

21 februari 2011

Technology Assessment



Ontwerp van databases: een pleidooi voor structureel toezicht

Geert Munnichs

Leidt het elektronisch kinddossier tot minder kindermishandeling? Kan de OV-chipkaart veiliger? Draagt het Schengen Informatie Systeem bij aan een betere bewaking van de buitengrenzen van Europa? En wat doen bedrijven met de klantgegevens die ze op internet verzamelen?

Computersystemen slaan steeds meer gegevens over ons op. Overheden en bedrijven maken daarvan gebruik om de efficiëntie te verhogen of de communicatie te verbeteren. Maar doen databases wel wat ze moeten doen? Hoe staat het met de beveiliging van al die gegevens? Hoe betrouwbaar zijn ze? En welke mogelijkheden hebben personen om controle uit te oefenen op hun eigen gegevens?

Aan de hand van zes casestudies gaat Databases in op deze vragen, en komt tot vrij onthutsende conclusies. Aan het gebruik van databases blijken allerlei risico's te kleven waaraan vaak onvoldoende aandacht wordt besteed. De beloftes van ICT dreigen daarmee in hun tegendeel om te slaan. De risico's hangen samen met de architectuur – of: het ontwerp – van databases. De studie laat zien dat andere ontwerpkeuzes mogelijk zijn, waarbij meer aandacht uitgaat naar de positie van de reiziger, burger of consument over wie gegevens worden verzameld.

Technology Assessment

Databases

Over ICT-beloftes, informatiehonger
en digitale autonomie

Geert Munnichs, Mirjam Schuijff & Michiel Besters (redactie)

Rathenau Instituut

organisatie
verandering
debat
technology
R



Zes case studies



Rathenau Instituut

21 februari 2011

Technology Assessment

- OV-chipkaart & kilometerheffing
- Elektronisch patiëntendossier
- Elektronisch kinddossier
- Klantenprofielen op internet
- Schengen Informatiesysteem
- Gemeentelijke basisadministratie

Ontwerp van databases



Rathenau Instituut

21 februari 2011

Technology Assessment

- Ontwerp/architectuur centraal
- Technisch ontwerp (soort gegevens, centrale - decentrale opslag, toegang, versleuteling gegevens) en functioneren binnen bredere context
- Samenhang ontwerp met doelen
- Samenhang ontwerp met risico's
- Gevolgen voor de burger
- Lessen voor doordacht ontwerp

Beveiliging heet hangijzer



Rathenau Instituut

21 februari 2011

Technology Assessment

- OV-chipkaart vrij eenvoudig te kraken
- EPD kwetsbaar door vele UZI-passen, gebrekking risicobewustzijn en controle achteraf van raadplegingen
- Betere beveiliging door zwaardere technische maatregelen:
 - zwaardere OV-chip
 - decentrale opslag waarbij patiënt toegang beheert
→ ontwerpkeuzes
- Keuze Mifare Classic-chip vanwege lagere kosten
- Beveiliging is nooit 'af' en vraagt om continue monitoring

Betrouwbaarheid gegevens



Rathenau Instituut

21 februari 2011

Technology Assessment

- Fouten in registraties vormen serieus probleem
- Verschrijvingen, verouderde data, ID-diefstal, interpretatieproblemen
- EPD kan leiden tot nieuwe medische fouten
- EKD: risicoprofilering vormt grof instrument
- Klantenprofielen: statistische verbanden in consumentengedrag creëren virtuele identiteit, met flinke foutmarge
- Burger kan nadelen ondervinden: registratie als 'probleemgezin' of 'wanbetaler'

Rechtspositie burger



Rathenau Instituut

21 februari 2011

Technology Assessment

- Wettelijk inzage- en correctierecht in praktijk vaak lastig te effectueren
- OV-chipkaart, SIS, Klantenprofielen, EKD
- Databases vaak toegesneden op behoeften opdrachtgever, terwijl belangen burger ondergeschikt zijn
- Fundamentele vraag: vergroot gebruik database afhankelijkheid of autonomie burger?
- Klantenprofielen: dataverzameling grotendeels onzichtbaar
 - niet achterhaalbaar waarom klant bepaalde behandeling krijgt
 - asymmetrie/machtsongelijkheid klant - bedrijf

Doen databases wat ze moeten doen?



Rathenau Instituut

21 februari 2011

Technology Assessment

- EKD: risicoprofilering van ieder kind → onwerkbaar grote aantallen 'mogelijke' risicokinderen → schiet zijn doel voorbij?
- SIS: technisch-organisatorische problemen door veelheid aan politieke doelstellingen (van 7 naar 25 landen; uitbreiding functies)
- Te hoge ambities kunnen in tegendeel omslaan
- Select before you collect
- Reflectie nodig op eigenlijke doelstelling

Niet risicovrij



Rathenau Instituut

21 februari 2011

Technology Assessment

- Databases zijn geen risicovrije systemen
- Geen toevalligheden/slordigheden, maar patroon
- Te vaak te weinig aandacht voor risico's (beveiliging, betrouwbaarheid, nieuwe afhankelijkheden, doelmatigheid)
- Vooral burger de dupe
- Meer aandacht nodig voor risico's en voor positie burger

Kan het anders?



Rathenau Instituut

21 februari 2011

Technology Assessment

- 'Dikke variant' kilometerheffing
- Versleuteling gegevens in registratiekastje auto: alleen automobilist heeft toegang tot ritgeschiedenis
- Exploitant krijgt alleen versleutelde data
- Automobilist heeft bewijsmateriaal bij 'spookrekening'
- Privacyvriendelijk ontwerp als reëel alternatief
- ICT kan positie burger ook versterken
- Vereist andere keuzes in ontwerpfase

Aanbevelingen voor ontwerp



Rathenau Instituut

21 februari 2011

Technology Assessment

1. Maak zoveel mogelijk gebruik van technische maatregelen ter bescherming van gegevens
 2. Versterk de positie van de burger:
 - faciliteer het inzage- en correctierecht
 - geef de burger zo veel mogelijk regie over gegevens
 3. Houd het simpel: kies een welomschreven doel en beperk gegevensverzameling tot daarvoor noodzakelijke gegevens
- Aanbevelingen hangen samen: beveiligingsniveau, inbouw rechten burgers en doeleinden database staan niet los van elkaar
 - Bv: beveiliging kan botsen met inzage door burgers, of het delen van data

Aanbevelingen toezicht



Rathenau Instituut

21 februari 2011

Technology Assessment

- Iedere ontwerpkeuze heeft voor- en nadelen → behoeven reflectie
- Ontwerpkeuzes vergen:
 - kennis van (on)mogelijkheden van ICT
 - kennis van alternatieve ontwerpkeuzes
 - reflectie op doeleinden
- Vanwege groeiend belang van digitalisering structureel toezicht nodig op keuzes in ontwerpfase
- Bijvoorbeeld in vorm van ICT-autoriteit