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

Tweede Kamer der Staten-Generaal
T.a.v. de informateurs
Dhr. drs. W.J. Bos en dhr. H.G.J. Kamp
Postbus 20018
2500 EA Den Haag

Afschrift aan: fractievoorzitters Tweede Kamer

Amsterdam, 20 september 2012

Betreft: aanbevelingen van het Platform Bescherming Burgerrechten t.b.v. kabinetsformatie

Geachte heren,

Graag willen wij u als Platform Bescherming Burgerrechten een aantal aanbevelingen voorleggen die drie terreinen bestrijken, namelijk 1) privacybeschermende wetgeving en maatregelen, 2) onderwerpen die de democratische rechtsstaat betreffen en ons aller persoonlijke vrijheid en burgerrechten raken en 3) nieuwe technologieën en daaraan verbonden risico's voor de privacy.

De laatste jaren is in Nederland een tendens te bespeuren waarbij ieder maatschappelijk probleem met een standaard-recept lijkt te worden benaderd, namelijk meer digitale registratie, meer koppeling van bestanden en centrale ontsluiting van systemen en databanken die voor steeds meer functionarissen en derde partijen toegankelijk worden, inperking van professionele autonomie, preventieve controle en *profiling*.

Het lijkt erop of men, vooral in de politiek, gevoed door media en de *vox populi* voorzover ook weer beïnvloed door de media, in deze instrumenten een beheersing van de samenleving ziet die tot meer orde en rust en veiligheid zou moeten leiden.

Naar onze mening is het omgekeerde nu steeds vaker het geval.

Digitalisering brengt namelijk met zich mee dat de hoeveelheid gegevens die over iedere burger wordt opgeslagen steeds groter, onoverzichtelijker en onbeheersbaarder wordt. Dit geldt des te meer voor gegevens die foutief zijn ingevoerd, verkeerd gekoppeld of verouderd zijn.

Met de exponentiële toename van digitale registraties nemen de risico's van datalekken navenant toe en ontstaan nieuwe vormen van identiteitsfraude en -diefstal . Daarmee wordt de onveiligheid van digitale systemen een onveiligheid die burgers direct bedreigt. Daarnaast is er een risico dat burgers door digitale profilering verworden tot hun digitale 'dubbelgangers'. De autonomie van de vrije en participerende burger die zo belangrijk is in een democratische rechtsstaat komt daarmee ernstig in gevaar.

Terug naar een maatschappij zonder internet of digitale bestanden is echter iets wat wij geenszins voorstaan en is inhoudelijk onmogelijk.

Echter een verstandig gebruik van technische middelen, waaronder dataopslag en biometrie en andere technische verworvenheden, zal noodzakelijk zijn willen wij onze democratische rechtsstaat met de bijbehorende grondrechten overeind houden.

Juist in deze tijd van onvoorziene technische mogelijkheden moeten wij ons eens temeer realiseren hoe belangrijk de grondbeginselen van onze samenleving zijn. Iedere keer zal dan ook een afweging moeten plaatsvinden waar de grenzen van het toelaatbare liggen en hoe eventuele alternatieven in de menselijke sfeer zoals meer persoonlijke controles maar ook hulp en dienstverlening wenselijk dan wel noodzakelijk zijn.

Daartoe hebben wij de volgende aanbevelingen geformuleerd:

PRIVACY

1. De principes van noodzakelijkheid, proportionaliteit en subsidiariteit dienen een bepalende rol te spelen bij de opstelling van alle wetgeving en beleid die een inbreuk maakt op de persoonlijke levenssfeer.
2. Bij alle wetgeving en beleid die de persoonlijke levenssfeer kan aantasten dient een onafhankelijke *Privacy Impact Assessment* (PIA) te worden uitgevoerd.
3. *Privacy by design* moet als uitgangspunt gelden bij alle ICT-projecten die betrekking hebben op de verwerking van persoonsgegevens en in het verlengde daarvan de persoonlijke levenssfeer van burgers. De ontwikkeling van *privacy enhancing technologies* (PET) krijgt hoge prioriteit.
4. De Wet bescherming persoonsgegevens (Wbp) en relevante bepalingen van het Europees Verdrag voor de Rechten van de Mens alsmede het Handvest van de Grondrechten van de Europese Unie dienen strenger te worden gehandhaafd.
5. Er dient een universele *opt-out* mogelijkheid te zijn bij de verwerking en koppeling van persoonsgegevens en biometrie, noodzakelijke uitzonderingen daargelaten.[1]
6. Het College Bescherming Persoonsgegevens (CBP) dient meer middelen en bevoegdheden te krijgen, waaronder een boetebevoegdheid. Burgers dienen een klachtrecht bij het CBP te krijgen.
7. Het DDJGZ (Digitaal Dossier Jeugdgezondheidszorg, voormalig EKD) blijft uitsluitend een medisch dossier met de daaraan verbonden privacy-eisen.

DEMOCRATIE & RECHTSSTAAT

8. Er dient een Constitutioneel Hof te komen. Tevens dient het verbod op constitutionele toetsing en het verbod van direct beroep tegen algemeen verbindende voorschriften (art. 8:2 Awb) te worden afgeschaft.

[1] *Opt-out* mogelijkheden zouden onder meer mogelijk moeten zijn bij: a) DBC-systematiek in de GGZ, b) alle vormen van centrale registratie en c) alle vormen van gebruik van biometrie. Als aantekening hierbij willen we stellen dat we als eerste prioriteit hebben om überhaupt voorzichtig te zijn met koppeling van bestanden en het gebruik van biometrie en centrale registraties, waar alternatieven zouden moeten worden overwogen.

9. Er dient een publiek debat te komen over de noodzaak van beperking van grondrechten.[2]
10. De overheid dient vier algemene mensenrechtelijke plichten opnieuw in acht te nemen, te weten het Naleven, Beschermen, Verwezenlijken en Promoten van alle mensenrechten, inclusief de burgerrechten.
11. Het primaat van de formele wetgever dient in ere te worden hersteld. Er moet zeer voorzichtig worden omgesprongen met holle kaderwetgeving die middels AMvB's en ministeriële regelingen moet worden ingevuld en waarbij in de praktijk van de uitvoering de privacy in het geding kan raken.[3]
12. Bij alle wetgeving en beleid dienen de onschuldpresumptie en het verbod op zelfincriminatie (*nemo tenetur*) weer als uitgangspunt te gelden.
13. Er wordt een onderzoek of parlementaire enquête naar de kosten van de controlestaat ingesteld. Naar aanleiding van dat onderzoek zouden de kosten naar verhouding beperkt moeten worden.[4]
14. Het College voor de Rechten van de Mens dient meer financiële middelen en volledige procesbevoegdheid te krijgen.
15. De overheid dient transparanter te worden door modernisering en versterking van de Wet openbaarheid van bestuur (Wob). De Wob krijgt als uitgangspunt actieve openbaarheid van bestuur in plaats van de huidige passieve openbaarheid.
16. Er dient meer transparantie te komen bij de Raadsgroepen en werkgroepen van de Europese Unie.
17. Er dient een openbaar overzicht te komen van het stemgedrag van ieder Kamerlid gedurende zijn/haar gehele politieke loopbaan.
18. Er dient meer aandacht te worden besteed aan mensenrechteneducatie, waaronder voorlichting over de risico's van het afstaan van je persoonsgegevens aan derde partijen.

NIEUWE TECHNOLOGIEËN

19. Niet alles wat technisch mogelijk is, dient ook te worden toegepast. Er dienen heldere grenzen te worden gesteld aan de inzet van nieuwe controletechnologieën. Technologie behoort de vrije mens en de vrije samenleving te dienen in plaats van andersom.

---

[2] Op dit moment wordt de aantasting van grondrechten bijna als vanzelfsprekendheid doorgevoerd in het kader van bijvoorbeeld fraudebestrijding (sociale zekerheid) of kostenreductie (GGZ) waarbij de professionele autonomie en het vertrouwensbeginsel tussen behandelaar en patiënt worden aangetast, of bij "gewone" bureaucratische controle (onderwijs, politie e.d.). Naar onze mening wordt het tijd hierover een publiek debat te voeren waarin een bureaucratisch centralisme in combinatie met de zogenaamde marktwerking en instrumentalisme wordt gelegd naast een type benadering waarin professionele autonomie en grondrechten weer centraal staan.

[3] Nu zien we meer dan eens dat er sprake is van "vermijding" van formele wetgeving. De Tweede en Eerste Kamer moeten genoegen nemen met vage beloftes van een minister 'dat het allemaal wel goed komt' of zelfs soms aantoonbare onjuistheden. Dat wreekt zich met name op het terrein van de privacy. Als namelijk in de praktijk van de uitvoering een spanning gaat optreden met de Wbp kan de wetgever niet meer zo makkelijk en zeker niet met terugwerkende kracht alsnog gaan ingrijpen. Ook in dit verband kan een *Privacy Impact Assessment* nuttig zijn.

[4] Bart de Koning geeft een schatting van deze kosten in 2008 van 3,5 miljard euro in zijn boek *Alles onder controle*. Als we echter ook de immateriële kosten zouden berekenen van alle (eerstelijns) professionals die gedwongen worden een groot deel van hun tijd aan administratieve en inefficiënte controle-eisen te besteden wordt de rekensom veel groter.

20. Van biometrische registratie mag slechts sprake zijn op vrijwillige basis.
21. Openbaar cameratoezicht met gezichtsherkenning, geluidsopnamen op gespreksniveau en automatische gedragsprofilering dienen te worden verboden.
22. Er worden geen mobiele vingerscanners bij de politie ingevoerd.

Wij hopen u met deze aanbevelingen van dienst te zijn en zijn graag tot een nadere toelichting bereid.

Namens het Platform Bescherming Burgerrechten, verblijf ik,
Hoogachtend,

Vincent Böhre
voorzitter Platform Bescherming Burgerrechten
voorzitter@platformburgerrechten.nl

Namens de volgende Platformdeelnemers:
Humanistisch Verbond
Stichting KDVP
Stichting Meldpunt Misbruik ID-plicht
Ouders Online
Stichting Privacy First
Burgerrechtenvereniging Vrijbit
Jacques Barth (vanuit Stichting Brein & Hart i.o.)
Joyce Hes (adviseur Platform Bescherming Burgerrechten)
Kaspar Mengelberg (vanuit DeVrijePsych)