BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

NEDERLAND: EEN VRIJE EN BETROUWBARE INFORMATIESAMENLEVING

MANIFEST VOOR DIGITALE VRIJHEID

NEGEN PROGRAMMAPUNTEN

VOOR DE VERKIEZINGPROGRAMMA'S VAN 2010

over Bits of Freedom

Stichting Bits of Freedom verdedigt burgerrechten in de digitale wereld. Zij richt zich op twee grondrechten: privacy en communicatievrijheid. Haar activiteiten omvatten het voeren van een constructieve lobby en het organiseren van publiekscampagnes. Zie www.bof.nl.

Contact

Axel Arnbak, axel.arnbak@bof.nl, +31(0)624534440
Ot van Daalen, ot.vandaalen@bof.nl, +31(0)65438668

MANIFEST VOOR DIGITALE VRIJHEID

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Nederland: een vrije en betrouwbare informatiesamenleving

Digitale technologie is de zuurstof voor de Nederlander van de 21e eeuw. Vrijwel iedere Nederlander heeft een computer, een mobiele telefoon en breedbandinternet en maakt daar volop gebruik van. Wij drijven handel via innovatieve diensten als Marktplaats. Wij doen massaal belastingaangifte via internet. Wij werken samen aan de meest omvangrijke encyclopedie ooit, Wikipedia. Wij leggen nieuwe zakelijke contacten en onderhouden oude vriendschappen via sociale netwerken. Wij delen kennis, cultuur en meningen via Twitter. Wij bouwen via internet aan onze democratie en vragen aandacht voor onderdrukking in andere landen, zoals Iran. Digitale technologie heeft onze maatschappij ingrijpend veranderd en iedere burger ongekende vrijheid gegeven.

Maar Bits of Freedom constateert dat wij die vrijheid in sneltreinvaart verliezen. Een open en vrij internet staat onder druk, onder meer door vergaande plannen om miljoenen Nederlanders in één klap tot crimineel bestempelen.[1] Bij grote informatiseringsprojecten staat het belang van burgers niet centraal, en projecten als het EPD en de OV-chipkaart roepen dan ook veel maatschappelijke weerstand op. En digitale technologie wordt steeds vaker ingezet om onverdachte burgers in de gaten te houden, zonder dat nut en noodzaak is aangetoond.

Wij bevinden ons op een maatschappelijk kantelpunt: de politieke keuzes van nu zullen het lot van de Nederlandse informatiesamenleving in de komende decennia bepalen. Kiezen wij voor een open en vooruitstrevende Nederlandse informatiesamenleving waarin individuele vrijheid wordt verdedigd, waarin dienstenontwikkeling wordt gestimuleerd en waarin een gunstig digitaal vestigingsklimaat ontstaat? Of kiezen wij voor een maatschappij waar digitale technologie wordt ingezet om burgers vergaand te controleren en innovatie wordt afgeremd?

Politieke partijen moeten hun verantwoordelijkheid nemen en kiezen voor een vrije en betrouwbare informatiesamenleving, door de volgende negen programmapunten op te nemen in hun verkiezingsprogramma's voor 2010:

- **niemand mag van internet worden afgesloten**
- **er moet een robuust beleid op het gebied van netwerkneutraliteit komen**
- **de overheid moet cultuur stimuleren zonder burgers te controleren**
- **privacy by design moet het uitgangspunt zijn bij grote informatiseringsprojecten**
- **databanken moeten goed beveiligd worden**
- **bestaande grote informatiseringsprojecten moeten worden heringericht**
- **effectiviteit moet centraal staan bij de bestrijding van criminaliteit en terrorisme**
- **rechtsbescherming en controle moeten integraal onderdeel zijn van systemen**
- **surveillance-systemen moeten aan kritisch onderzoek worden onderworpen**

1 TNO, IViR, SEO, *Ups and downs. Economische en culturele gevolgen van file sharing voor muziek, film en games*, 12 jan. 2009, p. 4, te raadplegen via: http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs.pdf.

MANIFEST VOOR DIGITALE VRIJHEID

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Nederland moet een vrij en open internet beschermen

Een vrij en open internet is cruciaal voor de toekomst van Nederland. Iedereen moet kennis en cultuur kunnen delen met anderen, nieuwe diensten kunnen ontwikkelen en daarvan profiteren, en zich kunnen aansluiten bij de groep die bij hem of haar past. Dat is goed voor de kenniseconomie, goed voor het onderwijs, goed voor sociale cohesie en goed voor het mediabeleid. Nederland is van oudsher de bakermat van vrijheid en tolerantie, en heeft daar veel profijt van gehad. Met de volgende programmapunten zet Nederland deze traditie voort in de 21e eeuw:

- **Niemand mag van internet worden afgesloten** De overheid moet uitdrukkelijk afstand nemen van regelgeving – zoals voorgesteld in de geheime ACTA-onderhandelingen[2] – op grond waarvan mensen van internet worden afgesloten als zij drie keer een vermeende inbreuk hebben gemaakt op auteursrecht. Afsluiting betekent uitsluiting: van werk, onderwijs, overheidsdiensten, cultuur en gemeenschap. En niet alleen een overtreder, maar iedereen achter dezelfde verbinding – ook het gezin en collega's – worden door een afsluiting getroffen.

- **Een robuust beleid op het gebied van netwerkneutraliteit** De overheid moet het beginsel van netwerkneutraliteit waarborgen, door (i) Internet Service Providers (ISPs) te verbieden zich te bemoeien met het internetverkeer van hun abonnees en door (ii) internet niet te (laten) filteren.[3] Dat is ook belangrijk voor de economie, want zo blijft er op het internet een level-playing-field voor alle grote én kleine dienstenaanbieders en wordt voorkomen dat ISPs de concurrentie vervalsen. Het is ook goed voor sociale cohesie, want het zorgt ervoor dat iedereen toegang heeft tot *hetzelfde* internet.

- **Cultuur stimuleren zonder burgers te controleren** De burger mag niet het slachtoffer worden van repressieve maatregelen die tot doel hebben om verouderde bedrijfsmodellen van de contentindustrie in leven te houden. Steeds verdergaande handhaving van auteursrecht criminaliseert miljoenen Nederlanders en vereist uiteindelijk dat álle internetgebruikers – inclusief het bedrijfsleven, minderjarigen en senioren – continu worden gemonitord, laptops worden gecheckt etc.[4] De productie en verspreiding van cultuur – het uiteindelijke doel van het auteursrecht – wordt met zulke maatregelen niet bevorderd.[5] De overheid moet afstand nemen van repressieve handhaving, het downloadverbod niet introduceren, en de ontwikkeling van nieuwe bedrijfsmodellen die aansluiten bij de digitale realiteit aanmoedigen.

---

2 Het Anti-Counterfeiting Trade Agreement. Meer informatie is te raadplegen via: https://www.bof.nl/category/acta/.

3 Bits of Freedom, *Position paper Netwerkneutraliteit*, 5 jan. 2010, te raadplegen via: https://www.bof.nl/live/wp-content/uploads/2010/01/netwerkneutraliteit-def.pdf.

4 Bits of Freedom, *Kamerbriefing Downloadverbod*, 9 dec. 2009, te raadplegen via: https://www.bof.nl/live/wp-content/uploads/2009/12/filesharing-kamerbriefing-141209.pdf. Zie tevens het wetenschappelijk onderzoek onder voetnoot 1.

5 TNO, IViR, SEO, *Ups and downs. Economische en culturele gevolgen van file sharing voor muziek, film en games*, 12 jan. 2009, p. 4, te raadplegen via: http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs.pdf. De hoofdconclusie van het rapport luidt, dat “de economische effecten van file sharing op de Nederlandse welvaart op de korte en de lange termijn sterk positief zijn.”

De burger moet centraal staan bij informatiseringsprojecten

Grote informatiseringsprojecten zijn alleen duurzaam, als het belang van de burger bij deze systemen centraal staat. De OV-chipkaart, het EPD en het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) zijn ontwikkeld met de beste intenties, maar door privacyschendingen, systeemdwang en onwenselijke toegang tot privé-gegevens stuitten dit soort systemen op veel maatschappelijke weerstand en wordt de belastingbetaler op onvoorziene kosten gejaagd.[6] De volgende programmapunten zijn essentieel om de burger centraal te stellen bij de ontwikkeling van grote informatiseringsprojecten:

- **Privacy by design** De bescherming van privacy dient altijd het uitgangspunt – en niet een sluitpost – te zijn bij het ontwerp van grootschalige informatiseringsprojecten. Deze systemen moeten niet meer informatie opslaan dan strikt noodzakelijk (dataminimalisatie), alleen voor een vooraf beschreven doel (doelspecificatie), anoniem zijn waar mogelijk (anonimisering), zo kort mogelijk worden opgeslagen (termijnverkorting), de burger inzicht bieden in het gebruik én toekomstig gebruik van zijn privé-gegevens (transparantie) en alleen de burger laten bepalen wat er met de gegevens gebeurt en de mogelijkheid geven om de gegevens te vernietigen (zelfbeschikking). Bovendien moet duidelijk worden vastgelegd wie er toegang hebben tot de data (toegangscriteria).
- **Goede beveiliging van databanken** Grote databanken met privé-gegevens van miljoenen burgers, bedrijven en instellingen moeten met de grootste zorgvuldigheid worden beveiligd, en geregeld aan audits worden onderworpen. Met een wettelijke 'meldplicht datalekken' dient de overheid zichzelf en andere instanties te verplichten beveiligingslekken in datasystemen te melden aan het College Bescherming Persoonsgegevens en aan betrokkenen.[7] Alleen zo zullen instanties de beveiliging van databanken serieus nemen. Alleen zo kan dataopslag op voldoende draagvlak rekenen en kan het vertrouwen in digitale technologie wordt vergroot.
- **Herinrichting systemen in ontwikkeling** De overheid moet systemen die op dit moment worden ontwikkeld, zoals het EPD en de OV-chipkaart, inrichten volgens de beginselen die hierboven zijn beschreven.

6 Bits of Freedom, *Inbreng Project dataretentie*, 30 nov. 2009, te raadplegen via: https://www.bof.nl/live/wp-content/uploads/2010/01/Bits-of-Freedom-Inbreng-Voorstel-definitie-HNAW-301109.pdf.

7 Bits of Freedom, *Position paper Meldplicht datalekken*, 25 jan. 2010, te raadplegen via: https://www.bof.nl/live/wp-content/uploads/2010/01/datalekken-def.pdf.

Een rationeel en effectief beveiligingsbeleid

Burgers verwachten van hun overheid een rationeel en effectief beleid ter bestrijding van criminaliteit en terrorisme, en geen symboolpolitiek. De laatste jaren heeft Nederland digitale technologie gebouwd en ingezet om miljoenen onverdachte burgers te controleren, terwijl het nut en de noodzaak van deze maatregelen onvoldoende is onderzocht. Deze maatregelen zijn in strijd met de grondrechten van iedere Nederlander, duur en ineffectief. Bovendien kunnen zij in de toekomst misbruikt worden. De volgende programmapunten zijn essentieel voor een beveiligingsbeleid van een betrouwbare informatiesamenleving:

- **Effectiviteit moet centraal staan** De overheid dient wet- en regelgeving waarmee miljoenen onverdachte Nederlanders in de gaten worden gehouden pas na een grondige analyse in te zetten. Slechts in uitzonderlijke gevallen mogen grondrechten wijken voor surveillance systemen die op de gehele bevolking worden ingezet (noodzaak). De effectiviteit van dit soort systemen moet dan *vooraf* zijn aangetoond, en de nadelen moeten helder in kaart gebracht zijn (Privacy Impact Analyses). Wet- en regelgeving die de privacy van alle burgers vergaand beperken, gelden slechts voor een in de tijd beperkte periode (horizonbepaling). Vóór het verstrijken van deze periode worden de maatregelen grondig geëvalueerd (evaluatie), en zij worden alleen gecontinueerd als de effectiviteit voor het bereiken van het doel van de wet- en regelgeving is aangetoond (effectiviteit). Er dient controle te zijn op de uitvoering van de bevoegdheden door overheidsinstanties (controle en auditering).[8]
- **Rechtsbescherming en controle** De overheid moet mogelijkheden van rechtsbescherming in het leven roepen, waarmee burgers kunnen opkomen tegen besluiten die worden genomen op grond van gegevens die over hen bekend zijn. Zo kunnen de onwenselijke gevolgen van identiteitsdiefstal zo snel mogelijk worden beperkt. De wettelijke notificatieplicht – op grond waarvan burgers op de hoogte worden gesteld van het feit dat zij onderwerp van een opsporingsonderzoek zijn (geweest) – moet nageleefd worden.
- **Bestaande surveillancesystemen moeten kritisch worden onderzocht** De afgelopen jaren is Nederland getuige geweest van een wildgroei aan surveillance-systemen: telecomgegevens, bodyscanners, vingerafdrukken, PNR-gegevens, financiële gegevens en kentekengegevens van miljoenen Nederlanders worden opgeslagen en opgevraagd. Dit soort systemen zijn ingevoerd als symboolpolitiek naar aanleiding van een reeds gebeurde aanslag, en het onderzoek naar de noodzaak van dit soort systemen laat vaak te wensen over – als dit onderzoek al heeft plaatsgevonden. Nederland moet de bestaande surveillancesystemen aan een kritisch onderzoek onderwerpen, en opheffen tenzij nut en noodzaak door onafhankelijke experts worden vastgesteld. Ook dan moeten dit soort systemen aan periodieke evaluatie onderworpen blijven.

8 Zoals besproken tijdens de Expertbijeenkomst gegevensbescherming in de Eerste Kamer: *Kamerstukken I* 2007/08, 31200 VI, nr. F, p. 35 ev, 20 mrt. 2008, te raadplegen via: http://ikregeer.nl/document/KST118933.