

De jacht op informatie

Computers bieden vele voordelen. Computers zijn efficiënt en hebben saaiere arbeidsprocessen overgenomen van de mens. Complex wetenschappelijk onderzoek, bijvoorbeeld op het gebied van genetica, zou onmogelijk zijn zonder computers. Door de moderne medische diagnostiek is de gemiddelde leeftijd gestegen. Met behulp van DNA-databanken kunnen ernstige misdrijven worden opgelost.

De doorbraak van communicatie- en informatietechnologie heeft echter ook een schaduwzijde.

Steeds meer mensen ervaren de druk van de informatieoverlast en zuchten onder de bereikbaarheidsterreur. De invoering van moderne identificatiesystemen op basis van biometrie en chip-technologie heeft geleid tot druk op belangrijke grondrechten. Een groeiende bron van zorg, waar we allemaal mee te maken kunnen krijgen, is computercriminaliteit of cybercrime.

Zorgen

Nadat de elektronische persoonsregistratie in de jaren tachtig een grote vlucht nam, moest er beschermende wetgeving komen. Voortvloeiend uit artikel 10 van de Grondwet werd in 1989 de Wet persoonsregistraties ingevoerd. Inmiddels is deze vervangen door de Wet bescherming persoonsgegevens. Deze wet voorzag ook in de instelling van een toezichthouder, de Registratiekamer (thans het College Bescherming Persoonsgegevens, het CBP). Een terechte maatregel, zoals snel zou blijken. In het Jaarverslag 1997 signaleert de Registratiekamer een zorgelijke ontwikkeling. Uit signalen was gebleken dat de klinisch genetische centra in ons land, die zich bezighouden met erfelijkheidsdiagnostiek, 'steeds meer vragen van zorgverzekeraars krijgen over de individuele diag-

noses en relaties van verzekerden met andere individuele personen'. Daarmee werd een grens overschreden. Genetische kennis kan grote invloed hebben op het verkrijgen van een levensverzekering of bij sollicitaties. Het baarde de toezichthouder vooral zorgen dat het bij genetisch onderzoek niet alleen gaat om voorspellende informatie over individuen, maar over complete gezinnen en zelfs families.

Informatiemisbruik moet streng worden bestreden

Immense dossiers

Dit praktijkvoorbeeld illustreert dat de jacht op informatie is geopend. Informatie die voor een bedrijf of overheid nuttig is, kan echter de persoonlijke levenssfeer aantasten en grote gevolgen hebben voor iemands levensloop. Misbruik moet daarom streng worden bestreden, zeker met het oog op de grote veranderingen die op het gebied van persoonsregistratie op ons afkomen.

Door koppeling van bestanden ontstaan enorme databanken, vaak met gevoelige informatie

(bijvoorbeeld over levensbeschouwing en gezondheid). Binnen enkele jaren zullen immense elektronische persoonsdossiers operationeel zijn. Gebruik van ons unieke persoonsnummer, het Burger Service Nummer, is niet langer voorbehouden aan overheden. Het systeem wordt ook gebruikt in de private sector, door zorgverzekeraars en zorgverleners. Terecht eist de burger dat informatie optimaal is beveiligd. Alleen bevoegde personen mogen toegang hebben tot databestanden. Bovendien moet de opgeslagen informatie, bijvoorbeeld over medische diagnoses, correct zijn. Ik ben overtuigd voorstander van gebruik van het wettelijke recht op inzage en correctie van persoonsgegevens.

De wet op het net

Sinds de jaren tachtig hebben we te maken met cybercrime en het aantal gevallen neemt snel toe. Volgens het Handboek Digitale Criminaliteit (uitgave: Van Duuren Media) omvat cybercrime alle misdrijven die zijn verwezenlijkt met behulp van specialistische computerkennis, hardware of software. Bekende delicten zijn het ongeoorloofd verschaffen van toegang tot een computersysteem (computervredebreuk) of het onbruikbaar maken van een sys-



De jacht op informatie is geopend.

teem, kopiëren van vertrouwelijke gegevens, ongeoorloofd verwijderen van computerdata en het versturen van virussen.

Veel westerse landen zijn slecht voorbereid op cybercrime

Door de invoering van de Wet computercriminaliteit werd het Wetboek van strafrecht afgestemd op de technologische vooruitgang. Overheden en bedrijven als zorgverzekeraars, zorgverleners en banken beheren immense computerbestanden en dienen alert te zijn op cybercrime. Het grensoverstijgende karakter van internet maakt handhaving van het computerstrafrecht moeilijk. Daarom ondertekende Nederland in 2001 het Internationale Cybercrimeverdrag.

Cyberwar

Cybercrime is ook een militair-strategisch instrument. Moderne wapensystemen, maar ook infrastructuurle objecten en energiecentrales zijn computergestuurd en daardoor gevoelig voor mani-

pulatie en ontregeling. Deskundigen voorzien dat toekomstige gewapende conflicten voor een belangrijk deel zullen worden uitgevochten vanachter beeldschermen. China voert regelmatig cyberaanvallen uit op westerse doelen. Hierdoor kunnen verschuivingen optreden in de mondiale machtsverhoudingen.

Tegelijk openbaart zich een wrange tegenstelling. Overheden die op nationaal niveau cybercrime bestrijden, maken er op het internationale toneel gebruik van om hun strategische doelstellingen te verwezenlijken. Op 4 en 8 maart 2010 werd in publicaties in de Engelse dagbladen *The Guardian* en *The Times* gewaarschuwd voor de gevolgen van cyberwar. Veel westerse landen zijn onvoldoende voorbereid op deze dreiging.

Mondiaal machtsmisbruik

Een ethisch dilemma: is het acceptabel om in te breken in computersystemen om de beveiliging te testen, zoals gebeurde bij de OV-chipkaart? Voorstanders menen van wel, mits er geen schade wordt aangericht en de eigenaar achteraf wordt ingelicht over de kwetsbaarheid van het systeem. Vast staat dat cybercrime fundamentele grondrechten kan aantasten.

Christelijk-ethisch bezien blijft het een moeilijk onderwerp. In Bijbelse tijden waren er geen computers. Toch is het, gezien de dominante rol van de computer in onze samenleving en de afhankelijkheid ervan, belangrijk dat we hierop een bijbelse visie ontwikkelen. Een aantal aspecten is niet aan twijfel onderhevig. Computervredbreuk met als doel informatie te krijgen, kan worden beschouwd als diefstal en daarover is de Bijbel duidelijk (Ex. 20:15). Niet zelden worden gestolen gegevens gebruikt om de bankrekening van een benadeelde te plunderen of iemand middels informatie te benadelen. De Bijbel geeft ook voorbeelden, waarbij informatie werd misbruikt om personen te beschadigen en de persoonlijke levenssfeer aan te tasten. De profeet Daniël kreeg te maken met jaloerse mensen in zijn omgeving, die informatie over zijn geloofsbeleving verklikten bij de Koning. Daardoor kwam hij in de leeuwenkuil terecht (Dan. 6:12-14).

Het profetisch Woord is rotsvast en betrouwbaar

Alert blijven

Belangrijke reden om alert te blijven is het risico van machtsmisbruik op mondiaal niveau. Technologische of wetenschappelijke ontwikkelingen op zich vormen geen bedreiging. Het probleem ligt bij de mensen erachter die processen sturen en bereid zijn hun macht te misbruiken. In Openbaring 13 wordt een mondiaal dictatoriaal systeem beschreven dat beschikt over machtsmiddelen om mensen te manipuleren en uit te sluiten van het sociale en economische verkeer (vers 14-17). Eeuwenlang meenden Bijbeluitleggers dat hier sprake was van beeldspraak. In onze eenentwintigste eeuw kan niemand meer ontkennen dat het technisch realiseerbaar is. Het profetisch Woord is rotsvast en betrouwbaar. ◻