

Als Trump het wil, staat Nederland stil

Op 27 januari 2026 organiseert de Kamercommissie Digitale Zaken een rondetafelgesprek over de beoogde overname van Solvinity, en de gevolgen daarvan voor de vertrouwelijkheid, integriteit en beschikbaarheid van DigiD. Bits of Freedom zet zich als digitale burgerrechtenorganisatie al meer dan vijftientig jaar in voor het recht op privacy en communicatievrijheid in Nederland. Vanuit onze technische en juridische expertise maken we graag van de gelegenheid gebruik om een aantal aandachtspunten te delen.

1. Onze zelfbeschikking

Voor het autonoom kunnen beslissen en handelen over essentiële zaken als onze economie, democratie en samenleving, moeten we in grote mate de baas zijn over de infrastructuur waar de samenleving op draait. In grote mate, want digitale autonomie betekent niet dat elke digitale dienst en elk stukje digitale infrastructuur ontworpen, gemaakt en beheerd moet worden op eigen grondgebied door de Nederlandse overheid. Gelukkig maar, want behalve niet nodig en niet wenselijk, is het ook niet realistisch.

De relatie tussen burgers en haar overheid wordt steeds vaker digitaal gemedieerd, en DigiD speelt daarin een cruciale rol. **In 2021 had DigiD 16,5 miljoen actieve gebruikers, samen goed voor zo'n 557 miljoen transacties.** Toch zijn we op het punt gekomen dat het zou kunnen dat DigiD door een Amerikaans bedrijf wordt beheerd. Wat zijn daarvan de risico's en wat moet er nu gebeuren?

2. Amerika's digitale macht: infrastructuur en data

Er is de afgelopen jaren al veel gezegd over onze afhankelijkheid van Amerikaanse digitale diensten. Microsoft, Amazon en Google beheren naar schatting zo'n driekwart van de data die in Nederland wordt opgeslagen. En naar schatting maken 8 uit 10 Nederlandse kantoren gebruik van Microsoft Office. Big Tech heeft controle over onze smartphones (iOS en Android) en beheert onze communicatieinfrastructuur.

Naast het beheren van onze digitale infrastructuur, heeft Big Tech ook decennia aan historische data en geautomatiseerde, real-time toegang tot ons digitale leven, economie en politiek. En onder Trumps bewind neemt de datahonger en surveillanceinfrastructuur alleen maar toe. Palantir, het controversiële big data bedrijf met nauwe banden met de CIA, speelt daarbij een belangrijke rol. Palantir is niet meer weg te denken uit het Amerikaanse veiligheidsdomein, maar ook in Europa heeft het gebruik van Palantir door overheden een vlucht genomen. Het bedrijf verwerkt en genereert daarmee steeds meer informatie over Europeanen. Zorgelijk, wanneer je bedenkt dat mede-oprichter Alex Karp het werk van Palantir beschrijft als "the finding of hidden things".

Met andere woorden: de Amerikaanse overheid heeft momenteel toegang tot de meest omvangrijke surveillanceinfrastructuur en datasets die de wereld ooit heeft gekend.

3. DigiD laat zien hoe kwetsbaar onze afhankelijkheid ons maakt

De casus DigiD laat, helaas, in een notendop zien wat de VS met die infrastructurele- en datamacht kan doen. Wanneer een Amerikaanse partij het beheer van DigiD zou doen, kan deze worden gedwongen de dienstverlening te staken waardoor we van de ene op de andere dag niet meer kunnen inloggen. Daarnaast heeft de Amerikaanse overheid via deze partij toegang tot grote hoeveelheden informatie (vergeet niet: honderden miljoenen DigiD transacties per jaar) en kan zij deze combineren met andere datasets waar ze over beschikt.

Juridische waarborgen beschermen niet tegen een overheid die het recht en internationale verdragen niet respecteert. Maar ook al zou de Amerikaanse overheid dat wel doen, ook dan kan zij, netjes binnen het Amerikaanse wettelijke kader, toegang verkrijgen tot de IT-infrastructuur en data die bij Amerikaanse bedrijven staat, ook wanneer deze zich fysiek in Europa bevinden en ook wanneer dit strijdig is met Europese wetgeving.

4. Wat moet er gebeuren?

4.1 Nu

Met betrekking tot DigiD:

- **Maak de analyse.** Er moet een quickscan worden uitgevoerd naar alternatieven voor Solvinity's dienstverlening, en een risicoanalyse worden uitgevoerd door de AIVD;
- **Trek een plan.** Wanneer de risico's niet in voldoende mate gemitigeerd kunnen worden, moet de overname van Solvinity worden tegengehouden of moet DigiD bij Solvinity worden weggehaald voordat de overname een feit is.
- **Geef openheid van zaken.** Het vertrouwen in DigiD kan hersteld worden wanneer de overheid burgers goed informeert over de realistische risico's, de mitigatiemaatregelen, en wat dit voor burgers betekent.

Met betrekking tot onze digitale afhankelijkheid:

- **Herken de crisis.** DigiD is een van de vele voorbeelden waarbij we gevaarlijk afhankelijk zijn van de Verenigde Staten. Het water staat ons niet aan de lippen; we staan al onder water en Trump houdt zijn duim in de dijk. Maar hoe lang nog? Crises worden in het [Nationaal Handboek Crisisbeheersing](#) gedefiniëerd als "situaties [...] die de veiligheid van onze samenleving bedreigen en die vragen om urgente en gerichte aandacht". De nationale crisisstructuur kan worden geactiveerd in situaties "waarbij de nationale veiligheid in het geding is of kan zijn of [...] waarbij van een grote uitwerking op de maatschappij sprake is of kan zijn." De nationale veiligheid is op haar beurt in het geding "als een of meer vitale belangen van de Nederlandse staat en/of samenleving zodanig bedreigd worden dat sprake is van (potentiële) maatschappelijke ontwrichting". Het [Nederlands Instituut Publieke Veiligheid \(NIPV\)](#) legt vast op welke soorten crises wordt voorbereid. Cybersecurity is er één van. Hoewel Bits of Freedom er niet voor pleit de nationale crisisstructuur te activeren, pleiten we wel voor reflectie op de noodzakelijkheid en mogelijkheid hiertoe, bijvoorbeeld door het laten uitvoeren van een Situatieschets en Duiding (SenD). Zonder urgentie geen actie.

4.2 Morgen

Daarnaast is het belangrijk om op te merken dat dit niet de eerste keer is dat we hier zijn, en dat dat aangeeft dat er één of meerdere weeffouten zijn die geaddressiseerd moeten worden.

- **Maak een bouwplan, geen artist impression.** Hoewel de staatssecretaris in zijn antwoord op kamervragen aangeeft dat de Visie Digitale Autonomie (VDA) “strategische bouwstenen [benoemt] die nodig zijn om te komen tot een digitale overheid die grip heeft op autonomie”, beschrijft de VDA ons inziens niet de stenen, maar een conceptuele impressie van de gewenste toekomst. Prachtig om de verbeelding mee te prikkelen, maar wat we nu nodig hebben is een bouwtekening waarmee een aannemer aan de slag kan. De kamer mag met dit document dus geen genoegen nemen. De analyse over welke digitale infrastructuur als eerst in eigen beheer moet worden gebracht, en hoe we dat gaan doen, ontbreekt. De Kamer moet afdwingen dat het kabinet deze analyse oplevert.
- **Stop met migreren.** Mensen kijken machteloos toe terwijl de Belastingdienst naar Microsoft migreert, hun gemeente een TikTok-account opent, de politie slimme deurbellen van Amazon promoveert, en elke burger die bij de AIVD solliciteert bekend wordt gemaakt aan Google. De overheid moet stoppen met het migreren naar, en het in gebruik nemen van, Amerikaanse diensten.
- **Verklein onze afhankelijkheid van DigiD.** Idealiter is er een verscheidenheid aan manieren waarop, en diensten waarmee, mensen zich kunnen identificeren. Denk publieke en private initiatieven, maar denk ook aan diensten die wel en niet afhankelijk zijn van de infrastructuur van Apple en Google (zoals het geval is wanneer DigiD alleen nog maar via de app gebruikt kan worden). Ook moet het altijd mogelijk zijn voor mensen om de overheid offline te benaderen.
- **Ontwikkel meer inzicht in de overlap digitale zaken en veiligheid.** Het veiligheidsdomein digitaliseert in rap tempo, en digitale zaken komen steeds vaker met (nationale) veiligheidsissues. Het thema veiligheid ligt onterecht buiten de scope van deze Kamercommissie.