BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

Ot van Daalen
ot.vandaalen [at] bof [punt] nl
+31(0)654386680

E.J. Arkenbout
Ministerie van Justitie

Betreft Aanbevelingen Bits of Freedom t.a..v. evaluatie Wet bescherming persoonsgegevens

Amsterdam, 7 september 2009

Geachte heer Arkenbout,

1. De Stichting Bits of Freedom ("**Bits of Freedom**") stelt het zeer op prijs dat zij in de gelegenheid wordt gesteld haar standpunten met betrekking tot de Wet bescherming persoonsgegevens ("**WBP**") in het kader van de evaluatie hiervan met het Ministerie van Justitie te delen.

2. Bits of Freedom beveelt in deze brief aan dat in het kader van deze evaluatie de volgende maatregelen worden genomen, of een aanzet daartoe wordt gedaan:

   - De introductie van een meldplicht datalekken.
   - De introductie van een audit-verplichting voor beheerders van databanken.
   - De bevordering van beveiligingsmaatregelen door "*privacy-by-design*".
   - De verplichtstelling van privacy effect rapportages bij wet- en regelgevingsvoorstellen.
   - De beperking in de tijd van privacy-beperkende overheidsmaatregelen.
   - De versterking van de bevoegdheden van het CBP.

3. Voordat Bits of Freedom deze aanbevelingen uitwerkt, maakt zij graag van de gelegenheid gebruik om kort de achtergrond hiervan te schetsen. Daarbij merkt zij op dat zij zich in deze brief beperkt tot meer structurele aanbevelingen: zij gaat niet in op details van de WBP die mogelijk ook voor verbetering vatbaar zijn.

Zonder bescherming persoonsgegevens is burgerlijke vrijheid in gevaar

4. Zonder een goede bescherming van persoonsgegevens, zal het leven van iedere burger steeds gedetailleerder in kaart worden gebracht, en dit proces kan zeer moeilijk worden teruggedraaid:

   - Er zullen steeds meer persoonsgegevens digitaal worden opgeslagen. Een onderdeel van de transformatie naar een informatiemaatschappij is dat iedere burger steeds meer interacteert met informatie-verwerkende technologie. Hierdoor zullen steeds meer persoonsgegevens over iedere burger digitaal worden opgeslagen.
   - Persoonsgegevens kunnen zonder toestemming en kennis van de betrokkene worden verzameld, verwerkt en verspreid. Het is steeds makkelijker om persoonsgegevens te verzamelen, te verwerken en te verspreiden, doordat de kosten van digitale technologie steeds verder dalen. Het is bovendien eigen aan digitale informatie, zoals persoonsgegevens, dat deze verzameld, verwerkt en verspreid kunnen worden zonder toestemming van de betrokkene en zonder dat deze daarvan op de hoogte is.
   - Het opslaan van persoonsgegevens is in zekere mate onomkeerbaar. De ervaring leert tegelijkertijd dat wanneer informatie eenmaal digitaal is opgeslagen, het niet is uitgesloten dat deze informatie vervolgens tegen de wil van de betrokkenen in de openbaarheid komt, bijvoorbeeld door een breuk in de beveiliging van de databanken waarin de gegevens worden opgeslagen. De verspreiding van informatie die eenmaal in de openbaarheid is gekomen, kan bovendien niet meer worden teruggedraaid. Eenmaal gepubliceerde compromitterende homevideo's, ingescande dagboeken, creditcarddatabanken, scans van paspoorten, etc. weten snel hun weg te vinden naar mirrors en filesharingnetwerken. Pogingen om dit materiaal te verwijderen werken meestal juist averechts.
   - De verwerking van persoonsgegevens leidt tot een steeds gedetailleerder beeld van de burger. Naarmate meer persoonsgegevens beschikbaar zijn, kan een steeds gedetailleerder beeld van de burger worden gevormd. Daarbij neemt het aantal mogelijke koppelingen tussen die persoonsgegevens (zowel binnen een databank als tussen verschillende databanken) exponentieel toe, naarmate meer van deze persoonsgegevens beschikbaar zijn. Door deze koppelingen kan een een zeer fijnmazige analyse van iedere burger worden gemaakt. Het is daarbij al op dit moment niet in te schatten wat de gevolgen zijn van de complexe interacties tussen de reeds bestaande databanken. Naarmate meer databanken zullen worden aangelegd, en deze databanken meer informatie zullen opslaan, en de technologie die deze data kan verwerken steeds geavanceerder wordt, worden deze interacties nog complexer.

5. Naarmate het leven van iedere burger steeds gedetailleerder in kaart wordt gebracht, wordt de vrijheid van de burger verder beperkt:

- Ten eerste zullen burgers hierdoor terughoudender zijn in het vormgeven van hun eigen leven, in de wetenschap dat hun leven wordt vastgelegd en in de gaten wordt gehouden, en uit angst voor chantage, represailles etc.
- Ten tweede leidt dit tot een verstoorde machtsbalans tussen de burger en de beheerders van deze databanken: de beheerders van deze databanken weten vrijwel alles over een burger, maar de burger weet vrijwel niets over de beheerders van deze databanken.
- Ten derde is niet uitgesloten dat de burger verstrikt raakt in een Kafkaësk web van digitale informatie dat over hem of haar beschikbaar is, nu deze informatie deels incorrect is en het vaak moeilijk is om deze informatie te corrigeren.
- Tot slot is niet uitgesloten dat deze infrastructuur misbruikt wordt tegen de burger. Dit zal nu nog incidenteel van aard zijn. Op termijn kan dit structurele vormen aannemen, net zoals het persoonsregister in de Tweede Wereldoorlog is gebruikt voor de Jodenvervolging. Zoals hierboven is aangegeven is het veel moeilijker digitale informatie te vernietigen dan deze te genereren en te verspreiden, dus op het moment dat deze informatie misbruikt gaat worden is het al te laat en kan dit niet meer worden teruggedraaid.

6. Naar de mening van Bits of Freedom is het dan ook noodzakelijk dat een juridisch kader wordt ontwikkeld dat waarborgt dat iedere burger in de informatiemaatschappij de vrijheid behoudt die hij voorheen genoot. Bij het formuleren van beleid op grond van dit uitgangspunt, staat voor Bits of Freedom centraal dat iedere ontwikkeling die inbreuk maakt op de privacy niet beschouwd moet worden als een geïsoleerde ontwikkeling, maar in plaats daarvan beschouwd moet worden als onderdeel van een complex systeem van reeds opgeslagen persoonsgegevens, beschikbare technologieën en bestaande juridische bevoegdheden van databankbeheerders en derden.

7. Dit beschouwende commentaar leidt tot de volgende aanbevelingen.

Veiligheid databanken zou verder moeten worden gewaarborgd

8. Het is van groot belang dat de vele databanken met persoonsgegevens die op dit moment bestaan en nog zullen worden aangelegd voldoende veilig zijn. Deze bevatten vaak zeer privacy-gevoelige gegevens. Verspreiding van deze gegevens is onwenselijk en zoals hierboven opgemerkt is het vaak moeilijk de verspreiding van deze informatie ongedaan te maken als deze informatie eenmaal openbaar is gemaakt.

9. Het is echter niet vanzelfsprekend dat deze databanken, voldoende veilig zijn. Het goed beveiligen van databanken vergt een investering in tijd en geld. Beheerders van databanken

zullen deze investering niet altijd willen maken. De WBP schrijft weliswaar voor dat de verantwoordelijke en een eventuele bewerker passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen (artt. 13 en 14 WBP), maar de WBP stelt geen effectieve sanctie op overtreding van dit voorschrift.

10. In de praktijk zijn veel van deze databanken dan ook niet veilig. Geregeld is in het nieuws te lezen over USB-sticks, laptops en CD's met omvangrijke privacy-gevoelige databanken die kwijt zijn geraakt en in handen van onbevoegden zijn gekomen, of over organisaties die via hun website per ongeluk interne databanken ter beschikking stellen aan de buitenwereld.

11. Bovendien is het van belang dat als er een breuk is in de beveiliging van deze databanken, waardoor daarin opgeslagen persoonsgegevens mogelijk in de openbaarheid komen, de betrokkenen daarvan op de hoogte worden gesteld. Alleen dan kunnen betrokkenen immers maatregelen nemen om misbruik van hun persoonsgegevens te voorkomen. Zij kunnen dan bijvoorbeeld creditcards blokkeren, hun wachtwoorden aanpassen etc.

12. Het is echter ook niet vanzelfsprekend dat zo snel mogelijk nadat een breuk in een databank is geconstateerd, betrokkenen hiervan op de hoogte worden gesteld. Dit kan immers leiden tot reputatieschade, schadeclaims etc.

13. Bits of Freedom beveelt daarom de volgende maatregelen aan om de veiligheid van databanken met persoonsgegevens te waarborgen:

    - Ten eerste zouden artikel 13 en 14 WBP moeten waarborgen dat indien de gehanteerde beveiligingsmaatregelen tegen verlies of onrechtmatige verwerking zijn doorbroken, de verantwoordelijke zodra hij dit vaststelt, de betrokkenen hiervan op de hoogte stelt. Daarbij zou rekening moeten worden gehouden met de aard van de gegevens die zijn gecompromitteerd en de ernst van de breuk, om te waarborgen dat dit instrument effectief blijft. Bovendien zou deze meldplicht niet moeten leiden tot extra verzameling van contactgegevens; de vormgeving hiervan zou nader moeten worden onderzocht.
      Deze zogenoemde “meldplicht datalekken” is overigens al in meerdere landen geïntroduceerd, waaronder onlangs in Duitsland (zie onder meer het rapport “Melding Maken” van Research voor Beleid, gepubliceerd op 17 april 2009, voor een deeloverzicht hiervan). Op Europees niveau wordt deze meldplicht datalekken in het kader van de herziening van de ePrivacy-richtlijn (2002/58/EG) ook overwogen, maar die zou slechts gelden voor een beperkte sector. Bovendien pleit de Artikel 29-werkgroep voor een vergelijkbare meldplicht (zie opinie 1/2009 van 10 februari 2009). In 2005 is middels een motie opgeroepen tot invoering hiervan in Nederland door Van Dam (PvdA) en Gerkens (SP).

- Ten tweede zouden verantwoordelijken voor databanken met persoonsgegevens periodiek de veiligheid van de databanken waarin deze persoonsgegevens zijn opgeslagen moeten laten controleren door een auditor, die hierover een rapport uitbrengt. Dit rapport zou gepubliceerd moeten worden via de daartoe geëigende kanalen, zoals de website van de verantwoordelijke. Daarbij zou naar frequentie en grondigheid van het onderzoek onderscheid gemaakt kunnen worden tussen databanken met "gewone" persoonsgegevens en databanken met "gevoelige" persoonsgegevens.
- Ten derde zou bij de veiligheid van databanken (en dus de beoordeling daarvan) de voorkeur moeten worden gegeven aan oplossingen die de optimale bescherming van de privacy reeds bij het ontwerp hiervan als technische eis stellen ("privacy by design"). Ten aanzien van dit punt kan Bits of Freedom zich vinden in het rapport van de Commissie Veiligheid en Persoonlijke Levenssfeer ('**Commissie Brouwer**").
- Tot slot zou het CBP de bevoegdheid moeten krijgen om in geval van overtreding van artikel 13 en 14 een afschrikwekkende boete op te leggen. Deze bevoegdheid ontbreekt op dit moment.

14. Voor de goede orde merkt Bits of Freedom op dat zelfs als de veiligheid van een databank met persoonsgegevens gewaarborgd is, dit niet automatisch betekent dat het aanleggen van die databank en het daaruit opvragen van gegevens, ook acceptabel is. Grote terughoudendheid bij de aanleg en bevraging van databanken met persoonsgegevens is op zijn plaats, ook als deze goed beveiligd zijn.

Een privacy effect rapportage zou moeten worden geïntroduceerd

15. Zoals hierboven is opgemerkt, dient iedere ontwikkeling die inbreuk maakt op de privacy niet op zich beschouwd te worden, maar in plaats daarvan beschouwd te worden als onderdeel van een complex systeem van persoonsgegevens, technologieën en bevoegdheden dat ook in de toekomst nog zal bestaan en zich verder zal ontwikkelen.

16. Door op die manier een ontwikkeling te beschouwen, kan beter in kaart worden gebracht in hoeverre deze ontwikkeling een effect heeft op de privacy en de daarmee samenhangende individuele vrijheid, en kan bovendien meer inzicht worden verkregen in de complexe interactie tussen de verschillende ontwikkelingen binnen deze systemen.

17. Bij de introductie van de wet- en regelgeving die de afgelopen jaren is ingevoerd, is onvoldoende op structurele basis onderzoek gedaan naar het effect van deze wetten op de privacy. Soms wordt de verenigbaarheid van wet- en regelgeving met de Grondwet en het EVRM wel besproken, maar de effecten op de privacy worden nooit systematisch in kaart gebracht. Dit hangt samen met de conclusie van de Adviescommissie Informatiestromen

Veiligheid, dat geen "overzicht beschikbaar is van toepasselijke wetgeving ten aanzien van bevoegdheden en verantwoordelijkheden op het gebied van inwinnen en verschaffen van gegevens ten behoeve van het veiligheidsdomein" (zie rapport "Data voor Daadkracht", 1 september 2007).

18. Een oplossing die in andere landen is gekozen om op meer structurele basis te onderzoeken wat de effecten van wet- en regelgeving op de privacy zijn, is het verplicht stellen van een "privacy effect rapportage". Zo moet de overheid in de Verenigde Staten en Canada bij het nemen van bepaalde maatregelen een "Privacy Impact Assessment" opstellen, waarin de gevolgen voor de privacy van deze regelgeving worden bestudeerd. In Nederland is een dergelijk instrument al in gebruik om "het milieubelang een volwaardige plaats te geven in besluitvorming" (aldus het Ministerie van VROM op haar website): een milieu effect rapportage is verplicht bij de bouw van olieraffinaderijen, kerncentrales, chemische installaties etc.

19. Bits of Freedom beveelt daarom aan om bij wet voor te schrijven dat ieder voorstel tot wet- en regelgeving dat een substantiële inmenging vormt van het grondrecht op privacy zoals bedoeld in artikel 8 EVRM, vergezeld wordt van een "privacy effect rapportage". Daarin zou onderzocht moeten worden wat het effect van deze maatregel zou zijn op de privacy. Overigens kan ook al zonder dat dit wettelijk verplicht is, door het Ministerie van Justitie een pilot worden gestart om hiermee ervaring op te doen. Bovendien kan alvast opdracht gegeven worden tot het doen van een onderzoek naar de implementatie van een dergelijke verplichting tot het opstellen van privacy effect rapportage.

20. Een hiermee samenhangend instrument dat Bits of Freedom aanbeveelt, is om bij wet voor te schrijven dat toekomstige overheidsmaatregelen die een substantiële inmenging vormen op de privacy, beperkt worden in de tijd (een zgn. '*sunset clause*"). Na afloop hiervan kan vervolgens worden onderzocht of deze maatregelen voor voortzetting vatbaar zijn.

21. Voor de goede orde merkt Bits of Freedom ook hier op, dat als een privacy effect rapportage ten aanzien van een bepaalde maatregel is opgesteld of is besloten tot voortzetting van een bepaalde wet, dit niet automatisch betekent dat het nemen van die maatregel ook acceptabel is. Grote terughoudendheid bij het nemen van privacy-inbreukmakende maatregelen is op zijn plaats, ook als onderzoek is gedaan naar de effecten hiervan.

Handhavingsbevoegdheden CBP moeten worden uitgebreid

22. Het CBP heeft op dit moment slechts zeer beperkte bevoegdheden om de WBP te handhaven. Zij kan een last onder bestuursdwang opleggen en een boete van EUR 4.500

per overtreding opleggen bij het overtreden van de meldplicht. Deze boete is heel laag en bovendien beperkt tot slechts een soort overtreding. Hierdoor heeft de WBP onvoldoende afschrikwekkend effect.

23. Bits of Freedom beveelt daarom aan om de bevoegdheden van het CBP uit te breiden:

- De boetemogelijkheid zou mede omzet-afhankelijk moeten worden gemaakt, zoals de boetebevoegdheid van de NMa en OPTA, en het maximum hiervan zou hoger moeten worden gesteld, zodat hiervan een voldoende afschrikwekkend effect uitgaat.
- Bovendien beveelt zij aan om de boetemogelijkheid uit te breiden tot andersoortige overtredingen. Daarbij zouden met name overtredingen van het verwerkingsverbod (vgl. artt. 6, 8, 9 en 11 e.a.), de beveiligingsplicht (artt. 13 en 14) en de de informatieplicht (hfdstk. 5) hiervoor in aanmerking kunnen komen.

24. Bits of Freedom kan zich overigens voorstellen dat dit wel begeleid zou moeten worden met maatregelen om de rechtszekerheid voor verantwoordelijken te vergroten, gelet op de open normen van de WBP.

Tot slot: overige punten

25. Tot slot zij opgemerkt dat de aanbevelingen van Bits of Freedom grotendeels zijn toegesneden op de context van deze brief: namelijk de evaluatie van de WBP. Volledigheidshalve merkt zij een aantal punten op die buiten de context van deze brief vallen, maar wel de nodige aandacht verdienen.

26. Ten eerste vindt Bits of Freedom (i) de toenemende hoeveelheid databanken met persoonsgegevens die door de overheid en het bedrijfsleven worden aangelegd, (ii) de toenemende koppeling tussen deze databanken en (iii) de toenemende bevoegdheden van opsporings-, inlichtingen- en veiligheidsdiensten om hieruit gegevens op te vragen, een zeer zorgwekkende ontwikkeling. Nederland kan hierdoor in korte tijd in een "controlemaatschappij" veranderen, waarin het leven van de burger constant wordt bijgehouden en de vrijheid van de burger onomkeerbaar is ingeperkt. Deze ontwikkelingen staan op gespannen voet met het grondrecht op privacy en zijn om de in deze brief kort toegelichte redenen onwenselijk.

27. Ten tweede vindt Bits of Freedom de manier waarop het debat over de spanning tussen privacy en veiligheid wordt gevoerd, te eenzijdig. De stelling dat een burger die "niets te verbergen heeft, ook niets te vrezen heeft", heeft een stevige plaats in het debat verworven. Deze stelling staat een open discussie over de hierboven geschetste lange-termijn effecten van privacy-inbreukmakende maatregelen echter in de weg.

28. In verband hiermee vindt Bits of Freedom dat de stelling in het rapport van de Commissie Brouwer, dat "indien noodzakelijk voor de veiligheid, je moet delen" voorbijgaat aan de plicht van de overheid om de meest proportionele opsporingsmaatregel toe te passen. "Professionals" (zoals de Commissie Brouwer deze noemt) zouden slechts moeten delen als (i) de veiligheid van individuen concreet wordt bedreigd, (ii) het delen van persoonsgegevens dat risico kan wegnemen en (iii) – deze eis ontbreekt in het advies van de Commissie Brouwer – er geen andere, minder inbreukmakende mogelijkheid is om dit risico weg te nemen.

29. Tot slot herkent Bits of Freedom de constatering uit het rapport "Wat niet weet, wat niet deert" van de Rijksuniversiteit Groningen e.a., dat de burger onvoldoende gebruik maakt van de rechten die hem toekomen (zoals het inzagerecht op grond van artikel 35 WBP e.v.). De overheid zou een bijdrage kunnen leveren aan de bewustwording van de burger van zijn rechten, door hierover uitgebreider voorlichting te geven.

Over Bits of Freedom

30. Bits of Freedom verdedigt burgerrechten in de digitale wereld, waaronder het recht op privacy. De organisatie staat onder leiding van Ot van Daalen. Het bestuur van Bits of Freedom bestaat uit Doke Pelleboer (ex-directeur van XS4ALL), Joris van Hoboken (onderzoeker bij het Instituut voor Informatierecht van de Universiteit van Amsterdam) en Karianne Thomas (advocaat bij advocatenkantoor Van Doorne).

31. Bits of Freedom vertrouwt erop u hiermee voldoende te hebben geïnformeerd. Ik houd mij graag beschikbaar voor nader overleg, mocht hieraan behoefte bestaan. Ik ben bereikbaar via bovenstaande contactgegevens.

Hoogachtend,

Ot van Daalen