalen. Dat klopt niet, antwoordt de Europese Artikel 29-werkgroep waarin vertegenwoordigers zitten van de verschillende nationale overheden voor privacybescherming: vanaf het moment dat een referentiegegeven een persoon van een andere kan onderscheiden, ook al kent men zijn naam en adres niet, of de andere gebruikelijke identificatiegegevens, gaat het wel degelijk om een persoonlijk gegeven, temeer daar het vanaf dat moment

mogelijk is om met die persoon te interageren, bijvoorbeeld door hem via een klein videoscherm een reclameboodschap te sturen om hem aan te sporen om een of ander product te kopen.

Hoe gaat dit alles in zijn werk? Ik zal kort de manieren overlopen waarop gegevens worden verzameld en opgeslagen.

Alles is veranderd vanaf het moment dat terminals veel kleiner zijn geworden. Het gaat niet enkel meer over mijn pc, mijn telefoon of mijn gsm. Het kan ook mijn bril zijn, of een object dat zich in mijn kledij bevindt, of, wat nog meer verontrustend is, een element dat in mijn lichaam werd ingeplant ('body implant'). Ik kom er straks op terug. Het feit dat terminals nu overal zijn, zorgt ervoor dat er op elk moment kan getraceerd worden.

Het verzamelen van gegevens kan ofwel bij de betrokken persoon gebeuren ofwel bij derden. In het eerste geval kan dat bewust gebeuren – blogs, Facebook – of onbewust. Elk individu kan persoonlijke gegevens op het internet plaatsen, zonder dat hij altijd goed beseft wat de gevolgen zijn. Waarom doet hij dat dan? Gewoon omdat er een onmiddellijk voordeel aan vasthangt. Het is wel mooi om mensen aan te raden geen gebruik meer te maken van Facebook, maar dan moeten ze ook die buitengewone en, in zekere zin, bevrijdende mogelijkheid opgeven om met om het even wie te communiceren. Iedereen wordt zo steeds meer in de verleiding gebracht om persoonlijke gegevens te verstrekken. Dan vraag ik me af of we het hier nog kunnen hebben over een geldig contract of over de instemming van een zogeheten vrij en geïnformeerd persoon, dat de wettige basis is voor de verwerking van privacygegevens, terwijl we weten dat men gemakkelijk geneigd is om deze gegevens te verstrekken. Er is in dit verband nog veel meer aan de hand dan in het geval van Antwerpen. Ik kom daar nog op terug.

Op Tomorrowland werd met een vooraf opgestuurd armbandje de toegang en de automatische aanrekening van consumpties mogelijk gemaakt. Sterker nog was het verhaal van de Baja Beach Club in Barcelona die een RFID-betaalchip liet implanteren in het lichaam van vaste klanten. Meer dan de helft van hen ging daarmee akkoord om gebruik te kunnen maken van het onmiddellijke voordeel om met voorrang binnen te mogen en geen geld meer op zak te moeten hebben, daar alles rechtstreeks werd aangerekend. Dit soort van voordelen brengt mensen ertoe

‘extimiteit’ te aanvaarden en steeds gemakkelijker in te stemmen met het verstrekken van gegevens.

Moeten we het dan niet veeleer hebben over een collectieve reflectie en instemming?

Deze collectieve instemming kan bij voorbeeld worden bereikt op de discussiefora van Facebook waar de gebruikers te kennen geven hoe zij de verwerking van privacygegevens zien. Het lijkt me belangrijk dat men overgaat van een individuele naar een collectieve onderhandeling.

Het onbewust bijhouden van gegevens is nog veel problematischer. Recent vernam ik dat er in onze gsm’s die draaien op Android 4.0 een applicatie zit met de naam ‘Google Now’ die Google in real time in staat stelt te weten waar u zich precies bevindt. Mijn vriend en UCL-rector Vincent Blondel liet mij zien wat hij via zijn inzagerecht heeft kunnen bemachtigen. Het was een immens omvangrijk dossier, waaruit hij voor elke dag kon opmaken hoe hij zich in de universiteit en ook daarbuiten had verplaatst en op welke plaats hij zich op elk moment bevond. Deze wonderbaarlijke dienst wordt verstrekt aan mensen die dat wensen om advies te krijgen over hun reisweg of de locatie van een restaurant, maar het is ook een instrument waarmee al hun verplaatsingen in kaart worden gebracht, zonder dat ze zich daar bewust van zijn.

Er zijn nog andere voorbeelden, zoals onzichtbare hyperlinks die, wanneer u een website bezoekt, u meteen en zonder uw medeweten in verbinding brengen met een andere website die gegevens verzamelt over uw surfgewoonten en over uw bezoek aan de initieel bezochte website.

Gegevens kunnen ook bij derden gehaald worden, bij onze zogenaamde ‘vrienden’. Nog nooit moesten we zo op onze hoede zijn voor onze ‘vrienden’ als vandaag die foto’s posten die verband houden met u en aan de hand waarvan, dankzij systemen van beeldherkenning, kan achterhaald worden wie u bent en waar u zoal geweest bent.

We moeten het ook hebben over de veelbesproken openbare gegevens, die men kan terugvinden door te zoeken met de Google Search Engine of een andere zoekmachine. Gaat het echt om openbare gegevens? Het Hof van Justitie meent van niet omdat bij die persoonlijke gegevens een aantal rechten horen, zoals het vergeetrecht.

Dan kom ik tot mijn derde punt over wie: de nieuwe actoren.

De eerste categorie van actoren zijn de makers van software en de dienstverleners.

Zij ontwikkelen technologisch hoogwaardige systemen waarmee ze gegevens op een vrij geavanceerde manier kunnen verwerken. Veeleer dan de reglementering enkel toe te passen op degenen die gegevens verwerken en de betrokken personen, zou het misschien nuttig zijn om ook eisen te stellen aan de tussenpersonen die zulke technologische systemen aanleveren. Zo zou men hen beperkingen kunnen opleggen in verband met de hoeveelheid gegevens of onzichtbare verwerking verbieden. We weten dat het gebruik van cookies het voor veel bedrijven mogelijk heeft gemaakt om over bepaalde inlichtingen te beschikken.

Als technologie een probleem is, kan het tevens ook de oplossing zijn. Ik ben blij dat in de nieuwe Europese privacywetgeving met de Algemene Verordening Gegevensbescherming (AVG) de nadruk wordt gelegd op een aantal verplichtingen. De 'privacy impact assessment' en 'privacy by design' zijn verplichtingen die we zeker zullen moeten inpassen in onze reflectie.

De tweede categorie actoren zijn de bedrijven die bepaalde diensten monopoliseren, waaronder essentiële diensten, zoals het verlenen van toegang tot informatie of communicatie. Het betreft de vijf grote bedrijven die met de naam GAFAM worden aangeduid: Google, Apple, Facebook, Amazon en Microsoft. Om informatie op te zoeken, denkt men meteen aan Google. Facebook is overal aanwezig als het om communicatie en sociale netwerken gaat, ook al is er daarnaast ook nog Twitter dat echter heel anders werkt. Het feit dat die grote bedrijven, die een oligopolie- of zelfs een monopoliepositie innemen, steeds meer diensten aanbieden, is problematisch. Denk maar aan Google: ze zijn werkelijk overal aanwezig! Ze zitten in onze gsm, we hadden het daarnet al over Google Now op Android. Maar er is ook nog Google Maps, Google News, de Google Search Engine en DoubleClick, een cybermarketingbedrijf dat alle gegevens bijeenbrengt van alle andere Googlediensten en zo een heel precies beeld van uw persoonlijkheid krijgt. Facebook heeft Whatsapp gekocht. Om het hoofd te bieden aan dergelijke dominante posities voor diensten waarvan iedereen het sociale belang erkent, moeten de concurrentieregels beter spelen; hun toepassing zou de gegevensbescherming kunnen bevorderen.

Een vierde punt ter overweging is waarom dit allemaal zo gebeurt. Ik wil graag met u nagaan wat het doel is en hoe de profilering kan bijdragen tot het bereiken van dat doel. Twee doelstellingen lijken mij op dit moment essentieel in de gegevensverwerking, namelijk controle en veiligheid, enerzijds, en economisch gewin, anderzijds.

Wat controle en veiligheid betreft wil ik aantonen dat die doelstelling voortaan zowel door de privésector als door de overheid wordt nagestreefd. Ik kan u daarvan een voorbeeld geven in verband met die controle. Enkele jaren geleden werd ik uitgenodigd om deel te nemen aan een colloquium over veiligheid. Een bedrijf zette naar aanleiding daarvan uiteen hoe het het probleem van de controle van zijn werknemers had aangepakt.

Het had gewoon aan elke werknemer gevraagd een kleine badge te dragen die uiteraard RFID bevatte. De RFID was verbonden met een hele reeks leesinstrumenten, zodat de werkgever op elk moment kon weten waar de persoon zich bevond. Dat was een heel onopvallende controle waarmee op het einde van de dag of van de week de persoon kon worden gewezen op bijvoorbeeld een 'abnormaal' lang toiletbezoek of bezoek aan het restaurant. Ik heb de indruk dat de controle steeds systematischer gebeurt, zowel in het privé- als het openbare leven. We weten allemaal dat op het vlak van de sociale zekerheid, in het bijzonder op het vlak van sociale fraude, en op het vlak van de belastingen, steeds vaker software en big data worden gebruikt.

Het tweede punt is de economische winst. Immers, mensen die internet gebruiken om hun producten te verkopen, kunnen de efficiëntie van hun reclame maximaliseren. Het is interessant te onderzoeken hoe de reclame de voorbije tien jaar is veranderd. Tien jaar geleden was een reclameboodschap in een krant een uitnodiging tot 'nieuwe mogelijkheden', zoals reizen en droombestemmingen waaraan men niet had gedacht; reclame was een manier om op ideeën te komen. Vandaag wordt reclame op een totaal andere manier opgevat: ze stelt een product voor aan iemand die op basis van zijn of haar profiel vermoedelijk in dat product is geïnteresseerd. Vroegere keuzes van de persoon worden aldus bevestigd.

Ik kom tot het tweede punt, de optimalisatie van de doelstellingen en de profilering. Wat moet men daaronder verstaan? Het houdt in dat personen worden ingedeeld in categorieën die steeds fijner worden bepaald om een vooraf gedefinieerd resultaat te verkrijgen, bijvoorbeeld een resultaat

van een controle of van marketing. Dat gebeurt door middel van gegevensverzameling en de combinatie van gegevens op een volledig toevallige wijze op basis van een zelflerend systeem.

Waartoe dient profilering? Ik neem het voorbeeld van Amazon, dat gebruikmaakt van profilering om te bepalen of een persoon eventueel meer kan betalen voor een product waarvoor hij werd geprofileerd dan een andere persoon die niet voor dat product werd geprofileerd. Het gaat er in andere woorden om de prijzen te differentiëren naargelang het profiel en de aard van de veronderstelde vraag van de persoon. Met dat systeem kunnen trouwens ook fraudeurs worden opgespoord. Zo zouden bij de belastingdiensten profielen worden gedefinieerd waarvoor het risico op fiscale fraude het hoogst is. Die profielen hebben a priori niets te maken met het profiel dat men redelijkerwijze van een fraudeur kan verwachten.

Men vormt zich bijvoorbeeld een beeld van een persoon volgens de kleur van zijn of haar auto, van de plaats waar hij zich bevindt of van het soort verplaatsingen. Kortom, op basis van toeval kan men zeggen dat er 80% kans is dat die persoon een fraudeur is. Men zou dan uiteraard het onderzoek naar die persoon kunnen intensiveren. Die methode kan ook nuttig zijn voor publiciteitsdoeleinden.

Welke problemen kan profilering meebrengen? Eerst en vooral is het uiterst moeilijk, aangezien profilering gebaseerd is op wat men een echte statistiek kan noemen, er iets tegen in te brengen. Als 80% van de mensen statistisch als fraudeurs beschouwd worden, is het niet gemakkelijk aan te tonen dat men tot de overige 20% behoort. Met andere woorden, met die simpele statistische waarheid vindt geleidelijk aan een omkering van de bewijslast plaats.

Dan is er nog het probleem van de voorspelbaarheid. Ik geef een uitspraak van de CEO van Google: ‘Het zal in de toekomst steeds moeilijker worden ervoor te zorgen dat een persoon iets anders consumeert dan datgene op basis waarvan men hem heeft geprofileerd’. Dat vormt natuurlijk een probleem aangezien men niet gewoon op basis van het verleden werkt. Profilering maakt het mogelijk te werken op basis van de toekomst en te anticiperen op de acties van een persoon.

Als besluit zal ik het hebben over de laatste vraag: het debat en de uitdagingen. Is privacy een doeltreffend concept om het debat en de uitdagingen aan te gaan? De vraag wordt soms provocerend gesteld: ‘Privacy,

een geschiedenis voor oude zakken?' (J.P. Manach) of 'Privacy, een achterhaald concept' (M. Zuckerberg). Toch denk ik nog altijd dat privacy het essentiële concept is om de vragen van de informatiesamenleving te beantwoorden, op voorwaarde dat men dat concept niet reduceert tot wat men er gewoonlijk van maakt, namelijk een negatief beeld van privacy. Dat negatieve beeld, het *right to be let alone*, is het feit dat men vooral moet vermijden dat de anderen iets weten. We leven in een informatiemaatschappij waarin de mens moet kunnen communiceren en informatie uitwisselen en niet gewoon een defensieve houding aanneemt. Het negatieve aspect is zeer belangrijk. De mens moet zich steeds meer kunnen losmaken, anoniem kunnen handelen en, uiteraard, zich uit het zicht van de anderen plaatsen. De uitspraak van het Duitse grondwettelijk hof bevalt me: volgens het hof moet een computer gezien worden als een huis: het moet worden beschermd en men mag er niet gemakkelijk binnen raken: dit houdt de veroordeling in van spyware en andere indringers op onze schermen.

Privacy houdt ook een positief aspect in. Het is niet alleen de bescherming van het individu tegen de inkijk van de ander, maar het biedt hem ook de mogelijkheid zich zowel sociaal als qua persoonlijkheid te ontplooien. Privacy, dat zijn een aantal voorwaarden die de mensen de mogelijkheid moeten bieden zich vrij te ontwikkelen en hun waardigheid te laten respecteren. Zoals mijn vriend Giovanni Buttarelli ben ik ervan overtuigd dat het tijd is dat men privacy niet als een vrijheid naast de andere vrijheden ziet, maar als een voorwaarde voor de andere vrijheden. Dat is het geval met de vrijheid van meningsuiting en met de vrijheid om zich te bewegen Als ik weet dat ik bespioneerd word zonder goed te weten waarom, zoals in *Het proces* van Kafka, zal ik me uiteraard niet uiten zoals ik wil. Het is ook een probleem van zich vrij te kunnen bewegen. Als ik op elk moment word gecontroleerd, hoe kan ik me dan vrij voelen om te gaan en staan waar ik wil? Zoals blijkt uit de verklaring van de CEO van Google over profiling en het voorspellen van gedrag is het ook een probleem van consumptie en van keuzevrijheid van de consument.

De privacyvraag verwijst ook naar de sociale rechtvaardigheid. Het spreekt vanzelf dat de diensten van de informatiemaatschappij ervoor zullen zorgen dat een aantal e-diensten en meer bepaald op het vlak van e-health (zoals stresscontrole op afstand of geheugentraining), betaald zullen moeten worden door wie hiervan gebruik wil maken. Hoe staat het dan met de toegang van andere mensen tot die diensten en tot die gezondheidsdiensten in het bijzonder?

Het is tot slot ook een probleem van waardigheid in de betekenis van Kant: de mens mag nooit als een middel worden beschouwd, maar hij is een doel op zichzelf. Ik denk hierbij aan de toepassingen in de reclame, die ik hier niet hoef te herhalen.

Ik rond af met enkele bedenkingen voor u, wetgevers. Drie bedenkingen met als eerste: u moet aandacht besteden aan de technologie en aan de bedenkingen over de maatschappelijke impact van de technologie. We moeten voortaan zeker aandacht hebben voor de evolutie. We kregen het uitstekende voorbeeld van de afschaffing van cashgeld. Cashbetalingen afschaffen is uiteraard een manier om elke transactie transparant te maken, wat problemen kan opleveren voor een aantal essentiële vrijheden. Ik zal het hier niet hebben over biogenomica.

Tweede bedenking: het belang van de opvoeding. Men moet ervoor blijven zorgen dat de bevolking en meer bepaald jongeren zich bewust worden van de gevaren van het internet, maar ook van de kansen die het internet voor de vrijheden biedt.

Ten slotte bent u als openbare overheid verantwoordelijk voor het e-government dat wordt gevoerd: wees waakzaam dat het evenredigheidsprincipe wordt nageleefd. Vergeet niet dat de vrijheden op de eerste plaats komen en dat veiligheid slechts een uitzondering is die behoorlijk moet worden gemotiveerd en evenredig moet zijn in het geval de vrijheden worden ingeperkt. Aarzel niet om er zoals vandaag een openbaar debat van te maken met alle deelnemers uit de samenleving en dit in naam van de verdediging van onze vrijheden.

Leve de privacy. De technologie moet ten dienste staan van de mens, van zijn vrijheden en zijn waardigheid.

Politiek debat

Debat in aanwezigheid van de heer Philippe De Backer, staatssecretaris voor Bestrijding van de sociale fraude, Privacy en Noordzee, en van de vertegenwoordigers van de verschillende partijen

De heer Eddy Caekelberghs. – Ik nodig de heer staatssecretaris en de vertegenwoordigers van de partijen uit om vooraan plaats te nemen voor het debat.

(Verder in het Frans) Dames en heren afgevaardigden van de fracties, mag ik u verzoeken aan tafel te komen zitten en uw respectieve standpunten toe te lichten?

Zijn aanwezig: de heer Benoit Hellings voor Ecolo, de heer Andries Gryffroy voor de N-VA, de heer Jacques Brotchi voor de MR, staatssecretaris Philippe De Backer, de heer Philippe Mahoux voor de PS, de heer Bertin Mampaka voor de cdH en mevrouw Katia Segers voor de sp.a.

(Verder in het Nederlands) Mijnheer de staatssecretaris, kan u in enkele woorden de mening van de regering weergeven? Mogen we nu onmiddellijk of binnen enkele jaren wetgevend werk verwachten?

De heer Philippe De Backer. – Vooreerst ligt er reeds heel wat wetgevend werk op ons te wachten. Zo is er de Europese regelgeving die voor mei 2018 in Belgische wetgeving moet worden omgezet. Die regelgeving legt een heel duidelijk kader vast waarin de privacy en data protection voor onze burgers en onze bedrijven moeten worden geregeld. We moeten er in de eerste plaats voor zorgen dat deze wetgeving op een goede en duidelijke manier tijdig wordt omgezet, zodat onze bedrijven en instellingen op de juiste manier kunnen handelen en de privacy van onze medeburgers afdoende wordt beschermd.

Ten tweede moet er in het kader van die wetgeving de komende maanden gewerkt worden aan de Privacycommissie zelf, die onder de nieuwe Europese Data Protection Regulation toch een andere rol krijgt. De commissie dient te worden versterkt en moet een nieuwe inhoud krijgen, niet enkel op juridisch vlak, ze moet ook in staat zijn administratieve boetes op te leggen, maar ook op het vlak van expertise. Het colloquium en de verschillende sprekers hebben vandaag uitgebreid aangetoond dat

de Privacycommissie nood heeft aan meer technische en technologische competenties, om haar rol van behoeder van de privacy op een goede manier te kunnen spelen.

Ten derde is er nood aan bewustwording en bewustmaking bij bedrijven, burgers en consumenten, zodat mensen zelf ook keuzes kunnen maken. Dit valt niet te vatten in wetgevend werk. Ik wil niet de staatssecretaris zijn die alles beslist voor iedereen. Het is de bedoeling dat mensen voor het omgaan met hun privacy en hun eigen gegevens weloverwogen keuzes kunnen maken.

De heer Eddy Caekelberghs. – U zei daarnet dat wij onze bedrijven, kleine of grote, de geschikte gegevens moeten geven om een goede *efficiency* te bereiken. Wat met *e-government*? De heer Poullet en ook anderen hebben daarover gesproken. Is er een *welfare state* voor dat *e-government* of niet?

De heer Philippe De Backer. – Absoluut en ik sprak over bedrijven, maar ook over instellingen. Daar horen publieke instellingen absoluut bij. Voor mij is het zeer duidelijk, ook bij onze eigen overheden – wij hebben er heel veel – moet elk niveau zijn verantwoordelijkheid nemen en ervoor zorgen dat de principes van de Europese wetgeving ook bij de publieke instellingen ingang vinden. Wij hebben zeer veel gegevens over onze burgers. Soms is dat noodzakelijk, maar wij moeten ook vertrouwen hebben en stellen in een systeem zodat wij onze burgers kunnen uitleggen wat wij met die gegevens doen, waar ze bewaard worden en hoe wij daarmee omgaan, volgens de duidelijke principes van de GDPR.

De heer Eddy Caekelberghs. – Daar kom ik straks nog op terug. Misschien kan ieder van u nu kort een *statement* maken over het standpunt van uw fractie.

De heer Benoit Hellings (Ecolo) *(in het Frans)*. – Dit is een cruciaal punt in de geschiedenis van de privacy in België. De heer Rapaille herinnerde eraan dat we heel lang, onder bescherming van het Comité I, een sterk afgebakend systeem van gericht toezicht hadden.

De politie- en inlichtingendiensten kunnen het fundamentele recht op privacy van een burger die voor problemen zorgt aan de kant schuiven. Vandaag staan 450 à 500 personen, met reden, op een lijst van geradicaliseerde personen die regelmatig moeten gecontroleerd worden.

Enkele jaren geleden heeft de Senaat hierover vaak gedebatteerd. Er werd stelselmatig op gewezen dat België het systeem van gerichte controles wilde behouden. Het PNR-project van de regering, waarover de voorzitster van de Senaat zojuist sprak, zal op 21 oktober in de Kamer worden besproken. Daarmee wordt de koers gewijzigd. Het gaat dan niet meer om het in het oog houden van 450 à 500 personen, plus een hele reeks anderen die om evidente veiligheidsredenen moeten worden bewaakt. In het kader van de PNR zullen, enkel voor vliegtuigpassagiers, van dertig miljoen personen negentien essentiële gegevens worden verzameld, terwijl met vier gegevens de identiteit van personen gemakkelijk kan worden bepaald. Hier gaat het niet alleen om privacy, maar ook om efficiëntie.

Ik denk dat onze politiediensten zullen overstelpt worden met gegevens. De recente aanslagen hebben echter aangetoond dat het erop aankomt relevante gegevens te hebben van de persoon die een probleem kan vormen.

Dat is wellicht een tweede onderwerp waarover de Senaat een ander colloquium kan organiseren. Ik wil het hebben over het iPoliceproject van minister van Binnenlandse Zaken Jambon. Het doel hiervan is belangrijke gegevensbanken zoals de Algemene Nationale Gegevensbank (ANG), de gegevensbank van de politie, die daarstraks ter sprake kwam, de PNR, de Kruispuntbank van de sociale zekerheid en de gegevensbank van de Dienst Vreemdelingenzaken met elkaar in verbinding te stellen. Dit is een totaal ander kader. We gaan van gerichte controle, nodig en nuttig, onder leiding van het Comité I, over naar een veralgemeende controle, met alle gevolgen die hier tijdens deze reflectienamiddag werden besproken.

De heer Eddy Caekelberghs. – Dat is een aangelegenheid die minister Jambon aanbelangt, dus geef ik het woord aan de vertegenwoordiger van zijn fractie, de heer Andries Gryffroy.

De heer Andries Gryffroy (N-VA). – Voor de N-VA is het duidelijk. De overheid mag geen *Big Brother* worden. Soms moet men de privacy wel ter discussie kunnen stellen op een heel beperkt aantal domeinen. Het moet gaan over zeer uitzonderlijke omstandigheden, onder de controle van het parlement, bijvoorbeeld veiligheid. Ook in dit debat moeten we daarover breder durven te denken dan wat men nu doet. Men mag niet in hokjes denken.

Een voorbeeld is de discussie rond het vrijgeven van passagierslijsten. Die discussie zit op Europees niveau nog altijd voor een stuk vast. Het is onbegrijpelijk dat men de passagierslijsten voor vluchten in en buiten Europa niet kan matchen.

Anderzijds mogen we het kind niet met het badwater weggooien en gaan wij veeleer voor een eigendomsrecht dan voor een absoluut recht. Met een eigendomsrecht bedoel ik dat ik zelf wil beslissen wat ik doe met mijn privégegevens. Als ik beslis om bij mij thuis een digitale thermostaat te laten plaatsen en in bepaalde omstandigheden bereid ben informatie aan de provider te verstrekken, die daarmee gaat ingrijpen op bepaalde processen in mijn woning, moet ik me ervan bewust zijn dat er innovatieve technologieën worden gebruikt. We mogen die technologieën niet afremmen, maar het is een keuze die ik vrijwillig moet kunnen maken.

Daarom pleit ik met mijn fractie voor een eigendomsrecht in plaats van een absoluut recht.

De heer Eddy Caekelberghs. – Is het matchen van *big data*, waarover de heer Hellings het had, in het project van minister Jambon, niet gevaarlijk? Kan men verscheidene databanken laten matchen zonder effectieve controle door wie dan ook?

De heer Andries Gryffroy (N-VA). – Er moet uiteraard controle zijn.

De heer Eddy Caekelberghs. – Door wie?

De heer Andries Gryffroy (N-VA). – Het parlement moet daar in laatste instantie het controlerende orgaan zijn. Dat is een cruciale factor.

Het klopt dat er controle, duidelijke regels en duidelijke afspraken moeten zijn. Een verbod om te matchen is geen goede oplossing. De gewone man kan moeilijk begrijpen waarom passagierslijsten niet mogen worden gematcht. Hij vraagt zich immers af hoe zijn veiligheid kan worden verzekerd.

Hoeveel van de hier aanwezigen hebben op hun Facebookpagina gezet dat ze hier aanwezig zijn? Dat is een vrijwillige keuze, maar waarom is het dan een probleem dat de passagierslijsten zouden worden gematcht?

De heer Eddy Caekelberghs. – Het woord is aan mevrouw Segers voor de sp.a.

Mevrouw Katia Segers (sp.a). – In de eerste plaats bedank ik de voorzitster voor dit initiatief. De Senaat is de uitgelezen plek om met zijn allen – academici en politici – na te denken over een van de grootste uitdagingen voor onze toekomst, de dataevolutie en onze privacy. Ik spreek in dat verband ook graag over zelfbeschikking.

Op dit ogenblik zijn onze data in handen van enkele grote spelers die over een massa informatie beschikken. Zij weten alles over ons, maar wij weten niets over hen. Wij weten evenmin wat zij met onze gegevens doen. Zelfbeschikking is dus een fundamentele kwestie. Het verheugt mij de staatssecretaris te horen zeggen dat het finaal gaat over empowerment van de gebruiker – al heeft hij dat woord niet gebruikt –, die in een privacybeleid zeker centraal moet staan.

Met die empowerment of mediawijsheid zal de staatssecretaris samen met de Gemeenschappen rekening moeten houden bij het beleid dat op dat vlak wordt uitgestippeld. Minister Gatz heeft reeds initiatieven genomen, onder meer met betrekking tot het invoeren van digitale competenties, mediawijsheid, digitale geletterdheid in het lager onderwijs of in kleuterscholen. Het gaat natuurlijk allang niet meer over onze privacy online op sociale netwerken. Nu worden wij geconfronteerd met het 'Internet of Things', maar ook het 'Internet of Living Things', bijvoorbeeld de *Quantified Self Movement*: hoe gaan wij om met gegevens die wij verzamelen. Er is in die context verwezen naar implantaten. Er is een massa data die gegenereerd wordt en de uitdaging wordt hoe die informatie maximaal kan worden benut en tegelijkertijd de privacy kan worden beschermd. Vandaag is het machtsevenwicht eigenlijk verstoord. We moeten dat evenwicht herstellen. Wij zien dat als een gedeelde verantwoordelijkheid. Daarom ben ik blij dat enkele sprekers gewezen hebben op de rol en verantwoordelijkheid van de bedrijven zelf. Dat is een teer punt: zij nemen vandaag veel te weinig verantwoordelijkheid. Het is jammer dat Google hier vandaag niet aanwezig is. Dat is wellicht niet toevallig. Het weigert die discussie aan te gaan.

De overheid moet terughoudendheid aan de dag leggen in alle aspecten. Ze moet de 'dataobesitas' indammen in plaats van alles per se te willen verzamelen. Maar wat gebeurt er uiteindelijk met die verzamelde data? Ik ben het ermee eens dat projecten zoals e-politie moeten worden

uitgebouwd, maar er rijzen ethische vragen wanneer het gaat om *predictive policy*. In Eindhoven werden slimme lantaarnpalen geïnstalleerd die gezichten kunnen herkennen. Ze zouden op basis van de gelaatsuitdrukking van mensen en van het aantal mensen dat zich op straat bevindt, kunnen voorspellen dat er een risico bestaat op het uitbarsten van een rel. Dan komt men wel heel dicht in de buurt van *ethnic profiling*. Die lantaarnpalen dimmen het licht, veranderen van kleur, maar kunnen ook de politie waarschuwen, die dan kan ingrijpen voordat een incident heeft plaatsgevonden. Dat zijn scheidingslijnen waar belangrijke ethische vragen rijzen.

De heer Bertin Mampaka Mankamba (cdH) *(in het Frans)*. – Ik dank de voorzitster voor de organisatie van dit debat, dat verrijkend maar ook noodzakelijk is.

Elke partij heeft uiteraard haar standpunt over het onderwerp. Bij cdH zijn we van mening dat het recht op privacy deel uitmaakt van de fundamentele rechten die moeten worden beschermd. De eerbiediging van de privacy wordt dan misschien geen virtuele realiteit, maar in ieder geval een relatieve realiteit. Toen mevrouw De Block minister van Sociale Zaken was, heb ik haar, in deze vergaderzaal, gevraagd of sociaal assistenten het recht hadden gegevens van leefloontrekkers op Facebook na te gaan om de nood aan een leefloon vast te stellen. Ze antwoordde me dat de mensen vrij zijn om hun privéleven al dan niet op Facebook te delen.

Bij cdH denken we aan de mensen die niet anders kunnen dan te consumeren wat ze krijgen voorgeschoteld. Om toegang te krijgen tot bepaalde diensten, moet men een reeks vragen beantwoorden en zelfs heel wat informatie toevertrouwen. Heeft iedereen de mogelijkheid om in alle vrijheid dat soort overeenkomsten te sluiten of niet? Gelet op de problemen van een te zware schuldenlast, van de strijd tegen cybercriminaliteit, tegen kinderpornografie, enzovoort, zijn we van mening dat we voor waarschuwingen moeten zorgen.

Door de aanslagen die we hebben meegemaakt, protesteren de meeste burgers niet meer tegen de installatie van camera's in de straten of het aanbrengen van een chip op kaarten. Ze kunnen die praktijken trouwens niet meer weigeren. Weigeren dat soort informatie te geven, betekent soms dat men zich aan de rand van de maatschappij stelt, wat een vorm van uitsluiting is. We moeten wetten maken om te vermijden dat bejaarden of mensen die de middelen niet hebben om de moderne evolutie te

volgen, worden uitgesloten. In alle assemblees moet daartoe veel werk worden verricht, maar de waarschuwingen zijn onmisbaar. Sommige categorieën mensen moeten worden beschermd door wetten die meer zijn dan de loutere omzetting van Europese richtlijnen. We moeten verder gaan en de juiste middenweg vinden.

De heer Eddy Caekelberghs *(in het Frans).* – De uiteenzettingen doen me denken aan een boek met als titel *La pureté dangereuse*, de gevaarlijke zuiverheid. Men zou in dit geval kunnen spreken over de gevaarlijke transparantie. We bevinden ons op een kantelmoment. Hoe kunnen we op een verstandige manier het begrip transparantie, dat in zekere zin het maken van een inbreuk op iets inhoudt, in een wet gieten?

De heer Jacques Brotchi (MR) *(in het Frans).* – Ik heb veel geleerd vandaag en ik dank de voorzitster voor de organisatie van deze buitengewone zitting. Helaas heb ik niet alleen interessante dingen vernomen, maar werd ik soms ook ongerust. De hoeveelheid aan gegevens is groot en we moeten ze organiseren.

Als arts verdedig ik het medisch geheim. Ik hecht daar veel belang aan. Het is een belangrijk aspect, dat verband houdt met de kwestie van transparantie waarover u hebt gesproken.

Het medisch geheim gaat over de dialoog met onze arts en kan niet worden gedeeld, behalve als we zelf beslissen sommige gegevens mee te delen. Dat punt werd niet aangeraakt, maar het is van belang dat we in de toekomst, op een uiterst vertrouwelijke en beschermde wijze, een aantal gegevens op onze identiteitskaart of een andere drager kunnen zetten. Immers, als we onwel worden op straat en we met een ziekenwagen naar een ziekenhuis worden gebracht waar we geen vaste patiënt zijn, moet men weten of we antibloedstollingsmedicijnen nemen, of we aan diabetes of epilepsie lijden en of we een pacemaker hebben waardoor geen MRI-scan mag worden gemaakt.

De heer Eddy Caekelberghs *(in het Frans).* – Vanuit die overweging zouden diezelfde gegevens in sommige gevallen een hinderpaal kunnen vormen om een patiënt toegang te verlenen tot een bepaalde gespecialiseerde dienst, als men het gedrag van die patiënt als onvoorzichtig beoordeelt, op basis van de medische gegevens waartoe u de toegang hebt verleend.

De heer Jacques Brotchi (MR) *(in het Frans).* – Helemaal niet. Het concept waarover ik het heb, wint terrein, namelijk met de telegeneeskunde, de hightechdimensie in de geneeskunde, ten dienste van de gezondheid. Nogmaals, we moeten vrij zijn te beslissen wat we willen delen en wat we weigeren te delen.

Dat betekent niet dat we paranoïde moeten worden. Daarnet gaf een spreekster het voorbeeld van een camera die in staat is te onthullen dat een vrouw naar het ziekenhuis is gegaan voor een abortus. Men kan ook naar het ziekenhuis gaan om een vriend te bezoeken.

De voorbije drie tot vier jaar is de maatschappij erg veranderd. Sinds de aanslagen zijn de denkbeelden anders. We moeten ook maatregelen nemen om de maatschappij te beschermen. Ik ben blij dat er camera's zijn. Denk aan wat die camera's mogelijk hebben gemaakt, in het bijzonder na de aanslagen van Zaventem.

Natuurlijk moeten we ons de vraag stellen over de grens die niet mag worden overschreden.

De heer Eddy Caekelberghs *(in het Frans).* – Maar de camera's hebben niets verhinderd, zoals de heer Benoit Hellings zei.

De heer Jacques Brotchi (MR) *(in het Frans).* – De context is gewijzigd en we moeten enerzijds de vrijheid van eenieder beschermen en kijken tot waar we transparantie toelaten en anderzijds veiligheidsinstrumenten invoeren.

Zo vind ik het opmerkelijk dat de regering beslist heeft om de anonimiteit van prepaidkaarten af te schaffen, aangezien ze illegale praktijken mogelijk maakten, zonder gevaar om betrapt te worden. Dat is des te meer onmisbaar in de huidige omstandigheden.

Tot slot, wat de gecodeerde gegevens betreft, heb ik geleerd dat het moeilijk was een aantal boodschappen te ontcijferen. We weten nochtans dat de terroristische netwerken aan de hand van codes communiceren die de meest geavanceerde diensten niet kunnen kraken. Dat verontrust me ten zeerste.

De heer Eddy Caekelberghs *(in het Frans).* – De heer Mahoux heeft het woord. Toevallig volgen twee parlementsleden die arts zijn elkaar op.

Als men mij op een dag een geneeskundige behandeling weigert omdat de gegevens die ik vrijwillig op de chip van mijn identiteitskaart zou hebben laten plaatsen om mijn gezondheid te beschermen, het mogelijk maken om mijn sigarettengebruik op te sporen, zou dat toch een ernstig probleem vormen. Mevrouw Thatcher was overigens voorstander van die praktijk.

De heer Philippe Mahoux (PS) *(in het Frans).* – Dat is waar, maar u spreekt over een benadering van de gezondheid en de geneeskunde die gebaseerd is op gedrag. Ik weiger mee te gaan in die denkwijze. Ze is ethisch ontoelaatbaar, ook al kan men op basis van objectieve elementen nagaan of een patiënt een bepaalde therapie kan krijgen. Ik wil dat bijzondere kader overstijgen.

De voorzitster was zo tactvol het werk dat rond informatica en vrijheid is verricht, te vermelden. Het is vrij recent. Ik ken het onderwerp goed omdat ik het samen met anderen vroeger al heb onderzocht. De vragen die worden gesteld, zijn nog altijd precies dezelfde. Er is evenwel een verschil. Ik heb een spreker kritiek horen geven op de Commissie voor de bescherming van de persoonlijke levenssfeer, maar de Commissie was nuttig voor het werk van destijds. Immers, een van de prioriteiten was bepaald door die bescherming van de persoonlijke levenssfeer.

De voorbije twee of drie jaar zien we een technologische evolutie. Door de techniek kunnen we informatie op een steeds indringender manier delen. Tegelijkertijd lijkt men steeds meer de bescherming van de persoonlijke levenssfeer of zelfs de persoonlijke levenssfeer zelf te banaliseren. Ik heb daarnet gehoord dat de toegang tot informatie niets kost, maar ons privéleven wordt gekocht. Dat is ethisch gezien onvoorstelbaar. Immers, degenen die ons privéleven kopen, verkopen het ook. Er vindt een handel plaats zonder dat we daar volledig van op de hoogte zijn. We worden ingelicht door een tekst van tien bladzijden lang die we moeten ondertekenen. Door de tekst aan te klikken stemt men er automatisch mee in.

Het is daarover dat ik wil spreken. Het probleem van veiligheid en terrorisme in strikte zin moet misschien los gezien worden van het algemene debat. Anders geven we aan degenen voor wie het privéleven misschien minder belangrijk is, redenen om een recht dat voor ons essentieel is, aan banden te leggen.

Ik heb een spreker ook horen zeggen dat, aangezien het vergeetrecht bestaat, men zou kunnen denken dat de publicatie van bepaalde gegevens, bijvoorbeeld op Facebook, minder belangrijk zou zijn en dat het preventieve werk lichter kan worden.

Ik wil er de aandacht op vestigen dat het uiterst belangrijk is dit werk van informatie en preventie voort te zetten, vooral ten aanzien van jongeren.

In 2018 moet de richtlijn van toepassing zijn in alle Lidstaten. De wetgever moet op alle niveaus – federaal, gemeenschaps- of gewestelijk niveau – zijn werk op het vlak van informatie en preventie in het onderwijs voortzetten.

Men zou zich kunnen afvragen of het wel zin heeft wetten te maken, of het wel zin heeft verder te gaan, aangezien ze toch een voorsprong hebben en wetten dus nutteloos zijn. Ik denk dat dit niet waar is. We moeten wetten maken en teksten hebben waarmee we verder kunnen gaan. We moeten ook bestraffen.

Het is mogelijk dat voor de vijf groten die we daarnet al verschillende keren hebben vermeld, de sancties niets voorstellen. Maar als men ervan uitgaat dat men niets meer kan doen, dat wetgeving geen zin heeft, dan betekent dit dat men aan handen en voeten gebonden is aan die vijf groten die uiteindelijk misschien niet enkel ons consumptiepatroon, maar ook ons gedrag zullen bepalen.

De heer Eddy Caekelberghs *(in het Frans).* – Dames en heren, ik wil even terugkomen op de discussie rond de sociale dimensie, waarvan al sprake is geweest deze namiddag. Hoe gaan we die uitdaging tegemoet? Zoals reeds gezegd, betalen we thans in *privacy currency units*. We staan met andere woorden stukken van ons privé-DNA af om Google en andere soortgelijke bedrijven te betalen.

Om daar morgen aan te ontsnappen, zullen we wellicht echt moeten betalen. Tot nu toe kon ik een antireclamesticker op mijn brievenbus plakken. Zal ik morgen moeten afdokken als ik van bepaalde diensten algemene informatie wil ontvangen zonder te worden bespied? Hoe kunnen we dan vermijden dat er een sociale kloof ontstaat tussen degenen die zich kunnen veroorloven hun privéleven te beschermen en de anderen?

(Verder in het Nederlands) Mijnheer de staatssecretaris, bestaat daar al een goed antwoord op? Niet alleen in België natuurlijk, want Google, Yahoo en Facebook zijn natuurlijk niet Belgisch.

De heer Philippe De Backer. – Dat is juist. Daarom hebben we ook een Europese wetgeving gemaakt.

(Verder in het Frans) Het betreft geen richtlijn, maar een Europese verordening, de algemene verordening betreffende de gegevensbescherming, waarmee België zich in overeenstemming moet brengen.

Daarnaast lijkt transparantie me essentieel voor de consumenten. Het is niet aan mij om te beslissen of een deel van de gegevens mag worden doorgestuurd aan Google of Facebook, bijvoorbeeld om iets in de plaats te krijgen. Die vrijheid moet aan de consument worden gelaten. Het komt ons daarentegen wel toe om een kader te bepalen dat de grote principes definieert waarover de private en publieke instellingen het eens moeten worden en waaraan ze zich moeten houden.

(Verder in het Nederlands) Dat is essentieel in dit debat. Ik heb verschillende sprekers gehoord en soms doet men alsof het een zwart-witverhaal is. Men is ofwel voor privacy ofwel tegen privacy. Ofwel geeft men het op ofwel niet. We hebben in de Europese wetgeving precies principes gedefinieerd die voor een stuk een aantal elementen, die hier werden aangehaald, met elkaar kunnen verzoenen.

Ik geef een concreet voorbeeld. De eerste spreker sprak over Passenger Name Records (PNR). Ik zal kort schetsen hoe de algemene principes van toepassing werden op de PNR. Het betreft een Europese wetgeving, die nu naar Belgische wetgeving moet worden omgezet.

Vooreerst is er het aspect van de proportionaliteit. Is het verzamelen van de informatie al dan niet proportioneel met het doel dat men wenst te bereiken? De data die men opvraagt, zijn vandaag al beschikbaar bij alle vliegtuigmaatschappijen. Als consument heb je de gegevens al verstrekt. De vraag is of de overheid daartoe ook toegang kan krijgen in het kader van een duidelijke dataretentierichtlijn die vandaag bestaat. De data worden niet eeuwig, maar beperkt in de tijd bijgehouden.

Ten tweede, wat is de finaliteit? De finaliteit bepaalt wie toegang heeft en onder welke voorwaarden men toegang krijgt. Voor België hebben we

erover gewaakt dat de toegang alleen kan gebeuren in het kader van onderzoek naar terrorisme of zware misdrijven en altijd onder het toezicht van een procureur. Er is dus geen toezicht van het parlement, er is een justitieel overzicht en dat is cruciaal.

Ten derde zijn er de toegangsmodaliteiten. Wie kan toegang krijgen onder welke condities? Ook hier weer een justitieel overzicht.

Dat zijn de principes van de beveiligings- en beschermingsmaatregelen van *data protection* as such, technisch, technologisch, en de controle daarop. De kwaliteitsvereisten voor de opslag en het bewaren van die data zijn ook vastgelegd.

Ten vierde is er nog de transparantie, het inzagerecht. Een consument kan inzage krijgen in de opgeslagen data. Kortom, al die principes zorgen voor een gebalanceerde aanpak en zorgen ervoor dat men niet vervalt in een NSA-massasurveillance, maar aan de andere kant het doel van veiligheid proportioneel probeert toe te passen.

De heer Eddy Caekelberghs. – Blijft dat leefbaar? Wat als we in de toekomst verdragen sluiten met de Verenigde Staten of met Canada waarbij onze Europese privacywetten door grote multinationals worden genegeerd?

De heer Philippe De Backer *(in het Frans)*. – Ik denk dat uw informatie afkomstig is van een zeer specifieke bron, want noch in CETA, noch in TTIP is er sprake van de bescherming van de privacy.

Een tweede bedenking. Na het arrest Schrems van het Hof van Justitie van de Europese Unie werd een akkoord gesloten over de oprichting van het *Privacy Shield*, dat een grotere bescherming biedt voor de gegevensuitwisseling tussen Canada, Europa en de Verenigde Staten. Het betreft dus een zeer belangrijk initiatief, dat de bescherming van de privacy van onze burgers verhoogt.

Een derde element: de algemene verordening betreffende de gegevensbescherming formuleert strikte en duidelijke gedragsregels die moeten worden nageleefd door de ondernemingen die actief zijn op Europees niveau en die de gegevens van onze burgers gebruiken. Ik denk dat er ook op dat vlak iets moet gebeuren op Europees niveau. Als Facebook gegevens van Belgische burgers in België gebruikt – zoals we hebben gezien

met het probleem van de cookies – is het zeer moeilijk een procedure te starten tegen Facebook, omdat de verschillende Europese landen nog steeds niet over dezelfde technische mogelijkheden of over dezelfde juridische instrumenten beschikken. Er zijn dus initiatieven nodig op Europees niveau, zoals ik samen met de heer Buttarelli heb onderstreept. Als een burger van een EU-lidstaat met een probleem op dat niveau wordt geconfronteerd, zou het mogelijk moeten zijn de verschillende autoriteiten samen te brengen om te bekijken welke autoriteit het best in staat is om na te gaan of de regels worden geëerbiedigd, niet alleen vanuit juridisch, maar ook vanuit technisch oogpunt. Dat is de enige manier om een echte gegevensbeschermingsautoriteit op Europees niveau op te richten, om een belangrijke leemte in de algemene verordening betreffende de gegevensbescherming op te vullen. Dat is een van de essentiële opdrachten waaraan we ons de komende jaren moeten wijden.

De heer Eddy Caekelberghs *(in het Frans).* – Ik nodig nu de vertegenwoordigers van de partijen uit om ons hun standpunt te geven over het laatste element dat u hebt aangeroerd, namelijk wat er nog ontbreekt of wat er nog kan verbeteren.

De heer Andries Gryffroy (N-VA). – Om elk misverstand te vermijden, wil ik benadrukken dat wanneer ik sprak over de goedkeuring van het Parlement, het wel degelijk ging over het kader waarin de matching moet gemaakt worden, en uiteraard niet de eigenlijke matching zelf. Dat is voer voor de bevoegde diensten.

De kwestie van de sociale drempels, zoals daarnet door de heer Mahoux ook aangehaald, is een zeer lastige discussie. Als ingenieur heb ik echter ook een probleem als sociale drempels een rem kunnen zetten op innovatie. Moet men stoppen met innovatie of veeleer kijken hoe sociale drempels kunnen worden weggewerkt? Ik pleit voor innovatie en voor het aanpakken van de sociale drempels.

Als we met deze situaties worden geconfronteerd, is het dikwijls geen zwart-witverhaal, maar meestal is er een brede grijze zone. Nemen we bijvoorbeeld het medisch dossier. Ikzelf heb geen bezwaar tegen het feit dat mijn medisch dossier bij wijze van spreken op mijn identiteitskaart zou staan. Ik zou me zelfs beter voelen, als mijn gegevens bij een ongeval onmiddellijk en overal ter beschikking zouden zijn. Uiteraard moeten hier beperkingen worden toegepast, zoals de uitsluitende toegang voor

artsen. Naar mijn mening zouden we zelfs het RIZIV erbij kunnen betrekken, op een kostenefficiënte manier.

De heer Eddy Caekelberghs. – Gaat u ermee akkoord dat deze gegevens morgen door uw verzekeringsmaatschappij kunnen worden gelezen en dat u op basis daarvan al dan niet verzekerd zou kunnen worden?

De heer Andries Gryffroy (N-VA). – Neen, dat heb ik niet gezegd. Het opleggen van bepaalde grendels is wel een taak van het Parlement.

In het Vlaams Parlement heeft men ooit voorgesteld 100 kilowattuur gratis te geven aan elke burger. Dit werd berekend door een koppeling van de databases van de distributienetbeheerder en van het bevolkingsregister. Er is nu beslist om die gratis 100 kWh af te schaffen, maar tegelijk is ook de band tussen de twee gegevensbanken doorgeknipt. Nochtans bezorgde die link een schat aan informatie, zoals het gemiddeld verbruik van een één-, twee- of driepersoonsgezin. Deze gegevens kwamen anoniem in een databank en van daaruit konden die bestudeerd worden. Sinds 2016 gebeurt dit niet meer. Dat is jammer voor het energiebeleid.

De heer Benoit Hellings (Ecolo) *(in het Frans)*. – De methode is volledig veranderd. Als een politieagent of een belastinginspecteur twintig of dertig jaar geleden verdenkingen koesterde tegen een persoon of een groep personen, raadpleegde hij databanken die zich toen nog in een embryonaal ontwikkelingsstadium bevonden. Vandaag beschikken we over technische middelen waarmee we de informatie beter kunnen selecteren en er gemakkelijker toegang toe krijgen. Volgens de methode die ik voorsta, kunnen we een beroep doen op die middelen van zodra men een vermoeden van fraude heeft op basis van een inlichting die is ingewonnen op het terrein en die is geverifieerd via een verklikker of via maatschappelijk werkers, in het geval van een OCMW. In dat geval kan men zijn toevlucht nemen tot die instrumenten en de methode volgen die mevrouw Degrave daarnet heeft uiteengezet, namelijk databanken gebruiken en de informatie matchen. Mijnheer de staatssecretaris, met de PNR en uw systeem voor de controle op het energieverbruik, werkt het omgekeerd. Bestaande gegevensbanken worden met elkaar verbonden en een algoritme definieert een *hit*, met andere woorden, een profiel. Het systeem wordt dus omgekeerd.

De openbare overheden geven op die manier niet het goede voorbeeld. We kunnen de grote informatie- en technologie-industrieën niet verwijten

dat ze de privacy niet respecteren aangezien we de weg van de veralgemeende controle in plaats van de gerichte controle inslaan.

In sociale zaken gebeurt hetzelfde. Mijnheer De Backer, u zei daarnet dat de PNR proportioneel was. We zullen er nog over debatteren. Er is momenteel echter een klacht bij het Europees Hof van Justitie aanhangig over een PNR-akkoord tussen Europa en Canada. Dat heeft niets met CETA te maken. Aan het Hof werd de vraag voorgelegd of dat akkoord in overeenstemming is met het Europees recht. Volgens het advies van de advocaat-generaal, dat vaak wordt gevolgd, is het niet proportioneel, om dezelfde reden als de reden die ik daarnet heb vermeld: om de veiligheid te respecteren is het gerechtvaardigd dat de Staten een relevante inlichting delen over een potentieel gevaarlijk persoon, op gevaar af een beetje verder te gaan dan alleen de echt gevaarlijke personen in aanmerking te nemen, want vergissingen zijn mogelijk. Maar in dit geval worden gegevens van alle passagiers gedeeld. U wil netten uitwerpen om haaien te vangen, maar uiteindelijk zult u dolfijnen vangen.

Mevrouw Katia Segers (sp.a). – Ik wil even terugkomen op de discussie rond de sociale dimensie. We moeten het internet erkennen als een basisinfrastructuur en een basisrecht. Sinds 2014 ligt daarover in de Kamer een wetsontwerp klaar.

We moeten ook inzetten op e-inclusie. Vorige week besliste ING kantoren te sluiten. Uit een studie van de Gezinsbond blijkt dat één op twee vijfenvijftigplussers niet wil of niet kan internetbankieren. Er is nog een belangrijk vraagstuk van digitale kloof.

Ik kom terug op de essentiële vraag, namelijk zelfbeschikking. De vertegenwoordiger van Agoria zei: ‘Eigenlijk is de vraag simpel. Het gaat erover wie welke informatie mag hebben.’ Dat is niet de juiste vraag. De juiste vraag moet zijn: ‘Wat wil ik als individu, dat over mijzelf kan beschikken, vrijgeven?’

In tijden van digitale radicalisering moeten we zowel de businessmodellen als onze beleidsmodellen grondig herdenken. Iemand heeft berekend dat mocht Facebook een premiummodel aanbieden, een beetje zoals Spotify, gratis, met reclame, of betalend zonder reclame, dat men dan niet meer dan acht euro zou moeten betalen voor een abonnement op Facebook om niet gevolgd te worden, geen vervelende popupreclame te krijgen van reizen die men vijf weken geleden al heeft gemaakt.

Er zit ook een stuk empowerment achter. Ik kom terug op de gezondheidsaspecten. Platformen als 'PatientsLikeMe', waar patiënten met hetzelfde ziektebeeld informatie uitwisselen, zijn zowel voor henzelf als voor de wetenschap en de geneeskunde interessant. Uiteraard moeten die patiënten dan beseffen dat daar ook een businessmodel achter zit. Het inzicht daarin is essentieel.

Tevens denk ik dat big data *open data* moeten worden. Er moet zoveel mogelijk *open sourcing* mogelijk zijn. De mens zelf moet beschikken. Er zijn een aantal interessante aspecten. Onder andere professor Helbing uit Zürich heeft een alternatief ontwikkeld voor big data, namelijk Nervousnet. Daar kunnen mensen zelf aangeven wat ze vrijgeven. Dat wordt essentieel.

De heer Eddy Caekelberghs. – Deelt de regering dat standpunt, mijnheer de staatssecretaris? Bent u het eens met die definitie?

De heer Philippe De Backer. – Bij het gebruik van gegevens, bijvoorbeeld in de strijd tegen de sociale fraude, heeft de regering er altijd voor gezorgd dat ze over een aparte juridische basis kon beschikken, goedgekeurd door het Parlement. Dat is belangrijk, want op die manier erkennen we dat het om een uitzondering gaat. Dat betekent ook dat we voor dergelijke aangelegenheden telkens naar het Parlement komen en duidelijk de vraag stellen of we die gegevens al dan niet mogen gebruiken, of het proportioneel is en wat de finaliteit is. Dat is een belangrijk aspect waaraan ook wij als overheid ons moeten houden en dat doen wij ook.

Voorts wil ik het hebben over de PNR en het standpunt van het Europees Hof ter zake. Als lid van het Europees Parlement heb ik de debatten met Louis Michel meegemaakt over de balans tussen het verzamelen van gegevens en de PNR in de strijd tegen terreur, over het gebruik van die gegevens en de uitwisseling met andere lidstaten. De discussie gaat in de eerste plaats over het kader waarin wij de PNR hebben geplaatst. Daarover zijn de lidstaten en het parlement het eens geworden.

Ten tweede is er de vraag wie toegang krijgt tot die gegevens en op welke manier. Dat zijn twee afzonderlijke debatten. Het debat rond de toegang tot die databanken is een ander debat dan u wil voeren.

Ten derde beschikken big data over veel potentieel voor interessante toepassingen. Ze kunnen het persoonlijke leven van veel mensen verrijken.

Anderzijds hoed ik mij als staatssecretaris ten zeerste voor de automatisering van beslissingen die eraan gekoppeld kunnen worden. Dat is een aspect dat de parlementen onder elkaar fundamenteel moeten bekijken. Als ik gegevens binnenkrijg die vanuit big data zijn gegenereerd, die ik koppel aan andere gegevens, zorg ik ervoor dat er een discussie plaatsvindt en een afweging gebeurt over de manier waarop die gegevens gebruikt moeten worden. Dat is iets anders dan een geautomatiseerde beslissing die gebeurt op basis van een profiel. Het is belangrijk dat mensen zelf zicht krijgen op die gegevens. Daarom pleit ik voor de invoering van een privacypaspoort. Dat is een manier om aan burgers duidelijk te maken waar hun gegevens zich bevinden, wie over hun gegevens beschikt, wie er toegang tot heeft, wie ze raadpleegt. In Estland bestaat er een dergelijk systeem. Op die manier geven we burgers veel meer controle over hun gegevens, meer transparantie en inzicht over hoe er met hun gegevens wordt omgegaan.

De heer Eddy Caekelberghs. – Mevrouw zou dus kunnen weten wie in de administratie om 9 uur 's avonds haar foto heeft bekeken?

De heer Philippe De Backer. – Dat systeem bestaat vandaag in Estland. Als men gegevens raadpleegt, kunnen burgers dat zien. Bovendien, als een burger twijfels heeft over de rechtmatige toegang tot zijn gegevens, kan hij een klacht indienen. Er is dus ook een stok achter de deur.

De heer Eddy Caekelberghs. – Of ze zou kunnen afspreken met de persoon die haar foto heeft bekeken. Dat was een grapje.

De heer Jacques Brotchi (MR) *(in het Frans)*. – Iedereen plaatst op Facebook wat hij of zij wil. Niemand is verplicht zijn privéleven op Facebook te delen. Iedereen is verantwoordelijk en moet nadenken over wat hij of zij verspreidt.

Wat het medische aspect betreft, denk ik niet dat een verzekeraar toegang zou kunnen hebben tot de gegevens die op de identiteitskaart of een andere kaart zouden zijn aangebracht.

Dat alles moet uiteraard voortvloeien uit beslissingen met het oog op de bescherming van de privacy van eenieder. Vandaag gebeurt hetzelfde. Om toegang te krijgen tot een medisch dossier is er een code. Een arts die in een ziekenhuis werkt, heeft geen toegang tot de medische dossiers van andere ziekenhuizen.

Ik zie dus niet in waarom een verzekeraar toegang zou hebben tot de gegevens die zouden worden gedeeld om onze gezondheid te beschermen in het geval ons ergens iets overkomt.

Ik wil nog zeggen dat het niet toevallig is dat dit colloquium wordt gehouden. Op het federale niveau is er de wetgeving betreffende privacy, maar de deelstaten dragen ook verantwoordelijkheid. Het economisch beleid is een gewestelijke bevoegdheid geworden. Bijgevolg zijn de innovatie, de nieuwe technologieën en de informatica gewestelijke materie. Tot het niveau van de deelstaten behoren ook het hele culturele vraagstuk en het probleem van de bescherming van de privacy van adolescenten op de sociale netwerken.

Ik wil de voorzitster, mevrouw Defraigne, nog bedanken voor het initiatief van het debat van vandaag.

Tot slot wil ik zeggen dat de MR bijzonder waakzaam is over alles wat de privacy raakt. Wij zijn van mening dat bijzondere opsporingsmethodes, zoals telefoontap, controle van het internetverkeer en dergelijke, altijd gepaard moeten gaan met afdoende rechterlijke waarborgen om misbruiken te voorkomen. De staatssecretaris heeft dat daarnet al gezegd, maar ik wou het nog eens herhalen.

De heer Eddy Caekelberghs *(in het Frans).* – De heer Mahoux heeft het woord.

De heer Philippe Mahoux (PS) *(in het Frans).* – Wat de bijzondere methoden betreft waarover de heer Brotchi daarnet sprak, biedt onze wetgeving de mogelijkheid te controleren. De heer Rapaille heeft er ook naar verwezen. Ik herinner eraan dat onze controlestructuur uit drie magistraten bestaat. Dat is een zeer belangrijk element.

Mijn tweede opmerking gaat over de gezondheid. Informatie over mijn gezondheid op één plek samenbrengen kan nuttig zijn voor mij persoonlijk en zelfs voor de maatschappij, voor statistieken ten behoeve van epidemiologie of onderzoek.

Wat het al dan niet vrijwillige aspect betreft, wil ik mijn uitspraken illustreren met een voorbeeld. Vannacht werd ik om vier uur wakker en heb ik mijn tablet gebruikt. Ik ben er zeker van dat ik binnen de 48 uur een reclameboodschap zal krijgen voor middelen tegen slapeloosheid.

Dat is het probleem. Het zijn niet de gegevens die ik doorgeef die worden gebruikt. Indien dat het geval was, zou dat uiteindelijk geen probleem vormen. Het is mijn gedrag en de informatie die ik opzoek die worden gebruikt. Tegen wil en dank geeft de informatie die ik opzoek inlichtingen over mij.

Als men evenwel vrijwillig informatie geeft, moet dat met volledige kennis van zaken gebeuren. We moeten zeker de digitale kloof dichten.

Er is een gebrek aan transparantie over mijn toestemming als ik die media gebruik. Er moet wetgeving komen die dat verhindert. Dat is de enige mogelijke werkwijze.

De heer Bertin Mampaka Mankamba (cdH) *(in het Frans).* – Daarnet veerde Philippe Mahoux op toen professor Brotchi zei dat wie gegevens op Facebook plaatst, ze de facto aan iedereen bekend maakt, ook aan de maatschappelijk werker of de belastingcontroleur die misschien geneigd is een aanzuivering van de belastingen te weigeren als hij foto's heeft gezien van de betrokkene tijdens zijn vakantie in Dubai, in een van de mooiste hotels ter wereld, in een kamer van zevenduizend euro per nacht. Ik begrijp dat dat reacties teweegbrengt.

Dat toont aan dat, ondanks bepalingen die vandaag van kracht zijn, het voortdurend nodig is onze wetgeving te verfijnen, met veel voorzichtigheid. Ik denk aan de consumenten.

Philippe Mahoux heeft een goed idee naar voren geschoven met zijn suggestie dit debat later op te splitsen tussen de veiligheidsproblematiek, die we jammer genoeg allemaal kennen via de aanslagen in Parijs, Brussel en elders, en andere aspecten.

Zoals reeds gezegd, willen velen een zekere soepelheid aan de dag leggen op het vlak van de bescherming van de privacy om een collectieve veiligheid te herwinnen. Ik heb het gevoel dat daarover misschien een diepgaand debat moet worden gevoerd.

Als het over de gewone burger gaat, de kleine consument, die op Facebook graag uitpakt met zijn vakantie in Zuid-Frankrijk en wiens sociale uitkeringen worden afgepakt, of nog, over mensen die geweigerd worden bij sommige verzekeringsmaatschappijen wegens inlichtingen die verkeerd worden gebruikt, denk ik dat het nodig is dat de overheid over

technische bevoegdheden kan beschikken – de staatssecretaris heeft dat trouwens gezegd – en dat er binnen een redelijke termijn wetgevend moet worden opgetreden om de gewone burger, die bestookt wordt met allerlei voorstellen, te beschermen.

De heer Eddy Caekelberghs *(in het Frans)*. – Dames en heren, waarschijnlijk zult u weldra de ontwikkelingen kunnen volgen in de verslagen van de Kamer.

Ik dank u voor uw antwoord op de vragen. Voor de conclusies van onze debatten geef ik nu het woord aan de heer Louis Michel, minister van Staat en Europarlementslid.

Besluit

De heer Louis Michel *(in het Frans).* – De organisatie van dit colloquium, over een onderwerp dat ons allen aanbelangt, is een schitterend initiatief van de voorzitster.

Nadat ik alle sprekers heb gehoord, heb ik het gevoel dat de politieke gezagsdragers zich ook in dit geval weer in een reactieve in plaats van in een proactieve positie bevinden. Hetzelfde geldt wanneer men het heeft over het wereldwijde 'financiérisme' of over de platte speculatie. Men heeft de indruk dat de politiek zich in een toestand van onmacht bevindt, dat de gebeurtenissen, het leven en de geschiedenis sneller gaan dan wijzelf. De nieuwe technologieën en de media spelen daarin ongetwijfeld een rol. In dat opzicht rijst het probleem van de macht van de politiek in de meest verheven zin van het woord, en van de verantwoordelijkheid van de politiek, twee begrippen die in onze democratie nauw met elkaar verbonden zijn.

Uit alles wat ik heb gehoord, kan ik opmaken dat de manier waarop de overheid persoonlijke gegevens gebruikt, apart moet bekeken worden. Daartoe moet er een kader bestaan, ook al betreft het zaken die het algemeen belang dienen. Iemand had het over de kruispuntbank. Toen ze werd opgericht, maakte ik deel uit van de regering. Het was een vrij moeilijk en netelig debat. Dat was ook het geval voor de Commissie voor de bescherming van de persoonlijke levenssfeer. De kruispuntbank functioneert vandaag relatief goed. Het debat over de PNR en over de anonimisering van gegevens zorgde voor een probleem want daardoor zou ze vrijwel niet meer kunnen werken. Er was sprake van om informatie, ook die van een instelling zoals de kruispuntbank, na vijf jaar anoniem te maken. Het opnieuw coderen en aanpassen van de gegevens zouden enorm veel werk hebben gevergd. Wij hebben het recht om een onderscheid te maken tussen het gebruik van gegevens voor doeleinden van openbaar nut, enerzijds, en voor privédoeleinden, anderzijds. Op het Europese niveau bestaan er voor dat laatste strikte regels. Dat geldt overigens ook voor het gebruik van privégegevens door de overheid.

Ik had het daarnet over de onmacht van de politiek. Ik ben er niet zeker van dat er ook maar één parlementslid van deze vergadering in de Senaat of in de Kamer, ook al had hij tal van rechtmatige argumenten, had durven pleiten voor het behoud van cashgeld. Als een politicus een dergelijk standpunt verdedigt, maakt hij zich automatisch verdacht.

Geen enkele politicus zal ervoor pleiten het gebruik van cash te behouden omdat het afschaffen ervan ingrijpt in het privéleven, in de vrijheid van het individu. Het gaat er niet om te frauderen of wit te wassen, dat spreekt vanzelf. Biljetten van vijfhonderd euro zijn gemakkelijker te transporteren dan biljetten van honderd of van vijftig euro. Als lid van de Panama Papers-onderzoekscommissie heb ik onlangs vernomen dat er systemen bestaan om biljetten van vijfhonderd euro om te wisselen tegen biljetten van vijftig euro. Sommigen zouden zelfs betalen voor biljetten van vijfhonderd euro.

Het streven naar transparantie is natuurlijk legitiem, maar het mag niet tot gevolg hebben dat mensen karakterloze wezens worden, die geen recht hebben te worden vergeten, geen recht om een andere weg te bewandelen, om van gedachte te veranderen, om een ander leven te leiden. Al die gegevens, die vertaald worden in mathematische algoritmen, kunnen een beeld geven van een perfecte mens. In het verleden had men ook opvattingen over het beeld van de perfecte mens. En ook van de nieuwe mens. We staan voor een fundamentele filosofische kwestie. Ik zou dus graag de mening van de filosofen over dit onderwerp horen.

Ik wil mij niet laten leiden door een moralisme dat voorhoudt dat mensen voorbeschikt zijn. Men kan dan niet meer een klein beetje zondigen. Dat stoort mij. Een mens zit ingewikkelder ineen. Een mens is geen schepsel dat definitief af is. Hij maakt een voortdurende evolutie door. Hij is drager van verschillende identiteiten. Wij hebben allemaal een heleboel identiteiten en onze persoonlijkheid kan niet worden herleid tot de optelsom van die identiteiten. Er vindt een integratie van die identiteiten plaats. We hebben identiteiten die elkaar herkennen omdat ze met elkaar verwant zijn. Over dat aspect moet ook van gedachten worden gewisseld.

Ik vond dit een zeer interessant colloquium, waarbij we veel hebben kunnen opsteken. Er werd een brug geslagen tussen de politieke en de academische wereld. Die twee werelden houden elkaar nog te vaak op een afstand. Soms is er sprake van argwaan of angst tegenover elkaar. Het Parlement heeft de academische wereld en de burgermaatschappij nodig. Men hoeft geen expert te zijn om deel te nemen aan de uitwerking van een strategie of van een beleid. Het is dus belangrijk dat er regelmatig vergaderingen zoals deze worden georganiseerd.

Ik had een tekst van elf bladzijden voorbereid, maar ik vond het beter om het over de kern van dit debat te hebben en over wat ik ervan heb

onthouden. Ik voel een grote vriendschap voor Philippe De Backer. Ik heb hem leren kennen als Europarlementslid en ik kan u zeggen dat hij zeer veel aandacht heeft voor de bescherming van de privacy.

Ik dank u nogmaals, mevrouw de voorzitster. Ik dank iedereen, in het bijzonder de oude bekenden die ik hier met veel plezier heb teruggezien.

Verantwoordelijke uitgever: Gert Van der biesen, secretaris-generaal van de Senaat

Drukkerij van de Kamer van volksvertegenwoordigers