# Opmars Internet van Lichamen vereist regulering

Allerlei apparaten op en in het lichaam leveren, via sensoren en draadloze verbindingen, een schat aan persoonlijke gegevens op. Dit 'Internet van Lichamen' vereist een zorgvuldige regulering van de eigendoms- en gebruiksrechten van de gegevens.

**IN HET KORT**

- Het aantal apparaten in het Internet van Lichamen zal naar verwachting snel toenemen.
- Vraagstukken rondom de beveiliging, eigendoms- en gebruiksrechten en privacy vragen om (verdere) overheidsregulering.

**FRANK DEN BUTTER**
*Hoogleraar aan de Vrije Universiteit*

Het Internet van Lichamen (*Internet of Bodies*, IoB) omvat een systeem van met het internet verbonden 'slimme' apparaten, uitgerust met sensoren, die zijn bevestigd aan, geïmplanteerd in of opgenomen binnen menselijke lichamen om zo de lichamelijke toestand en het gedrag te monitoren, te analyseren en zelfs te veranderen. Deze persoonlijke gegevens worden via het internet, of via een lokaal netwerk, verzonden. Als bron voor big data is IoB verwant aan het Internet der Dingen (*Internet of Things*) waar onderlinge communicatie tussen apparaten via internet grote hoeveelheden gegevens oplevert. Voorbeelden zijn slimme thermostaten, zelfrijdende auto's en koelkasten met een eigen voorraadbeheer.

Marr (2019) onderscheidt drie generaties IoB. Ten eerste draagbare apparaten buiten het lichaam, zoals de slimme horloges van Apple, of Fitbits die informatie over gezondheid en prestatievermogen verschaffen. Verder apparaten waarmee er op afstand kan worden waargenomen of de baby het nog goed maakt, of dat de luier verschoond moet worden; en contactlenzen waarmee er toegevoegde beelden – *augmented reality* – kunnen worden bekeken.

Ten tweede apparaten en sensoren in het lichaam, zoals pacemakers, implantaten om gehoorfuncties te herstellen en digitale pillen die lichaamsfuncties in de gaten houden en kunnen aanvullen.

Ten derde apparaten en sensoren in ons lichaam die realtime met apparaten buiten het lichaam zijn verbonden, zoals geïmplanteerde microchips die toegang bieden tot kantoor of waarmee er op een computer kan worden ingelogd. Een medisch voorbeeld van een IoB-apparaat van de derde generatie is een 'slimme pil' die elektronische sensoren en computerchips bevat. Eenmaal ingeslikt, kunnen deze digitale pillen gegevens over onze organen en medicatie verzamelen, en deze daarna doorsturen naar een extern apparaat.

Volgens een rapport van de Rand Corporation (Lee et al., 2020) zal de acceptatie van IoB snel toenemen. Het rapport schat dat er rond 2025 meer dan 41 miljard actieve IoB-apparaten zullen zijn, die dagelijks vele triljoenen gegevens over het milieu, vervoer, de lokalisering, voeding, lichaamsbeweging, biometrie en sociale interacties, en dus het dagelijks leven van de mens opleveren.

Deze verwachte opmars van IoB biedt voordelen op het gebied van gezondheid en andere innovatieve toepassingen van IoB, zoals in het werk en in het uitgaansleven (Liu en Merrit, 2020). Tegelijkertijd roept deze ontwikkeling vragen op over zowel beveiliging, eigendoms- en gebruiksrechten als privacy. Dit artikel betoogt dat regulering op deze drie punten nodig is om het publieke belang dat met de verzameling en toepassing van IoB-gegevens gemoeid is, te borgen.

## Beveiliging

Een belangrijk aandachtspunt bij IoB is dat de verbinding tussen het apparaat en de externe ontvanger van gegevens veilig moet zijn. Denk aan een pacemaker waarvan de verbinding niet verstoord of gehackt mag worden. Iets soortgelijks geldt bij het Internet of Things. Een zelfrijdende auto mag niet door een kwaadwillende hacker de sloot in worden gedirigeerd. In beginsel zal de fabrikant/leverancier van het IoB-apparaat zelf voor een goede beveiliging van de verbinding dienen te zorgen en dat ook willen. Dat veronderstelt echter wel een perfect werkende markt. Immers, hacken of andere problemen met de verbinding zou reputatieschade kunnen opleveren. In werkelijkheid zullen de kopers van de IoB-apparaten geen volledige informatie hebben over de wijze waarop de apparaten veilig te gebruiken zijn. Deze informatie-asymmetrie impliceert een rol voor de overheid: er is namelijk sprake van een publiek belang.

De oplossing ligt in de regelgeving bij het ontwerp van het IoB-apparaat en de transmissie van de gegevens. Net als bij het Internet of Things (Den Butter en Den Butter, 2016) is hier ook sprake van een gestaffelde *principaal-agent-relatie* waarbij de fabrikant van het apparaat verantwoordelijk is voor de handhaving van de regelgeving, maar die verantwoordelijkheid aan de ontwerper doorgeeft. Net zoals bij een nieuw gebouw de opdrachtgever verantwoordelijk is dat de er aan de bouwvoorschriften wordt voldaan, en die verantwoordelijkheid ook doorgeeft aan de architect en/of uitvoerder. In het geval van IoB ligt het voor de hand dat de maker/ontwerper zich moet houden aan richtlijnen die dienen te worden opgesteld wat betreft de beveiliging van de verbinding. Op de handhaving ervan kunnen dan nationale overheden toezien, of dit toezicht uitbesteden aan een onafhankelijk panel van deskundigen.

## Eigendoms- en gebruiksrechten

Daarnaast speelt de vraag over de eigendoms- en gebruiksrechten van de IoB-gegevens, net zoals dat bij genetische gegevens het geval is (Den Butter, 2020). Het is denkbaar dat, wanneer de persoonlijke IoB-gegevens wijzen op een gezonde leefstijl, en daarmee dus aangeven dat het ziekterisico minder dan gemiddeld zal zijn, men bij een ziektekostenverzekering een lagere premie zou kunnen bedingen. In het Nederlandse zorgstelsel is echter een dergelijke selectie van goede risico's niet toegestaan. Vanwege de 'ingebouwde risicosolidariteit' – ongelijke risico's betalen gelijke premies – is er een acceptatieplicht voor alle zich aanmeldende verzekerden. Zorgverzekeraars mogen dus niemand weigeren op basis van IoB-informatie. In die zin hebben ze dus van die informatie geen gebruiksrechten. Ook mogen ze geen premiedifferentiatie aanbieden op basis van beschikbare IoB-informatie, ook al zouden degenen op wie de gegevens betrekking hebben – en dus over de eigendomsrechten beschikken – daar voordeel bij hebben. Het publieke belang betreft in dit geval dus handhaving van de risicosolidariteit bij de ziektekostenverzekering.

Zowel de maatschappij als ziektekostenverzekeraars hebben er ook in meer algemene zin belang bij wanneer mensen gezonder gaan leven en daardoor meer aan ziektepreventie doen. Zo komen klanten van A.S.R. in aanmerking voor beloningen, als ze ervoor kiezen om meer te gaan bewegen met een app van een gezondheidsprogramma – en ook bereid zijn om privacygevoelige informatie te delen. Dat betreft dan een korting op de aanschaf van een 'slim horloge' of stappenteller, of minder premie voor de aanvullende verzekering (een lagere ziektekostenpremie mag dus niet). Ook Menzis heeft zo'n 'verdienen door bewegen'-programma. In feite betekent deze aanzet tot een gezondere levensstijl dat zo'n benutting van IoB-apparatuur een positief extern effect oplevert, namelijk een verlaging van de totale ziektekosten. Hierbij is dan een politieke afweging nodig tussen het behoud van risicosolidariteit en de inbouw van een geldelijke prikkel tot kostenreductie in de gezondheidszorg. En misschien is het toch politiek haalbaar om enige premiereductie toe te staan op basis van objectiveerbare gegevens over de levensstijl.

## Privacy

Nog meer in het oog springend is de vraag hoe de privacy van de gegevens die IoB oplevert kan worden gegarandeerd en geregeld. Het publieke belang betreft daarbij in eerste instantie de rechtsbescherming. Vanuit dat gezichtspunt moet de overheid paal en perk stellen aan wie er over de IoB-gegevens kan beschikken, en hoe deze gebruikt worden. In die zin is beveiliging van de verbinding, zodat er geen privacygevoelige gegevens ontvreemd kunnen worden, belangrijk. In ieder geval dienen degenen op wie de informatie betrekking heeft, inzicht te krijgen in wie er over die informatie beschikt.

De beschikking over persoonsinformatie is geregeld via de 'privacywet' (de Algemene verordening gegevensbescherming, AVG), die op 25 mei 2018 van kracht werd en voor alle Europese landen gelijk is. Daarbij geldt dat de verwerking en het delen met derden van persoonsgegevens verboden is, tenzij de AVG een uitzondering maakt. Zo'n uitzondering kan ontstaan in het geval van een uitdrukkelijke toestemming. Maar, zoals het voorgaande al laat zien, betekent toestemming van de gegevenseigenaar niet automatisch dat er dan gebruiksrechten zijn voor degene aan wie toestemming is verleend.

Net als bij de genetische gegevens is het de vraag in hoeverre de overheid additionele gebruiksrechten zou moeten verkrijgen voor de via IoB vergaarde informatie. IoB-gegevens van bijvoorbeeld smartphones kunnen, net als DNA-profielen, een belangrijke bron zijn bij misdaadbestrijding. Zo mag de politie van Singapore gegevens van de *TraceTogether*-app (die in het verband met de coronabesmetting onderlinge contacten registreert) inzetten bij onderzoek naar misdrijven. Overheden kunnen IoB-gegevens ook gebruiken voor een gerichte nudging van doelgroepen, of zelfs voor het creëren van een digitale identiteit, waarbij alle persoonlijke informatie die over een individu beschikbaar is, wordt gebundeld. Dit kan nuttig zijn, maar kan ook risico's met zich meebrengen (Dawson en Duda, 2021; World Economic Forum, 2018). Zo kunnen deze gegevens worden misbruikt door autoritaire overheden om het gedrag van burgers te observeren en bewaken via een sociaal kredietsysteem (Hinchliffe, 2020), waarbij er een orwelliaanse controle-samenleving dreigt (Lindsey, 2018). Al met al betekent het dat er voor de overheid beperkingen moeten gelden bij het gebruik van IoB-gegevens, zoals die ook dienen te gelden voor de gebruiksrechten door de overheid van de biometrische gegevens, zoals gezichtsherkenning (Gerritsen et al., 2020).

## Tot besluit

Het Internet van Lichamen neemt snel in belang toe. De gegevens die via apparaten op of in het lichaam worden verzameld en extern worden opgeslagen, dragen bij aan levensvreugde en welzijn. Bovendien kan het kostenbesparingen opleveren, waarbij er sprake is van positieve externe effecten. Tegelijkertijd raken, rondom IoB, beveiliging, eigendoms- en gebruiksrechten en privacyvraagstukken het publieke belang. Asymmetrische informatie, negatieve externe effecten en politieke afwegingen ten aanzien van risicosolidariteit vragen om een (verdere) overheidsregulering.

## Literatuur


Butter, F.A.G. den (2020) Eigendoms- en gebruiksrechten van genetische informatie. *Beleid en Maatschappij*, 47(4), 439–450.

Butter, F.A.G. den, en G.G.J. den Butter (2016) Het verband tussen publiek belang en ontwerp bij het internet der dingen. *Beleid en Maatschappij*, 43(1), 24–41.

Dawson, J. en C. Duda (2021) *How digital identity can improve lives in a post-COVID-19 world*. The Davos Agenda 2021, 14 januari. Te vinden op www.weforum.org.

Gerritsen, J., J. Hamer, L. Kool en P. Verhoef (2020) Beter beschermd tegen biometrie. *Beleid en Maatschappij*, 47(4), 451–466.

Hinchliffe, T. (2020) *Your digital identity can be used against you in the event of a great reset*. Artikel op sociable.co, 23 november.

Lee, M., B. Boudreaux, R. Chaturvedi et al. (2020) *The Internet of Bodies: opportunities, risks, and governance*. Rand Corporation, Research Report, 3226.

Lindsey, N. (2018) *Internet of Bodies: the privacy and security implications*. Artikel op www.cpomagazine.com, 14 december.

Liu, X. en J. Merritt (2020) *Shaping the future of the Internet of Bodies: new challenges of technology governance*. World Economic Forum Briefing Paper, juli.

Marr, B. (2019) What is the Internet of Bodies? And how is it changing our world? *Forbes*, 6 december.

World Economic Forum (2018) *Identity in a digital world: a new chapter in the social contract*. Insight Report, 25 september.