
*Veiligheid en privacy*

# De hekkensluiters van online hulpverlening

**Veel professionele begeleiders zijn aangesloten bij een beroepsorganisatie met een eigen beroepscode inclusief ethische regels. In de codes staan uitgebreide paragrafen over hoe om te gaan met de privacy en de gegevens van de cliënt: geen informatie delen met onbevoegden en cliëntgegevens netjes achter slot en grendel bewaren. Inmiddels is door het gebruik van computers en internet het een stuk lastiger geworden om te voldoen aan de beroepscodes. Soms schieten deze codes zelf tekort omdat ze geen rekening houden met de bijzondere dynamiek van online begeleiding. Uit recent onderzoek blijkt dat we door het gebruik van online hulpwebsites en apps vaak de privacy van onze cliënten schenden, omdat veel van deze technische hulpmiddelen onveilig in gebruik zijn.**

**Alexander Waringa**

Ruim tien jaar geleden werd ik gevraagd om mee te werken aan een experiment met een sociale robot. Het ging hier om een klein apparaat dat de vorm had van de kop van een kat. Deze kater kon verschillende menselijke gezichtsuitdrukkingen ('emoties') laten zien en interactief met zijn eigenaar communiceren. De robot werd bij bejaarden thuis geplaatst om hen te helpen herinneren dagelijkse routinehandelingen, zoals het innemen van medicijnen, en het spelen van eenvoudige spelletjes. Voor het programmeren van de robot was veel persoonlijke informatie van de gebruiker nodig. Op mijn vraag hoe het zat met de privacy van de bejaarden, gaven de ontwikkelaars aan daar nog niet over te hebben nagedacht; ze waren al lang blij dat het hen gelukt was om deze robot te ontwikkelen.

## Vandaag de dag

In een recent verschenen onderzoeksrapport van het Rathenau Instituut (2014) worden diverse geautomatiseerde feedbackprogramma's beschreven die ondersteuning bieden bij gedragsveranderingen, zoals websites, computers, tablets, polsbandjes, smartphones en horloges met speciale intelligente softwareprogramma's (zogenoemde 'apps', 'applicaties', 'applets' en 'widges'). Bij de meeste van deze websites en apps worden er vraagtekens gezet bij de veiligheid en privacybescherming van de gebruikers.
Daarnaast blijkt er veel onduidelijkheid te bestaan over de commerciële belangen van de aanbieders van deze hulpmiddelen. Zo bleek bijvoorbeeld uit Amerikaans onderzoek (Christopherson, 2007) dat de verzamelde gegevens uit twaalf apps voor gezondheidsbevordering in totaal met 76 verschillende (commerciële) partijen werden gedeeld. Dat het slecht gesteld is met de privacy van de meeste hulpwebsites werd nog eens pijnlijk duidelijk bij de presentatie van Winfried Tilanus (2014) tijdens het Congres Online Hulp. Zijn onderzoek toonde aan dat van de 26 online hulpomgevingen 80% onbedoeld informatie verstrekt aan advertentieverkopende bedrijven. Daarnaast bleek bij een derde van de hulpwebsites de beveiliging onvoldoende, waardoor kwaadwillenden makkelijk met de hulpverlening mee kunnen kijken.

## Beweegredenen

Er zijn verschillende redenen aan te wijzen waarom het met zoveel hulpwebsites en apps niet goed geregeld is qua veiligheid en privacy:

- bedrijfsmatig en financieel perspectief: technische aanpassingen of voorzorgsmaatregelen worden bij de ontwikkeling van hulpwebsites of apps niet genomen, omdat deze economisch niet rendabel zijn;
- commercieel gewin: online omgevingen en apps worden opgezet met als doel om zoveel mogelijk verkoopbare informatie van gebruikers te vergaren;
- gebrekkige technische kennis: het gaat hier om ontwikkelaars, die voor hun websites of apps gebruikmaken van verouderde technieken of hulpmiddelen van derden, maar zelf niet goed begrijpen hoe deze werken.

De laatste twee genoemde redenen zijn vaak onbekend bij de inkopers en gebruikers van hulpwebsites of apps. Het gaat dan vooral om websites en apps die gebruikmaken van elementen (functies) die door andere partijen (gratis) worden aangeboden:

- diensten voor mail, chat en beeldbellen, zoals: Gmail, Hotmail, Google Hangout, Whatsapp, Skype, Facetime, Facebook en Twitter;
- diensten voor het verbeteren van een

website, zoals: Google Analytics, externe javascripts, Font services en Google Translate;
- diensten om websites op te leuken, zoals: Youtube, Vimeo, affiliate-programma's en de mogelijkheid om in te mogen loggen met bijvoorbeeld het eigen Facebook inlogaccount.

Een belangrijk nadeel van deze (gratis) elementen, hulpfuncties of externe functionaliteiten is dat ze vaak niet goed zijn beveiligd. Dat wil zeggen dat de informatie (bijvoorbeeld de mailtjes, chatberichten of videogesprekken) onbeveiligd wordt verzonden en opgeslagen. Derden kunnen deze informatie relatief eenvoudig onderscheppen.
Een ander vaak niet direct zichtbaar nadeel van deze programma's is dat de aanbieders informatie verzamelen van de gebruikers. Deze persoonlijke informatie van de gebruikers wordt gebruikt om gerichte advertenties aan te bieden.

### Marketingobject

Op het moment dat u gebruikmaakt van bijvoorbeeld het mailprogramma Gmail van Google worden alle door u verzonden en ontvangen mailtjes gescand en bewaard op de computers van Google. Daarnaast bewaart Google geruime tijd al uw zoekopdrachten die u in de zoekmachine van Google heeft ingevoerd. Ook is Google in staat om uw bewegingen op het internet te volgen met behulp van 'cookies' (kleine computerbestandjes) die uw internetgedrag vastleggen. Al deze gegevens worden door Google gecombineerd en gebruikt om persoonlijke advertenties aan u te communiceren. Door deze aanpak wordt het mogelijk dat er tijdens het bezoeken van een website advertenties verschijnen die specifiek voor u interessant zijn. Andere grote softwarebedrijven zoals Microsoft, Facebook, Apple en Yahoo gebruiken soortgelijke technieken.

Als er in een online hulpomgeving gebruik wordt gemaakt van bijvoorbeeld YouTube filmpjes (YouTube is van Google) en de gegevens van uw cliënt niet voldoende worden afgeschermd, zal Google in staat zijn om meer internetgedrag van uw cliënt samen te voegen tot een profiel. Hierdoor kan het gebeuren dat een patiënt die online met u communiceert over bijvoorbeeld seksuele problemen later tijdens het gebruik van internet steeds vaker advertenties tegenkomt over Viagra, escorteservices of andere aan seks gerelateerde zaken. Of een cliënt met een eetstoornis krijgt opeens advertenties voorgeschoteld over afslankpillen, Weight Watchers en nieuwe diëten. Hoe meer externe (gratis) online functies in een online hulpomgeving zijn verwerkt, hoe groter de kans dat de inhoud van een traject als input zal dienen voor advertentiecampagnes gericht op uw cliënten.

### Zakelijk

Ook in een zakelijke omgeving kunnen derden toegang hebben tot de inhoud van een mailbox. Zo heeft een werkgever in principe (technisch) toegang tot de mailbox van zijn medewerkers met speciale software programma's zoals Shadow, SpyAgent en Silent Watch. Met deze computerprogramma's kunnen mailconversaties gemonitord worden op bijvoorbeeld steekwoorden. Dat deze programma's ook echt worden ingezet bleek reeds in 2012 uit een grootschalig onderzoek door 'De Groene Amsterdammer': ruim een derde van de werkgevers in Nederland leest de e-mails van hun werknemers. Het is in deze situatie raadzaam om gebruik te maken van een e-mailadres van buiten de organisatie. Een andere optie is om als gebruiker er zelf voor te zorgen dat e-mailberichten beveiligd worden verzonden, zodat meelezen vrijwel onmogelijk wordt gemaakt. Dit kan bijvoorbeeld bij het mailprogramma Outlook van Microsoft, dat de mogelijkheid biedt

om berichten en bijlagen te versleutelen (coderen); een relatief simpele oplossing die maar weinig mensen gebruiken. Ook bestaat er speciale veiligheidssoftware gebaseerd op PGP (Pretty Good Privacy) om berichten te versleutelen.

### Overtreding

Gezien de technische staat van vele hulpwebsites, apps en e-mailprogramma's is het zeer aannemelijk dat we bij gebruik van deze instrumenten de beroepscodes van onze eigen beroepsorganisaties overtreden.

Artikel: 3.5.4. De counsellor is er, behoudens bij elke situatie van overmacht, voor verantwoordelijk dat het dossier op zodanige wijze wordt bewaard dat redelijkerwijs niemand toegang heeft tot de gegevens in het dossier zonder de toestemming van de counsellor (Algemene Beroepsvereniging voor Counseling).

Artikel: III.3.3.2 De psycholoog neemt in redelijkheid alle voorzorgen dat er in de schriftelijke, telefonische of elektronische communicatie met de cliënt of met andere betrokkenen geen vertrouwelijke gegevens over de cliënt, zonder diens instemming, ter kennis komen van derden (Nederlands Instituut van Psychologen).

- Neem de juiste hard- en software maatregelen om de integriteit en de privacy van het door de cliënt gebruikte computersysteem te beschermen en na afloop van een traject de opgeslagen informatie veilig te verwijderen.
- Blijf op de hoogte van alle wettelijke eisen die online werken beïnvloeden (Association for Counselling and Therapy Online)

Verder kennen we in Nederland ook nog wettelijke regels als het gaat om het verwerken van persoonsgegevens, zoals de Wet Bescherming Persoonsgegevens (WBP), de Wet op de Beroepen in de Individuele Gezondheidszorg (Wet BIG) die beschrijft dat bepaalde beroepsgroepen (onder anderen artsen, psychotherapeuten en gezondheidszorgpsychologen) een (medisch) beroepsgeheim hebben. Het doorspelen van informatie van cliënten aan derden is in veel gevallen dan ook illegaal.

Overigens lijkt de Nederlandse overheid op dit gebied met dubbele maten te meten omdat zij zelf steeds meer persoonlijke informatie verzamelt (door overheidssystemen aan elkaar te koppelen), de verplichte bewaartermijn voor telefoon- en mailgegevens (voor telecomaanbieders en internetproviders) verder oprekt en zichzelf de bevoegdheid wil geven om te mogen 'inbreken' in computersystemen.

### Selectiecriteria

De eerder genoemde onderzoeken en toelichtingen laten zien dat de beveiliging en betrouwbaarheid van vele hulpwebsites, e-mailprogramma's en apps te wensen overlaat. Het is aan ons, hulpverleners, ons ervan te vergewissen hoe de privacy van onze cliënt wordt gewaarborgd. Dit betekent dat wij heldere voorwaarden en eisen moeten stellen aan ontwikkelaars en leveranciers van e-healthtoepassingen. Hierbij dienen minimaal de volgende drie selectiecriteria naar tevredenheid beantwoord te worden:

***Hoe wordt de hulpwebsite of app afgeschermd en wie heeft toegang tot de informatie?***

Wordt informatie van cliënten met andere partijen gedeeld? Zo ja, met welk doel en hoe is dit te voorkomen? Is toegang

afgeschermd met een gebruikersnaam en wachtwoord? Wat is het wachtwoordbeleid, oftewel: hoe sterk is het wachtwoord (hoeveel tekens, hoofdlettergevoeligheid en bijzondere tekens zijn er nodig), hoe worden ze verzonden (versleuteld of niet) en hoe lang bewaard? Zijn er nog aanvullende maatregelen getroffen? Wachtwoorden zijn namelijk vrij makkelijk te kraken door geautomatiseerde programma's die honderden wachtwoorden per seconden kunnen uitproberen. Extra maatregelen om dit te voorkomen of te bemoeilijken zijn:

- CAPTCHA-beveiliging[1]: een slecht leesbaar teken dat extra ingevoerd moet worden. Over het algemeen kan alleen een mens deze tekens ontcijferen, met andere woorden: om te kunnen inloggen, moet u bewijzen dat u een mens bent.
- Two-way identificatiemiddelen: hierbij worden er per inlogpoging nieuwe unieke codes gevraagd. Meestal gaat dit met behulp van apparaatje (reader, dongel) of SMS-code. Vrijwel alle banken en andere instellingen die veel waarde hechten aan beveiliging gebruiken deze vorm van identificatie.

***Hoe is de online communicatie met de cliënt beveiligd?***

Wordt er gebruik gemaakt van Secure Sockets Layer (SSL) of een ander veiligheidsprotocol? Een website die gebruikmaakt van het SSL protocol zorgt ervoor dat alle informatie van de desbetreffende website gecodeerd (versleuteld) naar de computer van de gebruiker wordt verstuurd. Alleen als de ontvanger de juiste sleutels heeft kan de informatie gelezen worden. Dit soort websites is te herkennen aan de toevoeging van een 's' in het internetadres (https), waarbij de 's' staat voor 'secure'. Via ***www.ssllabs.com*** is eenvoudig te controleren of een SSL certificaat wordt gebruikt en of deze ook naar behoren werkt.

***Waar, hoe en hoe lang wordt de verzamelde informatie opgeslagen?***

Computers van aanbieders van zogenoemde 'cloud'-diensten staan over het algemeen in Amerika. De informatie van uw cliënten wordt derhalve verzonden naar Amerika en daar opgeslagen. Vanuit Nederland is het lastig om te achterhalen wat er precies met de informatie gebeurt. Ook gelden er in Amerika andere privacyregels dan in Nederland. Duidelijk dient te zijn welke personen toegang hebben tot de computers (servers) waar de gegevens zijn opgeslagen en wie deze gegevens kan en mag inzien of bewerken.

Daarnaast is het van belang dat de informatie op de computers van de leveranciers gecodeerd wordt opgeslagen, zodat eventuele onbevoegden zoals inbrekers (hackers) deze niet kunnen lezen. Het gecodeerd bewaren van de gegevens gebeurt overigens zelden en daarom komen er regelmatig persoonlijke gegevens op straat te liggen.

Meestal wordt een onbeperkte bewaartermijn aangehouden, tenzij deze wettelijk is vastgelegd. Daarom is het verstandig heldere afspraken te maken over de termijn waarop informatie wordt vernietigd.

## Verantwoordelijkheid

In de protocollen van enkele bekende helpwebsites zoals Karify, Minddistrict en Pluform zijn veel van bovengenoemde aandachtspunten redelijk tot zeer goed geregeld. Goede apps zijn te vinden op ***www.artsennet.nl*** waar zorgverleners (medische) gezondheidsapp bespreken en beoordelen. Mocht u gebruik willen gaan maken van een externe aanbieder van e-healthtoepassingen, vraag dan altijd naar hun privacy-voorwaarden en de manier waarop ze de beveiliging hebben georganiseerd. Beoordeel of ze voldoen aan onze beroepscode(s) en de wettelijke regels. Mocht u gaan werken met een eigen systeem, zorg dan samen met de ict-afdeling

[1]CAPTCHA is een acroniem voor: 'Completely Automated Public Turingtest to tell Computers and Humans Apart'.





56

van uw instelling voor een helder protocol. Gebruikt u alleen e-mailprogramma's voor uw begeleiding? Zorg ook dan voor goede beveiliging. Het is uiteindelijk aan u als professionele hulpverlener om een gewogen besluit te nemen over welke instrumenten u wilt inzetten ter online ondersteuning van uw cliënten. De eindverantwoordelijkheid ligt namelijk bij de aanbieder van e-health en dat bent u.

## Referenties


- Blankers, M., Donker, T., & Riper, H. (2013). E-mental health in Nederland. *De Psycholoog,* 12-23. http://www.mblankers.com/pdf/Blankers-Donker-Riper-2013-E-Mental-Health-in-Nederland.pdf
- Christopherson, K.M. (2007). The positive and negative implications of anonymity in internet social interactions: On the internet, nobody knows you´re a dog. *Computers in Human Behavior 23*, pp. 3038-3056.
- Kool, L., Timmer, J., & Est, R. van (red.) (2014). *Eerlijk advies: De opkomst van de e-coach*. Den Haag: Rathenau Instituut.
- Mayer-Schonberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Canada: Eamon Dolan/Houghton Mifflin Harcourt.
- Metze, M. (2012). Tweederde bazen bespiedt personeel, in: *De Groene Amsterdamer, 23*.
- Ribbers, A.P.C, & Waringa, R.A. (2012). E-coaching: Direct aan de slag met Het Nieuwe Coachen. Amsterdam: Boom/Nelissen.
- Reijerman, D. (2014). *CBP dreigt Google met miljoenenboete om privacy-inbreuken. http://tweakers.net/nieuws/100261/cbp-dreigt-google-met-miljoenenboete-om-privacy-inbreuken.html*
- Tilanus, W. (2014). *Factsheet onderzoek online hulpverlening en privacy.* Congres Online Hulp 2014. *http://www.congresonlinehulp.nl/archief/2013-2/parallelsessies-2013/8-petje-op-petje-af-duidelijkheid-over-veiligheid/*


Alexander Waringa is als gedragswetenschapper verbonden aan de Universiteit van Tilburg. Hij is Ambassadeur eHealth van het Nederlands Instituut van Psychologen (NIP) en co-auteur van het handboek: 'E-coaching: Direct aan de slag met Het Nieuwe Coachen'. Daarnaast is hij medeoprichter van eCoachPro ***(www.ecoachpro.nl)*** en initiatiefnemer van het Register voor Certified eCounselors (***www.ecounselorregister.com)*** en de veilige online werkomgeving ***Pluform (www.pluform.com).***