Platform Bescherming Burgerrechten
Weteringschans 259
1017 XJ Amsterdam
www.platformburgerrechten.nl

Tweede Kamer der Staten-Generaal
Vaste commissie voor Veiligheid en Justitie
Postbus 20018
2500 EA Den Haag

Afschrift aan:
Staatssecretaris van Veiligheid en Justitie

Amsterdam, 10 september 2011

Betreft: AO privacybeleid 15 september 2011

Geachte voorzitter en leden van de vaste commissie voor Veiligheid en Justitie,

Ter gelegenheid van het aanstaande Algemeen Overleg over het privacybeleid brengen wij graag de volgende onderwerpen onder uw aandacht:

a. de verwerking van persoonsgegevens van onschuldige burgers in het kader van toezicht zonder dat er sprake is van een redelijke verdenking. Iedereen wordt nu in principe behandeld als verdachte;
b. de aantasting van de privacy middels Automatische NummerPlaat Registratie (ANPR);
c. het inrichten van een surveillancesamenleving die het fundamentele recht van burgers om onbespied te kunnen leven aantast;
d. de ontwikkeling van een technocratisch controlenetwerk met open toegang en uitwisseling met andere landen dat niet past in een democratische rechtsstaat.

Eerder dit jaar vond er een debat in de Eerste Kamer plaats rond digitale gegevensverwerking. Hiertoe verstuurden de staatssecretaris van Veiligheid en Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties op 29 april 2011 een brief met bijlagen naar de Kamer. In deze brief stonden een aantal zaken die wij als zeer zorgelijk ervaren.

Op pagina 1 van de eerste bijlage bij de brief staat dat de verwerking van persoonsgegevens in de visie van het kabinet een belangrijke ondersteuning kan betekenen voor een beleid dat gericht is op de veiligheid in de openbare ruimte. Deze ambitie betekent in de praktijk: het verwerken van persoonsgegevens voor het houden van toezicht. Geen opsporing, maar toezicht. Dit betekent dat gegevens van onschuldige burgers worden verwerkt, bijgehouden, wellicht samengevoegd tot een profiel en inzichtelijk gemaakt voor de overheid, zonder dat de burger iets heeft misdaan. Surveillance-technologie wordt hier tegen onschuldige burgers ingezet, waar dit vroeger nog op zijn minst door een officier van justitie moest worden bevolen en hiervoor eerst een redelijke verdenking nodig was. Het resultaat is dat iedereen in onze samenleving wordt behandeld als een verdachte. Een dergelijke wantrouwige houding is meer gepast binnen een totalitaire samenleving dan binnen een democratische rechtsstaat.

Het blijft niet alleen bij woorden, dit kabinet formuleert ook ambities om deze controlewens uit te voeren. Zo wordt er ingezet op ANPR voor de gehele bevolking. ANPR wordt al toegepast, maar herkent nu slechts nummerplaten die zijn opgeslagen in een politiedatabase. Hierdoor blijven ‘onschuldige’ burgers buiten beschouwing. Het Duitse Constitutionele Hof besloot op 11 maart 2008 bij eenzelfde uitbreiding van de *scope* naar alle burgers dat dit een ernstige schending vormt van het grondrecht op bescherming van de persoonlijke levenssfeer (privacy). Toen twee Nederlandse politiekorpsen in 2010 een proef deden waarbij alle voertuigen werden geregistreerd, werden zij op de vingers getikt door het College Bescherming Persoonsgegevens. De reactie van de toenmalige ministers van Binnenlandse Zaken en Justitie was ontluisterend, aangezien zij formeel hun excuses aanboden maar tegelijkertijd aankondigden dat ze dan de wet wel zouden aanpassen opdat deze evidente inbreuk in de toekomst wel door de beugel zou kunnen. Als de rechtvaardiging van een wet

in de wet zelf zou liggen, dan is die rechtvaardiging weinig waard. Het eindresultaat is een databank waarin massaal de gegevens van álle burgers worden opgeslagen ter opsporing van strafbare feiten. Dit is een omkering van het klassieke beginsel “geen inbreuk op privacy zonder voorafgaande redelijke verdenking”. Voor ons is de vraag inmiddels of de wetgever in deze tijd de grondrechten van burgers voldoende beschermt en in dat opzicht een afdoende garantie van controle op de uitvoerende macht is. Kennelijk vertrouwt de uitvoerende macht erop dat de wetgever vrijwel ongezien dit soort inbreuken op grondrechten in een wet zal gaan verankeren.

Een ander onderwerp dat ons grote zorgen baart is dat dit kabinet ook inzet op uitbreiding van cameratoezicht in de openbare ruimte. Allereerst is het daarbij zorgelijk dat totaal voorbij wordt gegaan aan alle onderzoeksresultaten over cameratoezicht die systematisch uitwijzen dat dit vaak geen effectieve methode vormt om de veiligheid te vergroten. Daarbij komt nog dat in dit verband de link wordt gelegd met ‘de verwerking van persoonsgegevens’, hetgeen doet vermoeden dat dit kabinet camera’s wil gaan uitrusten met gezichtsherkennende software. Persoonsgegevens verwerken door middel van cameratoezicht leidt in de praktijk tot een automatische registratie van alle personen in de openbare ruimte. Hoewel dit kabinet nog niet openlijk inzet op het ontwikkelen van zo’n infrastructuur, wordt het bouwen daarvan op deze wijze van beleidsvorming wel degelijk voorbereid. De burger is niet bekend of camera’s (die in steeds grotere getale overal in de publieke ruimte worden opgehangen) kunnen worden gebruikt voor gezichtsherkenning, maar gezien de huidige stand van de techniek is dit zeer aannemelijk. De vraag dringt zich daarom op wat het beleid ten aanzien van uitbreiding van cameratoezicht in de praktijk betekent en hoe de technische mogelijkheid van het inrichten van een surveillancesamenleving zich verhoudt tot het fundamentele recht van de burger om onbespied te kunnen leven.

Dat wij ernstig bezorgd zijn over deze ontwikkelingen is niet zomaar. Zo werd al in het onderzoeksrapport ‘Security Applications for Converging Technologies’ van het Wetenschappelijk Onderzoek- en Documentatiecentrum van Justitie (WODC) uit 2008 (p. 105) besproken hoe gezichtsherkenning en bewegingsherkenning in de toekomst kunnen worden gebruikt om individuen in de massa te identificeren. In het EU-rapport ‘Safeguards in a World of Ambient Intelligence’ (SWAMI) wordt op pagina 37 gesteld dat dit soort technologieën handhavings- en inlichtingendiensten kunnen helpen bij het nemen van ‘preventieve maatregelen’.

Het verontrust ons dat diensten zoals de AIVD, die nauwelijks onder uw democratische controle staan, in de toekomst wellicht worden uitgerust met middelen waarmee ze willekeurig personen kunnen opsporen in openbare ruimtes en tevens profielen van die personen kunnen bijhouden. Dit vormt slechts de opmaat voor een nog intensievere bewakingsmaatschappij. In een ander scenario in het WODC-rapport wordt de situatie geschetst dat mensen in de toekomst in en rond hun lichaam RFID-chips zullen dragen en dat deze ook kunnen bijdragen aan toezicht (p. 183). Het is vreemd dat de regering bij de aanbieding van haar beleid geen enkele aandacht besteed aan de samenhang tussen camerabewaking, gezichtsherkenning, identificatieverplichtingen met documenten die voorzien zijn van digitale gezichtsscans en het OV-chipkaartsysteem (waarbij zowel gezichtsscans worden vastgelegd als camerabewaking wordt ontwikkeld voor allen die gebruikmaken van het Openbaar Vervoer). De samenhang tussen zulke belangrijke ontwikkelingen zou niet volkomen onbelicht moeten blijven bij de aanbieding van het beleid van deze regering. Dat het kabinet deze ontwikkelingen ondersteunt met beleidsnota’s die worden aangeprezen als beleid dat ‘krachtig inzet op meer aandacht voor informatiebeveiliging en de bescherming van persoonsgegevens’ achten wij verbazingwekkend. Aan u de taak om een open democratisch debat te entameren over de richting waarin de maatschappij zich ontwikkelt als de regering op de ingeslagen weg doorgaat.

Tevens wijzen wij u er op dat de ontwikkeling van een surveillancemaatschappij ook in breder Europees verband actief wordt vormgegeven. Het toezicht gaat volgens een EU Council Presidency paper zelfs nog een stuk verder: “Every object an individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts.” Daarnaast maakte de Europese Commissie duidelijk dat zij graag deze persoonlijke informatie wil delen met de Verenigde Staten.[1] Wij merken daarbij op dat hoewel het

[1] Zie *Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe* (COM(2010) 673 final), p. 3.

bestrijden van terrorisme en georganiseerde misdaad beide legitieme doelen zijn voor overheden om effectief gebruik te maken van de technische mogelijkheden om toezicht te houden, deze nooit het minutieus en gedetailleerd registreren en inzichtelijk maken van eenieders leven rechtvaardigen. Wie zich in de materie van de aantasting van de persoonlijke vrijheid verdiept, kan niet anders dan concluderen dat het Nederlandse volk langzaamaan wordt uitgeleverd aan een mondiale technocratie.

De grootschalige inbreuk op de grondrechten van de Nederlandse burger is de laatste jaren al veel te ver gegaan en het is aan u om dit een halt toe te roepen. Wij noemen in dit verband:
- het wetsvoorstel tot verplichte invoering van 'slimme' energiemeters;
- de invoering van een surveillancesysteem als betaalvoorziening voor reizigers in het OV;
- de opslag van vingerafdrukken en gezichtsscans middels de Paspoortwet;
- het doorontwikkelen van een landelijk EPD en Elektronische Kind-, Onderwijs- en Jeugdzorgsystemen;
- de invoering van een Strafketendossier voor mensen die slechts als verdachte worden aangemerkt;
- verplichte DNA-opslag voor justitiële doeleinden van iedereen die veroordeeld is voor een strafbaar feit waar 4 jaar hechtenis voor gegeven kan worden, ongeacht of er zelfs maar sprake is van strafoplegging;
- de verplichte opslag van ieders telecommunicatiedata.

Dit is zomaar een greep uit de lawine aan wet- en regelgeving waarbij er niet of onvoldoende sprake was van toetsing aan het grondrecht op bescherming van de persoonlijke levenssfeer.

Om het tij te keren achten wij het noodzakelijk dat er vanuit de Tweede Kamer een krachtig signaal wordt gegeven aan het kabinet. Daartoe verzoeken wij u om de huidige wetgeving en de komende wetsvoorstellen die van invloed zijn op de privacy van de burger grondig te toetsen aan het recht op respect voor het privéleven zoals omschreven in artikel 8 van het EVRM. Gezien het feit dat de noodzaak van een wet ook altijd afhankelijk is van het moment in de geschiedenis, is het tevens belangrijk om horizonbepalingen in de wetgeving op te nemen. Als controlerende instantie op de uitvoerende macht is het nu tijd om concrete maatregelen te nemen die ruimte bieden voor bezinning. Wij hopen dat u in dezen uw verantwoordelijkheid zult nemen.

Namens de deelnemers aan het Platform Bescherming Burgerrechten, verblijf ik,
Hoogachtend,

Vincent Böhre
voorzitter Platform Bescherming Burgerrechten
voorzitter@platformburgerrechten.nl

Mede namens de volgende Platform-deelnemers:
Vereniging Vrijbit
Stichting Privacy First
Ouders Online
Stichting Meldpunt Misbruik ID-plicht
Stichting KDVP
Joyce Hes
Jacqueline Gerretsen
DeVrijePsych
Jacques Barth