E. Kindt en Corien Prins[1]

Identiteit in de informatiemaatschappij

35 *Deze special rond 'Identiteit in de informatiemaatschappij' hebben wij voor u samengesteld omwille van het toegenomen belang van identiteit en van identiteitsgegevens in onze samenleving. In het editorial wordt reeds aangehaald hoe de concepten van (digitale) identiteit en identificatie zeer complex worden. Daarenboven lijkt door de groeiende invloed van de technologie identiteit te vervormen tot een groepsidentiteit waarop een individu geen grip meer dreigt te hebben.*

Het eerste artikel 'Identiteitsgegevens en -beheer in een digitale omgeving: een juridische benadering' van *Kindt* en *Van der Hof*, biedt een overzicht van de paradox aangaande identiteit in netwerken. Enerzijds kunnen gegevens in netwerken steeds eenvoudiger herleid worden tot identificeerbare personen. De auteurs illustreren deze stelling met de discussie die gaande is omtrent IP-nummers. Volgens sommigen valt de verwerking van IP-adressen onder de wetgeving inzake de bescherming van persoonsgegevens, omdat het mogelijk is de identiteit van de betrokken personen terug te vinden, terwijl anderen dit betwisten. Maar ook surf-, klik- en zoekgegevens worden steeds vaker gekoppeld aan identificeerbare personen. Anderzijds staat het zogenoemde identiteitsmanagement op netwerken voor steeds grotere uitdagingen. Op het internet geldt 'nobody knows you're a dog'. Terwijl authenticatie- en autorisatieprocedures steeds belangrijker worden, lijkt het steeds moeilijker om deze op betrouwbare wijze en met respect voor de rechten van het individu uit te voeren.
In het daaropvolgend artikel 'Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België' van *Dumortier* en *Robben*, gaan de auteurs dieper in op de noodzaak om over een sluitend gebruikers- en toegangsbeheer te beschikken bij de organisatie van het elektronische gegevensverkeer bij de overheid. De Belgische aanpak werkt met een gedecentraliseerd gebruikers- en toegangsbeheer, wegens de gevaren voor de persoonlijke levenssfeer van te vergaande gecentraliseerde verwerkingen. Dienstenintegrators moeten zorgen voor de correcte uitwisseling van de gegevens. Het artikel geeft aan welke bouwstenen daarbij gebruikt worden – zoals de Belgische elektronische identiteitskaart en gevalideerde authentieke bronnen – en toont de complexiteit aan van de organisatie van geïntegreerde elektronische diensten ten dienste van de burger.
Van der Meulen heeft het in haar artikel 'Identiteitsfraude: de eerste stap, nu nog de rest' over identiteitsfraude. Over het begrip bestaat geen eensgezindheid, hetgeen de strafbaarstelling bemoeilijkt. In verband met identiteitsfraude bespreekt de auteur ook de initiatieven op het gebied van de zogenoemde *data security breach*-aanpak, waarbij betrokkenen op de hoogte gebracht moeten worden over incidenten waarbij hun identiteits- of andere persoonsgegevens lekten. Deze nieuwe invalshoek zou bedrijven er ook toe moeten aansporen om voorzichtiger met persoonsgegevens om te gaan en om op die manier identiteitsfraude voorkomen.
In de bijdrage 'Identiteit en openbaarheid in sociale online-omgevingen' van *Marbus, Fennell-Van Esch* en *Roosendaal* onderzoeken de auteurs hoe online- en offline-identiteiten zich met elkaar verhouden. Zij komen tot de vaststelling dat deze begrippen met elkaar lijken te versmelten, ook al zijn er verschillen tussen een online-identiteit in een sociaal netwerk, zoals Hyves of MySpace, en een online-identiteit in een spelomgeving. Voor een online(spel)identiteit lijkt het doorgaans geen probleem om een andere identiteit aan te nemen en zijn de verschillenden tussen de offlinepersoon en het online-individu doorgaans groter. Verwijzend naar een (weliswaar in eerste aanleg) veroordeling van een vrouw wegens smaad voor uitlatingen in een online afgesloten ruimte, waar de rechter het 'woonkamerargument' afwees, stellen de auteurs een aantal criteria voor om de openbaarheid van onterende berichten op sociale netwerksites te beoordelen. De toegankelijkheid van de informatie dient volgens hen centraal te staan, teneinde recht te doen aan de eigenheid van de onlinewereld. Het samensmelten van de virtuele identiteit met de identiteit in de reële wereld betekent volgens de auteurs niet dat deze op dezelfde manier behandeld moeten worden, omdat er te veel verschillen bestaan tussen beide werelden. Weliswaar zal men ook rekening moeten blijven houden met de rechten van de betrokken slachtoffers van de uitlatingen.
In het laatste artikel van dit themanummer 'Ik ben user 712. Recht op toegang tot persoonsgegevens en op mededeling van de logica van geautomatiseerde verwerking', beargumenteert *Schreurs* treffend hoe door de verwerking en aaneenkoppeling van persoonsgegevens, een slimme omgeving ontstaat waarin ongemerkt op maat gesneden informatie wordt aangeboden aan het individu, vaak op basis van groepsprofielen. In deze intelligente omgeving (*ambient intelligence*) is het volgens de auteur van primordiaal belang dat het individu inzage heeft in de gegevenscollectie, de verwerking, de verantwoordelijk, de logica en de oorsprong van de gegevens. Het recht van toegang tot de gebruikte databanken en profielen ligt echter niet steeds voor de hand en het is hierbij ons inziens zeer de vraag of het grondrecht op respect voor privacy en de wetgeving gegevensbescherming voldoende mogelijkheden bieden om de zeggenschap en de controle van het individu te bewaren.
Veel leesplezier!

1 Mw. mr. Els Kindt is redacteur van *Computerrecht* en wetenschappelijk onderzoeker van het Interdisciplinair Centrum voor Recht en ICT (ICRI) van de K.U. Leuven, IBBT. Mw. prof. mr. Corien Prins is raadslid bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en hoogleraar bij Tilburg Institute for Law, Technology, and Society (TILT), Universiteit Tilburg.