

Privacybewuste oppositie in VK buitengesloten bij discussie over big-data in de zorg



In het Verenigd Koninkrijk blijkt de privacy-bewuste oppositie tegen het vermarkten van big-data in de zorg op een heel bijzondere manier buiten spel te zijn gezet. In de adviesraad, die daarover moet adviseren, zijn deze groeperingen niet meer opgenomen, evidente voorstanders wel. [8 februari stond op de website The Register](#) een in mijn ogen schokkend relaas hoe men tegenstanders in de privacy-discussie rond medische big-data buiten spel zet. De National Health Service(NHS) heeft rond 2012/2013 het Health and Social Care Information Centre (HSCIC) opgericht met databases, waarin geanonimiseerde patiëntengegevens van huisartsen worden opgeslagen. Het is de bedoeling, dat Care.data, een onderdeel van de NHS, deze gegevens beheert. De opzet is dat deze big-data van de zorg als basis dienen voor het optimaliseren van de zorg. Daarnaast wil men deze data ook verkopen aan derden. [Ondanks negatieve ervaringen in o.a. 2014](#) met het vermarkten van medische data(ziekenhuisgegevens) wil de NHS doorgaan met dergelijke praktijken.

Discussie

De discussie over de opzet en bedoelingen van Care.data werd

in 2014 gestroomlijnd door het opzetten van een [Advisory Group, die zeer breed van opzet was](#). Die Advisory Group werd in 2015 opgeheven en vervangen door de Strategic Oversight Board(SAB). Er is geen enkele richtbaarheid gegeven aan het opheffen van de Advisory Group. Alleen uit een overzicht van wat besproken was op een [Care.data-meeting op 19 oktober 2015](#) wordt dit duidelijk. Zelfs de website van de opgeheven Advisory Group, is intact gelaten [en is nu nog op het internet te vinden](#) . In de SAB blijken twee zeer kritische organisaties op het gebied van privacy niet meer opgenomen te zijn. Het gaat om medConfidential en Big Brother Watch. Daarentegen is een organisatie als Patients4Data die gelieerd is aan een biotech-bedrijf en een apart voorstander van zorg-big-data gebruik, wel in de SAB opgenomen. Het is een schokkende manier om de tegenstanders de mond te snoeren en tegelijkertijd extra voorstanders in huis te halen.

Anoniem?

De verzamelde gegevens worden gecodeerd opgeslagen [samen met de geboortedatum, het geslacht, de postcode en het NHS-verzekeringsnummer](#). De data zouden gepseudonimiseerd worden. De genoemde persoonskenmerken zouden nodig zijn om de data te kunnen koppelen met data uit andere databases. Er zijn mogelijkheden gecreëerd om de patiënten toch te identificeren door middel van zogenaamde “identifiers”. Die ontsleutel-mogelijkheid zou buiten het Care.data-systeem worden opgeslagen, maar het feit dat zulks mogelijk is, verontrust kritische burgers en organisaties. Ook de universiteit van Cambridge waarschuwde, blijkens het artikel in The Register.

Het is vergelijkbaar met de situatie met de gegevens in Nederland in het DBC-Informatie-Systeem(DIS). Daar blijkt dat de gepseudonimiseerde gegevens toch door bepaalde instanties tot personen herleidbaar te zijn. [Dat gaf recent de Nederlandse Zorgautoriteit\(NZa\) toe in een rechtszaak](#). Het is dus aan beide zijden van de Noordzee zo dat gegevens uit de zorg dus niet echt anoniem worden uitgewisseld.

Ont-anonimiseren

In Nederland liet [Matthijs Koot in 2012 in zijn proefschrift](#) met als titel "Measuring en predicting anonimity" al zien dat met een zeer beperkt aantal gegevens toch individuen geïdentificeerd kunnen worden. Dat zelfs inlichtingendiensten moeite hebben om metadata van personen te de-identificeren moge blijke uit een publicatie van Tamir Israel en Christopher Parsons op 3 februari 2016 op de website www.justsecurity.org. In hun artikel genaamd "[Why We Need to Reevaluate How We Share Intelligence Data With Allies](#)" gaat het om het uitwisselen van gegevens tussen inlichtingendiensten. Gegevens die het Canadese Communications Security Establishment(CSE) verzamelde, werden uitgewisseld met geheime diensten uit de Verenigde Staten, het Verenigd Koninkrijk, Australië en Nieuw Zeeland. Edward Snowden openbaarde dit Five-Eyes samenwerkingsprogramma. De CSE mocht alleen maar metadata van communicatie van niet-ingezetenen van Canada legaal vastleggen en uitwisselen, maar niet van Canadese burgers. Die data dienden geanonimiseerd te worden. Uit het artikel van Israel en Parsons blijkt, dat het niet-identificeerbaar maken van gegevens door de CSE niet goed ging. Met computertechnieken van de overige vier partners in het Five-Eyes-programma bleek het toch mogelijk de gegevens die uitgewisseld werden tot personen, in dit geval Canadese staatsburgers, te herleiden.

Onmogelijk

Uit het bovenstaande moge duidelijk zijn dat het eigenlijk onmogelijk is om data met enkele persoonsgegevens zo op te slaan dat die volledig anoniem zijn. Het is daarom uitermate dubieus wat de NHS nu met het Care.data-programma aan het doen is. Vermarkten van medische big-data dient niet plaats te vinden en gebruik van gegevens binnen de NHS dient met strenge regelgeving omgeven te zijn. Er dient volledige openheid te zijn over wat met welke data gebeurt. Door mist te creëren rond een adviesraad en bovendien bij de voortzetting onder een andere naam notoire tegenstanders buiten te sluiten en een

uitgesproken voorstander in huis te halen bewijst de NHS en de burgers van het Verenigd Koninkrijk een slechte dienst.

Voor Nederland is het een niet te veronachtzamen waarschuwing over hoe een staatsinstelling met privacy-bewuste organisaties en individuen omgaat.

Men zij gewaarschuwd.

W.J. Jongejan