# Digitale psychiatrie en privacy

M. MOSTERT

ARTIKEL

De digitale revolutie biedt vele mogelijkheden om de psychiatrische diagnostiek en zorg te verbeteren, zo concluderen Naarding e.a. (2019). In dit commentaar richt ik mij op de vraag hoe de geschetste ontwikkelingen in de digitale psychiatrie zich verhouden tot de wettelijke bescherming van de privacy van de patiënt. Daarmee blijft een breed scala aan relevante juridische aspecten buiten beschouwing. Voorbeelden hiervan zijn de (veranderende) wet- en regelgeving rond medische hulpmiddelen, de geneeskundige behandelingsovereenkomst (WGBO) en aansprakelijkheid (Hooghiemstra & Nouwt 2014; Ruesen 2017; Ministerie van VWS 2017).

## Privacy, gegevensbescherming en beroepsgeheim

De ontwikkelingen zoals beschreven door Naarding e.a. raken de kern van het recht op privacy. Het recht op privacy kan volgens het Europees Hof voor de Rechten van de Mens (EHRM) gekarakteriseerd worden als: de fysieke, psychologische en morele aspecten van de persoonlijke integriteit, identiteit en autonomie van individuen (van Dijk e.a. 2018). Wanneer het gaat om de verwerking van gegevens, wordt het recht op privacy rechtstreeks en direct geraakt wanneer: '(...) zeer precieze conclusies worden getrokken over het privéleven van de personen (...), zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.'

Het zijn dit soort gegevens die bij digitale fenotypering in de psychiatrie verzameld worden. Daar komt bij dat het veelal om (psychische) gezondheidsgegevens gaat, die extra gevoelig van aard zijn en aanvullende bescherming genieten onder de Algemene Verordening Gegevensbescherming (EU 2016/679) (AVG). Worden de gegevens in het kader van een behandelrelatie verzameld, dan is daarnaast het medisch beroepsgeheim van toepassing. Verder is nog de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) van belang, vooral als elektronisch uitwisseling van patiëntgegevens plaatsvindt via een systeem dat door meerdere zorgaanbieders wordt gebruikt.

De bescherming van privacy wordt in de praktijk regelmatig als belemmerend ervaren. Dit bleek bijvoorbeeld tijdens een deskundigenbijeenkomst in 2016 in de Eerste Kamer, waar de toenmalige voorzitter van de Brancheorganisaties Zorg zich als volgt uitsprak over de Wabvpz: 'het risico [is] heel groot (...) dat je wetgeving invoert die niet handhaafbaar is, enorm veel tijd wegneemt van de zorgverleners en innovatie en kwaliteit van zorg in de weg staat, (...).' Een dergelijke impact is uiteraard niet het doel van privacywetgeving, maar het valt niet uit te sluiten dat dit een neveneffect is. Wet- en regelgeving hebben tot doel om kwalitatief goede zorg op een verantwoorde manier mogelijk te maken. Zonder een passende bescherming van privacy en in het bijzonder het beroepsgeheim kan het vertrouwen van de patiënt verloren gaan. Ook komt dan de toegang tot de gezondheidszorg in het gedrang, zo overwoog het EHRM (1997).

## Duidelijke wet- en regelgeving

Naarding e.a. concluderen dat heldere regelgeving nodig is, maar geven geen onderbouwing van deze conclusie. Deze roep om duidelijkheid staat echter niet op zichzelf. Zo heeft onduidelijkheid over wet- en regelgeving jarenlang in de top drie gestaan van ervaren belemmeringen door medisch specialisten (Nictiz en Nivel 2015). Ook blijkt uit kwalitatief onderzoek dat onzekerheid bestaat over juridische normen waar het gaat om privacy en gegevensbescherming in psychiatrisch en psychosociaal onderzoek met big data (Mostert 2018). Deze onzekerheid wordt vooral toegeschreven aan een gebrek aan toegankelijke expertise en wijzigingen in wetgeving.

Als wet- en regelgeving in de praktijk vooral als onduidelijk of belemmerend worden ervaren, dan kan dit een probleem zijn. Het doet in potentie afbreuk aan de rechtszekerheid en het beoogde effect van die wet- en regelgeving. Daarmee kan het bewaken van de privacy en het vertrouwen van de patiënt in het gedrang komen, maar ook kan het leiden tot te restrictieve opvattingen over wat toegestaan is.

Hoewel het een goed streven is om juridische normen te verduidelijken, is het onrealistisch om te verwachten dat dit de noodzaak wegneemt tot investering in juridische expertise en interdisciplinaire samenwerking. De toepassing en de interpretatie van privacynormen zijn nu eenmaal in grote mate contextafhankelijk. Dit wordt ook

erkend in de AVG, in het bijzonder middels de regulering van data protection impact assessment (DPIA) en de uitgangspunten van privacy by design & default.

De DPIA is een instrument dat bruikbaar is bij het in een vroege fase in kaart brengen van de privacyrisico's van een bepaalde gegevensverwerking. Een DPIA is verplicht als de gegevensverwerking waarschijnlijk een hoog risico inhoudt voor de betrokkenen (artikel 35 AVG), wat veelal het geval zal zijn bij digitale innovaties in de psychiatrie. De Artikel 29 Working Party (2019) publiceerde richtlijnen die gevolgd kunnen worden bij het inschatten van de noodzaak en het uitvoeren van een DPIA.

Verder verplichten de uitgangspunten van privacy by design & default om gedurende de gehele levenscyclus van een systeem rekening te houden met de bescherming van persoonsgegevens (artikel 25 AVG). Dit houdt in dat men al vanaf de ontwerpfase van een digitale innovatie organisatorische en technische maatregelen neemt in lijn met de gegevensbeschermingsbeginselen, zoals dataminimalisatie, doelbinding en beveiliging.

## Tot slot

Bij digitale innovaties in de psychiatrie moet het bewaken van de privacy en het vertrouwen van de patiënt voorop staan. Onnodig belemmerende factoren in wet- en regelgeving dienen gemitigeerd te worden, zodat waardevolle innovaties voldoende ruimte krijgen. Daarnaast blijft investeren in juridische expertise, interdisciplinaire samenwerking en privacy-by-designoplossingen essentieel. Het is mijn overtuiging dat de bescherming van privacy op deze manier bij kan dragen aan duurzame en verantwoorde digitale innovaties in de psychiatrie.

## LITERATUUR


- Art. 29 Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679. 2017. Endorsed by the EDPB. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
- EHRM. 25 februari 1997. Z t. Finland. Nederlands Juristenblad 1998, 516.
- Hooghiemstra TFM, Nouwt S. Een juridische blik op trends in e-health. Ned Tijdschr Geneeskd 2014; 158: A8423.
- HvJ-EU. Zaak C-293/12. Digital Rights Ireland. ECLI:EU:C:2014:238.
- Ministerie van VWS. Handreiking nieuwe regelgeving medische hulpmiddelen en in-vitro diagnostica. https://www.igj.nl/zorgsectoren/medische-technologie/documenten/brochures/2017/12/12/handreiking-nieuwe-regelgeving-medische-hulpmiddelen-en-in-vitro-diagnostica
- Mostert M, Koomen BM, van Delden JJM, Bredenoord AL. Privacy in Big Data psychiatric and behavioural research: A multiple-case study. Int J Law Psychiatry 2018; 60: 40-4.
- Naarding P, Marijnissen RM, Westerhof GJ. Digitale psychiatrie. Tijdschr Psychiatr 2019; 61: 335-42.
- Nictiz en Nivel. eHealth-monitor 2015. https://www.nictiz.nl/programmas/e-health-monitor/ehealth-monitor-2015/
- Ruesen MRL. Ongeschikte medische apps: wie is aansprakelijk? Computerrecht 2017; 49.
- van Dijk P, van Hoof F, van Rijn A, Zwaak L. Theory and practice of the European Convention on Human Rights. Antwerp: Intersentia; 2018.



## AUTEUR

**MENNO MOSTERT**, universitair docent gezondheidsrecht, Julius Centrum, UMC Utrecht.

**CORRESPONDENTIEADRES**

Mr. dr. M. Mostert, Julius Centrum, UMC Utrecht, Huispostnummer Str. 6.131, Postbus 85.500, 3508 GA Utrecht.
E-mail: m.mostert-2@umcutrecht.nl



Geen strijdige belangen meegedeeld.

Het artikel werd voor publicatie geaccepteerd op 16-4-2019.


## TITLE IN ENGLISH

Digital psychiatry and privacy