

Pas op voor de handel in onze hartslag en bloeddruk

Door nieuwe mobiele apps en wearables staat de vertrouwelijkheid van onze biologische gegevens onder druk. De aankomende herziening van het dataproctierecht beschermt burgers onvoldoende tegen bedrijven die handelen in die gegevens. Daarom is een fundamentele herbezinning op ons privacyrecht nodig.

Technologie en mens raken steeds inniger met elkaar verbonden. Technologie nestelt zich nabij en tussen ons, en verzamelt informatie over ons. Via internet raken mensen, apparaten, diensten en bedrijven steeds meer met elkaar verbonden. Bedrijven volgen surf- en klikgedrag. Daar komen nu biologische gegevens bij. Dat komt door de opkomst van wearables, zoals fitnessarmbanden en apps waarmee we slaappgedrag, beweging, voeding en stress bijhouden. Uit biodata is waardevolle én gevoelige informatie over onze fysieke en mentale gezondheid af te leiden. Looppatronen kunnen vroeger tekenen van demantie laten zien.

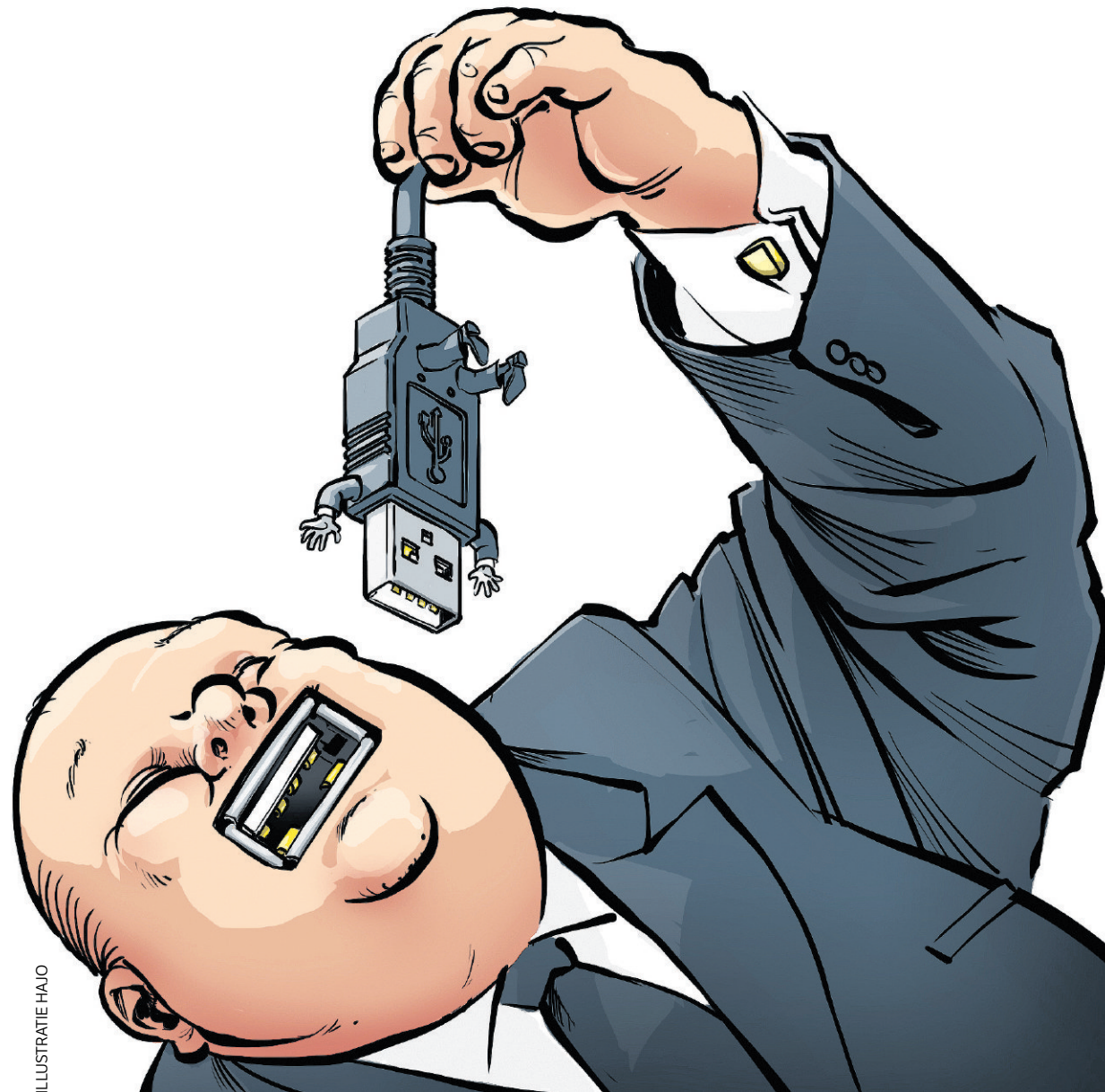
Veel mensen vinden het interessant om biologische data van zichzelf te verzamelen. De gegevens bieden nuttige inzichten: bijvoorbeeld dat ze

Met fitnessarmbanden en mobiele apps laten sommigen vrijwillig slaappgedrag, beweging, voeding en stress bijhouden. Bedrijven handelen in die data en dringen straks monitoring op, waarschuwen Rinie van Est en Linda Kool.

slechter slapen op avonden dat ze laat gegeten hebben. Meer en meer bedrijven willen die biodata oogsten: uit onderzoek bleek bijvoorbeeld dat 20 populaire gezondheidsapps data delen met meer dan 76 partijen. Verder experimenteren zorgverzekeraars, bijvoorbeeld Menzis, met wearables en gezondheidsapps: wie gezond leeft, kan punten verdienen om minder premie te betalen. Chipmaker ASML stimuleert zijn werknemers hun fysieke en mentale fitheid te monitoren,

om de productiviteit te verhogen. Die zaken gebeuren nu nog op basis van vrijwilligheid. Maar het is zeker denkbaar dat er meer druk op werknemers en verzekerden komt om hun gezondheidsgegevens te gaan bijhouden.

Er geldt een soort bescherming - het begrip 'geïnformeerde toestemming', in Nederland onderdeel van in de Wet bescherming persoonsgegevens. Echter, in de digitale wereld verliest het betekenis. Voor individuen is het ondoenlijk te overzien wat er met hun data gebeurt en wat daarvan de consequenties zijn. Denk aan de ellenlange, ondoorzichtige gebruikersvoorwaarden van websites, apps en wearables. Die voorwaarden kunnen bovendien op elk moment eenzijdig door bedrijven worden aangepast. Belofte om data niet te delen, komen na bedrijfsovernames vaak op losse schroeven te staan. Tel daarbij op de geavanceerde surveillancetechnieken van een complex netwerk van datahandelaren, trackingbedrijven en advertentienetwerken. Gegevens worden in miniseconden verhandeld via online veilingen en verrijkt tot gedetailleerde profielen. Die datahandel wordt achter de schermen beheerst door grote, vaak onbekende bedrijven, zoals Experian, Datalogix of Axciom. Consumenten weten niet in



ILLUSTRATIE HAJÓ

welke profielen ze zijn ingedeeld, noch welke producten en diensten hun op basis daarvan (niet) worden aangeboden. Ze weten dus ook niet hoe ze worden beïnvloed of hoe ze daar bezwaar tegen kunnen maken. Naast privacy komen ook keuzevrijheid en autonomie in het gedrag.

Er is dus sprake van een grote informatie-asymmetrie tussen het individu en bedrijven. Daarom vernieuwt de Europese Unie de wetgeving voor persoonsgegevens. In de voorgestelde dataproctieverordening komt de EU met noodzakelijke verbeteringen zoals het 'recht om vergeten te worden', 'recht op dataportabiliteit' en toegankelijke privacy-informatie. Ook moet privacy in de techniek worden ingebouwd en gaan de boetes op overtredingen omhoog. Het idee is dat bedrijven verantwoordelijker zullen omgaan met gegevens en dat met een betere privacy klanten kunnen worden gelokt.

Dat idee is mooi, maar nog onvoldoende om het machtsverschil tussen bedrijven en die van individuen aan te pakken. De grootste datahandel vindt immers achter de schermen plaats; consumenten hebben geen rechtstreeks contact met de grote datahandelaren. Die bedrijven hebben weinig reden om transparanter te handelen: de huidige onzichtbaarheid geeft hun speelruimte om zaken te doen. De online datahandel, de ontstane informatie-asymmetrie en de effecten die het gebruik van data op individuen kan hebben, vragen om een fundamentele herdenking van

ons privacyrecht.

Dat privacyrecht is onder meer vastgelegd in artikel 10 van onze grondwet. Het beschermt iedereen tegen inmenging in het privéleven. Tot nu toe werd dit grondrecht vooral gezien als een manier om burgers te beschermen tegen de macht van de staat. Nu ook databedrijven een grote machtsfactor zijn, is een ruimere uitleg van ons privacyrecht nodig. De overheid zou via de grondwet burgers ook moeten beschermen tegen de digitale praktijken van bedrijven, zelfs als die burgers zelf met die bedrijven in zee zijn gegaan.

Privacy geeft ons de vrijheid zelf te bepalen wat we met anderen willen delen, en de mogelijkheid in vrijheid te kiezen, niet beïnvloed door anderen. Zonder zo'n ruimere interpretatie van het privacyrecht verliezen we die vrijheid. Dan wachten onze biologische data hetzelfde lot als onze klik- en surfgegevens; ze worden massaal verhandeld en mogelijk in ons nadeel gebruikt. Overheid, maak haast met burgers te beschermen tegen de data-industrie.



Linda Kool en Rinie van Est zijn onderzoekers aan het Rathenau Instituut. Dit opiniestuk is gebaseerd op het essay 'Intieme technologie' uit *Liberaal Reveil*.