# Kom op voor de publieke zaak in de digitale wereld[1]

Bart Jacobs

Een groot deel van ons dagelijkse leven vindt plaats in de digitale wereld. Maar in die wereld is er nog veel onzeker. Neem online kopen of verkopen. Met wie heeft u als burger te maken? Is de figuur betrouwbaar waarmee u contact denkt te hebben? Hoe worden uw gegevens beschermd? Is iemand die zich online arts noemt echt dokter? Woont die op het opgegeven adres? En hoe oud is die? Allemaal vragen, die getuigen van de behoefte aan digitale zekerheid. Zekerheid die de burger houvast geeft in zijn dagelijkse reis door de digitale wereld.

Maar wie biedt deze zekerheid? De ICT-giganten — de frightful five: Google, Facebook, Amazon, Apple, Microsoft — de leverancier van uw laptop of mobiele telefoon, uw internet of telecomprovider doen dat nauwelijks. Is dit dan een taak voor de overheid? Die boekt op dit terrein vooralsnog weinig succes. Wie neemt het dan op voor de publieke zaak in de digitale wereld? En wie helpt er zekerheid te bieden nu de Nederlandse burger te maken krijgt met een persoonlijke gezondheidsomgeving (PGO)? Zo'n PGO is de digitale omgeving waar medische gegevens van een individuele burger straks kunnen worden opgeslagen. Daar moet de burger op kunnen inloggen. Hoe doet die dat en hoe betrouwbaar, begrijpelijk en privacy-vriendelijk zijn de benodigde technieken? Het is niet de bedoeling dat anderen in uw PGO kunnen.

Om de persoonlijke gezondheidsomgeving zo betrouwbaar mogelijk te maken en zekerheid te bieden, zijn specifieke authenticatie-technieken nodig. Technieken die de rijksoverheid tot nu toe niet aanbiedt, maar gemeentelijke overheden al wel. Neem IRMA. Dat is een digitale identiteit die digitale zekerheid biedt. Het bestaat al meer dan tien jaar en is voortgekomen uit de Digital Securitygroep van de Radboud Universiteit in Nijmegen. Ik ben daar nauw bij betrokken.

[1]Verschenen in: M. van Houdenhoven en J.-H. Zwaveling (red), *Data dilemma's in de zorg. Op weg naar betere oplossingen in het belang van de patiënt*, Bohn Stafleu van Loghum, 2019, p. 127–135.

## Versleuteling

IRMA, voor de duidelijkheid, is een privacy-vriendelijk identiteitsplatform voor zowel authenticatie, versleuteling als ondertekening van uw (medische) gegevens. IRMA is een spin-off van de universiteit die sinds drie jaar ondergebracht is bij een onafhankelijke stichting (Privacy by Design) zonder winstoogmerk. Die stichting zorgt ervoor dat uw digitale identiteit niet langer wordt bepaald door de internationale ICT-giganten. Een utopie? Nee, zolang bedrijven, overheden en burgers meedoen. Ieder vanuit de eigen rol, ten behoeve van onderlinge zekerheid en vertrouwen in de digitale samenleving.

Maar eerst stap één. Voor haar digitale contacten met burgers werkt de Nederlandse overheid, zoals bekend, met het bsn, het burgerservicenummer. Ook de zorg is daarop gebaseerd. Het burgerservicenummer is wettelijk strak gereguleerd. Dat is een goede zaak. Want stel dat Facebook en anderen het bsn als sleutel zouden benutten, dan kan iedereen in Nederland met dat unieke nummer worden getraceerd. Dan wordt er bij elke transactie met Apple of Amazon gevraagd: Laat maar even uw bsn zien. Ook als u iets zoekt op Google Maps. Om dit te voorkomen mag de private sector onze bsn's niet gebruiken.

Stap twee. Stel dat u wilt inloggen op een PGO van, zeg, Philips, dan mag u evenmin uw burgerservicenummer gebruiken, en daarmee niet uw DigiD. Want DigiD is gebaseerd op bsn. Om die reden moet Philips een eigen, privaat inlogmiddel hebben dat van een hoog betrouwbaarheidsniveau dient te zijn om uw gevoelige medische gegevens goed af te schermen. Als u eenmaal op uw PGO bent ingelogd en u uw medische gegevens van het ziekenhuis of uw huisarts wilt ophalen, dan heeft u ineens wel uw bsn nodig. Het ministerie van Volksgezondheid, Welzijn en Sport heeft jarenlang gezegd: 'Dan moet u maar twee inlogmiddelen gebruiken.' Dat wil de PGO-sector natuurlijk niet.

Daarom stap drie. IRMA kan dit allemaal wel. Dan kunt u één middel voor beide zaken gebruiken. Hoe dan? IRMA is gebaseerd op attributen. Attributen zijn persoonlijke kenmerken, zoals: u bent Nederlander, u woont in Eindhoven, dit zijn uw mailadressen en dit is uw burgerservicenummer. Vandaar de naam: IRMA is een afkorting van I reveal my attributes Ik onthul mijn kenmerken. Deze persoonlijke kenmerken staan alleen op uw telefoon, in de IRMA app. Zij zijn uitsluitend zichtbaar voor u als burger; ze staan nergens anders, ook niet in de cloud.

Attributen zijn gekoppeld aan uw persoon, maar u heeft ze niet allemaal voor elke login nodig. Beter gezegd: U laat met IRMA alleen relevante delen van uw identiteit zien, bijvoorbeeld uw naam, geboortedatum en emailadres om in te loggen op uw private PGO, en uw bsn om medische gegevens op te halen uit de publieke zorgsector. Ergens anders, bijvoorbeeld om online een game te spelen, gelden leeftijdsgrenzen: 12, 16, 18 of 21 jaar. Dan laat u alleen het relevante attribuut 'ouder dan 16' zien. Als u een specifieke film wilt zien, dan moet u bewijzen dat u ouder dan 18 bent en lid bent van die club. U gaat akkoord met het onthullen van desbetreffende attributen vanuit uw IRMA-app en dan begint de film. Er zijn nu al IRMA-portals als u contact zoekt met uw zorgverzekeraar en portals voor artsen om via IRMA in te loggen bij gegevens van de patint.

## Privacyvriendelijk

Wie privacyvriendelijk wil inloggen, heeft IRMA nodig. U kunt de gevraagde persoonlijke kenmerken aantonen met de gelijknamige app op uw mobiele telefoon, voorzien van een pincode. De IRMA-app is gratis en wordt verstrekt door de onafhankelijke stichting Privacy by Design. Zodra u de IRMA-app benut en de pincode intikt, ontgrendelt u een digitale kluis met allemaal mapjes met uw persoonsgegevens. Dat is uw persoonlijke digitale paspoort: kleine stukjes informatie over uw leeftijd, adres, volledige naam of geboortedatum enz. Om in te loggen laat u dus selectief verschillende persoonlijke kenmerken zien. Bij dat inloggen komt er een QR-code tevoorschijn (Quick Response). Dat is een tweedimensionale streepjescode, die u kunt scannen met de IRMA-app op uw telefoon. Vervolgens ziet u welke partij om welke kenmerken van u vraagt. U kunt daar dan wel of niet mee akkoord gaan.

IRMA is een Zwitsers zakmes voor digitale identiteit en zekerheid. De opzet omvat drie technische basisbegrippen: authenticatie, versleuteling en ondertekening. Authenticatie staat voor bewijzen wie je bent. Het regelt uw online toegang als u daar recht op heeft. Versleuteling is het mechanisme om de inhoud van berichten te verhullen, zodat alleen de juiste ontvanger erbij kan. Digitale ondertekening, tenslotte, betekent dat de persoon die ondertekent zich committeert aan de inhoud van een digitale boodschap.

Authenticatie, versleuteling en ondertekening vormen de basis voor een betrouwbare ICT-infrastructuur, zowel voor burgers als voor bedrijven en overheden. Zij vereisen onderlinge samenwerking, afstemming en vertrouwen. Daarvoor zijn open technieken nodig. Technieken die duidelijk zijn,

die iedereen kan gebruiken, waarop iedereen kan vertrouwen, en die kunnen worden ingepast in andere ICT-systemen. In de praktijk komen deze eisen het beste tot hun recht via systemen die open source zijn, zodat iedereen zekerheid kan krijgen over de gebruikte software en cryptografie. Open source wil zeggen dat er vrije toegang is tot de programmatuur (source) van het eindproduct. IRMA werkt met open source. Omwille van transparantie en om klemmende afhankelijkheden (vendor-lockins) te voorkomen zou de hele publieke sector met open source software moeten werken.

## Eilandencultuur

Nu kent de zorgsector een eilandencultuur, zeker als het om ICT gaat. Fabrikanten en leveranciers moedigen dat aan: hoe meer eilanden, hoe vaker zij dezelfde apparaten en software kunnen verkopen. Doordat zij typisch alles met gesloten source doen, ontstaat eerdergenoemde vendor lock-in: de klant wordt afhankelijk van de leverancier. Hij kan geen kant op en slaagt er niet in van leverancier te veranderen zonder extreem hoge kosten te maken of uitermate veel hinder te ondervinden.

De stichting achter IRMA probeert deze dure afhankelijkheden te doorbreken. Niet iedereen is daar blij mee. Gelukkig zijn er steeds meer zorgpartijen die dit oppakken — zie bijvoorbeeld nuts.nl — en met IRMA en open source willen werken. Ook bij veel gemeenten is het besef gegroeid dat zij vaker gezamenlijk en in open source moeten software ontwikkelen. Via de Vereniging van Nederlandse Gemeenten zijn zij het project Common Ground begonnen, waarbij ook IRMA gebruikt wordt.

Voor de duidelijkheid: IRMA is gericht op de bescherming van de eigen persoonsgegevens. Maar IRMA kan ook gebruikt worden om anderen daarmee te helpen, bijvoorbeeld via machtigingen.

Machtigingen in de zorg zijn erg belangrijk maar zijn niet systematisch goed geregeld. Machtigingen komen veel voor binnen een gezin of familiesituatie, waarbij de een de DigiD-logingegevens van een ander heeft. Dat is meestal niet zo'n probleem. In de thuiszorg hebben medewerkers soms tientallen DigiD-logins van hun patiënten. Is dat veilig? Is dat hoe we deze zaken willen regelen?

De overheid werkt aan een centraal DigiD-machtigingsregister, met koppelingen tussen twee bsn's: een van de machtiginggever en een van de machtigingnemer. Hier heeft uw zorgverzekeraar niets aan zodra degene die u een machtiging wilt geven daar geen klant is, want dan mag diens bsn niet

verwerkt worden. Mijn conclusie is dat dit decentraal allemaal veel beter werkt. Hoe dan? Door burgers het onderling te laten regelen. Zorverzekeraar VGZ laat mensen onderling een machtigingsrelatie vastleggen via een IRMA-attribuut. Dat is in snel zelf geregeld, en kan ook zo nodig snel weer teruggetrokken worden.

In het begin van mijn betoog vraag ik me af wie het opneemt voor de publieke zaak in de digitale wereld. Dat doet bijvoorbeeld Privacy by Design, de onafhankelijke stichting achter IRMA. Zij zet zich in voor het publieke belang, het common good. Tegenwoordig geldt die publieke zaak als iets muffigs uit de jaren vijftig van de vorige eeuw. Ik ben er echter van overtuigd dat we daar naartoe terug moeten. Als onze onderlinge verhoudingen in de digitale wereld — uit naïviteit of uit laksheid — worden overgelaten aan de Googles en de Facebooks, en straks aan de Alibabas, dan kunnen we voorspellen hoe het eindigt. Kijk naar Facebook en Cambridge Analytica. Een ander soort, op publieke waarden gebaseerde, ICT-infrastructuur is hard nodig. Wie kiest daarvoor?