Vertrouwen door transparantie

Transparantie, en daarmee het vertrouwen in een digitale oplossing, zijn **niet** geborgd in het conceptbesluit. Identiteitsmiddelen vormen niet alleen een fundament onder de digitale samenleving maar inmiddels ook voor de fysieke wereld, waar we ons bijvoorbeeld met smartphones authentiseren. Wie we zijn, en met wie we te maken hebben is een fundamenteel aspect in ieders leven. Op termijn is alles digitaal gefaciliteerd, ook belangrijke levensmijlpalen waar in emotionele context administratieve processen moeten worden doorlopen (huwelijken, scheidingen, overlijden etc.). Vertrouwen in een digitale oplossing voor dit soort momenten is de sleutel en wordt dus alleen maar belangrijker. Zo'n fundamentele dienst en infrastructuur dient volledig transparant geëxploiteerd te worden. Hier zijn gedeelde of onduidelijke belangen van de aanbieder absoluut niet op hun plaats. Daarnaast dient de broncode van de geleverde oplossingen open-source te zijn, zodat verbeteringen aan veiligheid, functionaliteit en gebruiksgemak niet afhankelijk worden van een enkele dominante partij. Iedereen moet dit kunnen controleren en waar nodig aan bij kunnen dragen. In het licht van het fundamentele karakter van deze toe-passingen voor de samenleving is deze aanvullende eis onontkoombaar.

Centrale opslag is onnodig

Het gebruik door aanbieders van *centrale opslag* van persoonsgegevens aan de éne kant en gebruiksgegevens aan de andere kant wordt in het toetsingskader niet uitgesloten; dit is uiterst problematisch. Centrale opslag levert per definitie meer en grotere risico's op het gebied van be-schik-baar-heid, aanvallen en misbruik, en is niet nodig voor een goed functionerend en veilig middel. Dit bewijzen onder meer IRMA en Sovrin.

Dataminimalisatie

Daarnaast is een centrale data-architectuur niet in lijn met de AVG-eisen ten opzichte van dataminimalisatie. Deze eisen stellen dat dataminimalisatie waar mogelijk zal worden toegepast. De persoons- en gebruiksgegevens zijn dermate gevoelig dat dit aspect niet genegeerd kan worden. Het idee is dat eventuele applicaties voor digitale identiteit in meer dan alleen overheidsscenario's ingezet zullen worden. Het is dan de vraag wat het (juridisch) kader is waaronder een centrale opslag van persoons- en gebruiksgegevens acceptabel is. Wanneer er in de fysieke wereld bij iedere authenticatie-actie (postkantoor, fitnessclub, drankwinkel, etc.) een mannetje over de schouder mee zou kijken en aantekeningen zou maken over de tijd, plaats en gebruikte gegevens, dan zouden we dit lacherig afdoen als een idiote fantasie. Waarom wordt dit in het digitale domein als acceptabel ervaren? Als iets technisch haalbaar is, betekent dat zeker niet dat we dit ook moeten doen, en sowieso niet dat er juridische grond is.

Privacy by design

Een belangrijk deel van de toelichting van het ministerie gaat in op situaties die alleen voorkomen bij een centraal georganiseerd systeem. Bij een decentraal georganiseerd middel is fraude alleen mogelijk met het fysieke middel, het niveau van de gebruiker zelf. Dit beperkt zich dus tot één enkel middel per keer. Het loont

zich derhalve nooit voor grotere, georganiseerde aanvallers of staten. Veiligheid en privacy zijn dan ‘ingebouwd’ in de architectuur. Dat is precies wat de AVG met ‘privacy by design’ beoogt. Zo realiseer je de verplichte scheiding van gegevens van gebruikers en gebruik. Je hoeft bij decentrale dataopslag geen extra regels te stellen aan het personeel dat toegang heeft tot de gegevens. Dit gebeurt automatisch. Er is immers geen sprake van een database (anders dan bij de gebruiker zelf).
Het gebruik van gegevens voor commerciële toepassingen wordt door de Wdo uitgesloten. Maar het concept besluit is veel minder stellig in het vasthouden aan de specifieke doelbinding. Daar waar opslag van gegevens nodig geacht wordt voor het specifieke doel van ‘herstelvermogen’ is een aanvullende eis noodzakelijk dat de daarvoor benodigde gegevens versleuteld zijn opgeslagen en *uitsluitend* door de eindgebruiker kunnen worden ontsleuteld en gebruikt.
Ook is het volledig onduidelijk hoe toezicht en handhaving wordt georganiseerd, zeker wanneer we bedenken dat niets de grote internationale partijen weerhoudt deze diensten te gaan leveren. Het is moeilijk voor te stellen dat we daar effectief kunnen controleren en handhaven. Nogmaals, het vermijden van de centrale databases is de enige manier waarop garanties kunnen worden ingebouwd in het ontwerp.

De Wet digitale overheid is een goede stap in de richting van een veilig en democratische digitale toekomst. Maar op het gebied van de bescherming van onze digitale identiteit worden een aantal kernvoorwaarden gemist qua transparantie en dataopslag. Voorwaarden die cruciaal zijn in het uitvoeren van de kerntaak van de overheid: het beschermen en waarborgen van de nationale en individuele veiligheid en soevereiniteit van alle Nederlanders.