Een gedragscode voor gezondheidsapps

APPS & WEBSITES **Mobile health vormt een nieuwe uitdaging voor de privacy. Een nieuwe Europese verordening over privacy in cyberspace moet de burger beter beschermen in een globale markt. Ontwikkelaars van mHealth-apps vertaalden de Europese regels zelf in een gedragscode.**

©Belga Image

Hoe moet ik toestemming krijgen van gebruikers? Mag ik reclame tonen? Waar moet ik tonen hoe gebruikers me kunnen contacteren? Een eigen Code of Conduct moet dat voor de ontwikkelaars van gezondheidsapps allemaal veel duidelijker maken.

Behoort privacy tot de verleden tijd? Mensen gooien zelf vaak privégegevens te grabbel op open fora en in sociale media. Maar die houding hangt sterk af van de context – en van hoe mensen die inschatten. Als puntje bij paaltje komt, vinden velen het helemaal niet leuk dat zaken over hun privéleven bij personen of instanties terechtkomen voor wie ze niet bedoeld waren. "Als het over gezondheidsgegevens gaat, moet de lat bovendien hoger liggen", stellen **Edwin Jacobs** en **Hans Graux**, van het advocatenbureau **time. lex**, gespecialiseerd in informaticarecht.

> "De gedragscode wordt co-regulerend met de wet" – advocaat Hans Graux

Privacy is geen detail

Het is een kwestie van transparantie, en van controle. "Wat een app doet met je gegevens moet je vandaag nog al te dikwijls zoeken in de 'kleine letters', ergens onder de algemene voorwaarden. De wet eist nochtans dat de gebruiker uitdrukkelijk toestemming moet geven. Wie gegevens over iemand verzamelt, moet duidelijk zeggen waarvoor hij dat doet. En waarvoor hij die nodig heeft. Wat hij wil weten moet in verhouding staan met wat hij ermee voor ogen heeft", voegt Hans Graux eraan toe.

Europese privacyverordening

Een probleem is dat de wetgeving erg complex is. En een app wordt meestal niet alleen voor Belgische gebruikers ontwikkeld. Apps komen van over de hele wereld. "In Europa gold tot nog toe grosso modo als principe dat een producent de wetgeving volgt van de lidstaat van waaruit hij opereert. Maar gevoeligheden verschillen nogal eens tussen de landen. Zo geldt in België de regel dat gezondheidsgegevens alleen onder het toezicht van een arts mogen verwerkt worden. Niet alle Europese landen leggen die regel op", aldus Hans Graux.

Dat soort verschillen maken de zaak vooral voor ontwikkelaars heel ingewikkeld. Ze krijgen te maken met een erg verdeelde markt. Maar ook de gebruiker wordt er niet beter van. "De Europese Commissie werkt aan een *General Data Protection Regulation* – een Europese Privacyverordening. Die moet de bestaande richtlijn uit 1995 vervangen. Twee jaar nadat de Verordening wordt gepubliceerd, wordt ze in alle Europese landen van kracht."

De eerste publieke versie van de Privacyverordening dateert van 2012 maar kreeg nogal wat kritiek en moest worden aangepast. In december 2015 bereikten de Commissie, de Europese Raad en het Parlement een akkoord over de tekst. De tekst ondergaat nog een aantal technische correcties en wordt vertaald naar de officiële talen. De Privacyverordening gaat overigens niet specifiek over gezondheidsgegevens. Die vallen, zoals bij de huidige wetgeving, wel onder de draagwijdte van de nieuwe verordening.

Code of conduct

"De Verordening zal heel wat problemen oplossen", zegt Hans Graux. "Hij legt regels vast die in alle lidstaten gelden. Maar de verordening is voor niet-juristen moeilijk verstaanbaar. Het is een lange tekst is met heel wat jargon."

"Daarom werkte de industrie een *Code of Conduct* uit – time. lex tradt op als *editor*. Het zijn de ontwikkelaars zelf die in die gedragscode de regels verwoorden. Dat moet het voor hen allemaal veel duidelijker maken. Hoe moet ik toestemming krijgen van gebruikers? Mag ik reclame tonen? Waar moet ik tonen hoe gebruikers me kunnen contacteren? Wat moet ik doen als een ander bedrijf voor mijn servers zorgt? Eigenlijk vind je dat allemaal in de Privacyverordering terug, maar deze gedragscode gaat specifiek over de ontwikkeling van gezondheidsapps.

Klare regels

De gedragscode beschrijft om te beginnen wat gezondheidsgegevens zijn. Dat is ook contextueel bepaald. Een fitness-app of een app die je helpt op je voeding te letten, valt veeleer onder de noemer levensstijl. De app heeft misschien wel je lichaamsgewicht nodig. Maar wat als dat erg hoog is? Dan wordt het een medisch gegeven. "Zo een app geeft mogelijk prijs dat je diabetes hebt. Die gegevens moeten dan niet bij een verzekeraar terechtkomen", geeft Edwin Jacobs nog als voorbeeld.

Een greep uit de regels:

- De gebruiker moet duidelijke informatie krijgen en uitdrukkelijk zijn toestemming geven. Belangrijke items mogen niet verscholen zitten in een lange tekst.
- De gebruiker moet vlotte toegang behouden tot zijn gegevens.
- Bij het ontwerpen van de apps gelden de principes van *privacy by design* en *privacy by default*: wanneer de ontwikkelaar keuzes maakt, kiest hij de meest beschermende oplossing.
- Beveiliging moet de standaard zijn: encryptie, anonimisering, verwijdering van oude gegevens...
- Gezondheidsdata kunnen alleen met uitdrukkelijke toestemming van de gebruiker worden doorgegeven aan bijvoorbeeld mogelijke adverteerders.

Controleerbaarheid

"De Code of Conduct heeft op zichzelf geen juridische kracht. Maar de bedoeling is de zogenaamde *article 29 working party* – die alle nationale toezichthouders op Europees niveau verenigt – de tekst naleest en valideert. Daardoor kan men de tekst niet zomaar naast zich neerleggen. Het is dan niet meer een louter autoregulerende tekst van de industrie. Hij wordt dan co-regulerend met de wet", aldus Hans Graux.

De ontwikkelaars zullen de mogelijkheid hebben de gedragscode te onderschrijven. Aan een systeem om dat te registreren, wordt gewerkt. De Europese Privacyverordening zal zaken verder in beweging brengen, menen de advocaten van time. lex. Er zal niet alleen meer duidelijkheid komen, maar zeer waarschijnlijk ook meer controle.

Wouter Colson

Big data

Hans Graux: "Een app op je smartphone kan een hoop gegevens over de eigenaar registreren. En naarmate meer zaken over een persoon geregistreerd worden, worden de risico's groter. Er komen nu ook steeds meer *wearables* op de markt. Daarnaast krijg je het *Internet of Things*, dat allerlei gegevensbronnen met elkaar kan verbinden. En pas daar dan big data-analyse op toe." Ook op dit vlak schept de Code of Conduct meer klaarheid over welke regels er gelden. De producent van de app blijft verantwoordelijk – hij biedt de gebruiker garanties. Hij moet zich ervan vergewissen dat die gerespecteerd blijven wanneer andere partijen de persoonsgegevens verwerken.