ISSN 1879-9523
journal of chain-computerisation
information exchange for chain co-operation
Universiteit Utrecht

Wetenschappelijk artikel

Keteninformatisering en privacy

M. van der Veen

Journal of Chain-computerisation
Information Exchange for Chain Co-operation

2011 – Volume 2, Art. #11

Ontvangen: 1 maart 2011
Geaccepteerd: 1 april 2011
Gepubliceerd: 14 april 2011

2011 – Volume 2, Art. #11
URN:NBN:NL:UI:10-1-101416
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Uitgever: Igitur publishing in samenwerking met het Department of Information and Computing Sciences, Universiteit Utrecht

Keteninformatisering en privacy

M. van der Veen
Capgemini Consulting, cluster Veiligheid en rechtsketen
Postbus 2575, 3500 GN Utrecht
E-mail: maveen@capgemini.com

Samenvatting: Het leerstuk Keteninformatisering levert een grote bijdrage aan *privacy by design* doordat noodzakelijkheid, proportionaliteit en doelbinding van gegevensuitwisseling in de methodiek centraal staan. Toch ontstaan, ondanks toepassing van het leerstuk, grote risico's voor de privacy. We gaan in op deze risico's en bieden een oplossing in de vorm van een privacyscan, de Smart Privacy Approach. Deze privacyscan biedt een hulpmiddel om de privacyrisico's van de ketensamenwerking te operationaliseren. Dit helpt om het leerstuk zorgvuldiger toe te passen en waar risico's voor de privacy ontstaan maatregelen te nemen.

Trefwoorden: Keteninformatisering, privacy, 'privacy by design', risico

1 Keteninformatisering en privacy

Privacybescherming is een terugkerend en fundamenteel vraagstuk in debatten over de inrichting van de zorg- en veiligheidsketens. Voorbeelden hiervan zijn het Elektronische Patiëntendossier (EPD), de opname van biometrische gegevens in het paspoort en de aanpak van veelplegers en jeugdige criminelen. Meer ketensamenwerking leidt tot een groei van het aantal systemen en koppelvlakken, redundante opslag van gegevens en meer betrokken partijen, wat dan weer leidt tot problemen op het gebied van beheersbaarheid, overzicht in informatiestromen en (mede hierdoor) privacybescherming. In antwoord op de ontwikkeling van de groeiende, grootschalige keteninformatisering is het leerstuk Keteninformatisering ontstaan (Grijpink, 1997). Een belangrijk voordeel van dit leerstuk is dat het privacyaspect al vanaf het begin bij de inrichting van ketensamenwerking en in het ontwerp van keteninformatiesystemen wordt meegenomen (*privacy by design*). Het leerstuk bevat daarnaast al diverse handvatten om privacybescherming in ketens te vergroten (Grijpink, 1999, pp. 137 e.v.; Grijpink, 2010, p. 16).

Er is echter een aanvulling op het leerstuk nodig, omdat de praktijk anders werkt dan volgens de uitgangspunten van het leerstuk het geval is. Hierdoor ontstaan, ondanks het *privacy by design*-karakter van Keteninformatisering, alsnog grote privacyrisico's. Dit wordt beschreven in paragraaf 2. Een oplossing voor deze privacyproblemen in een keten is een privacyscan waarbij niet een systeem of theoretisch kader, maar de risico's voor de betrokken personen centraal staan. Deze risico's zullen vragen om reflectie op het informatieproces. Die kan leiden tot betere toepassing van het leerstuk of het nemen van aanvullende, risicoverlagende maatregelen.

2 Kritiek op privacywaarborgen

Keteninformatisering speelt zich volgens het leerstuk Keteninformatisering af binnen een context die wordt gekenmerkt door irrationele besluitvorming, samenwerking van partijen rondom een dominant ketenprobleem en gegevensuitwisseling op meerdere niveaus. De partijen in de keten zullen in deze context alleen een minimale, maar effectieve informatiedeling tot stand kunnen

brengen. De beste privacybescherming bieden keteninformatiesystemen waarbij geen centrale opslag of uitwisseling van broninformatie mogelijk is en databases alleen door verwijsindexen informatie kunnen toetsen. Maar ook in minder vergaande oplossingen dwingt de ketenaanpak tot een kritische houding ten opzichte van informatiedeling.

Het is echter onwaarschijnlijk dat uitgangspunten van het leerstuk Keteninformatisering zo worden geïmplementeerd dat ze de beoogde betere privacybescherming ook daadwerkelijk kunnen afdwingen, omdat:

- irrationele besluitvorming kan worden doorbroken door politieke druk, consensus of ter beschikking stellen van meer middelen, zoals tijd en geld of subsidies. Lastige vragen en problemen kunnen worden 'afgekocht';
- het dominante ketenprobleem onvoldoende scherp gedefinieerd en getoetst zal worden binnen een omgeving die minder irrationeel acteert dan het leerstuk veronderstelt. Dat kan leiden tot breder gebruik van de minimale gegevensset en tot uitwisseling van een set gegevens die breder dan noodzakelijk is;
- in een omgeving waarin al samenwerkingsverbanden bestaan men eerder voor oplossingen zal kiezen die makkelijk in de bestaande structuren in te passen zijn, wat leidt tot bredere verspreiding van gegevens dan noodzakelijk is (Kouwenhoven, 2007).

Vanwege deze omgevingsfactoren is het onwaarschijnlijk dat de kritische houding waar toepassing van het leerstuk toe leidt concrete werkelijkheid wordt. Er zal meer informatie worden gedeeld en opgeslagen dan noodzakelijk is, met alle privacyrisico's van dien. Om deze risico's in te dammen zullen privacyvraagstukken gestructureerd moeten worden aangepakt, te beginnen met het beter benoemen van privacyproblemen.

3 Privacy concretiseren: Smart Privacy Approach

Om de borging van privacy in een bepaalde ketensamenwerking kritisch te toetsen moet de privacy beter 'vast te pakken' zijn. Allereerst is er behoefte om privacy beter te beschrijven en te operationaliseren. We onderkennen hierbij de volgende problemen. Ten eerste zal een burger een privacyschending anders percipiëren dan een instelling 'met een missie'. Ten tweede speelt een privacyincident al gauw op meerdere niveaus tegelijk: van een individuele burger tot het niveau van mensenrechten. Waar ligt bijvoorbeeld de grens tussen een camera als handig hulpmiddel en Big Brother? Ten derde kent privacy een enorme dynamiek vanuit de specifieke sociale context waarbij de grenzen van privacy kunnen veranderen onder invloed van incidenten. Burgers zijn geneigd privacy in te leveren in ruil voor meer veiligheid, mede omdat veiligheid concreet is en privacy een abstract begrip blijft.

Om privacyvraagstukken concreet te maken hebben we een gestructureerde privacyscan ontworpen uitgaande van het werk van Daniel Solove. Solove stelt dat privacy een paraplubegrip is voor zestien risico's van informatieverwerking tussen personen en organisaties (Solove, 2006; 2008). Privacy is ongrijpbaar in een uitspraak als 'koppeling van bestanden in ketensamenwerking schendt onze privacy'. Met de in dit artikel geïntroduceerde Smart Privacy Approach zou het probleem benoemd kunnen worden als 'aggregatie van bronbestanden verhoogt het risico op foutief hergebruik van gegevens en het trekken van foutieve conclusies over personen (false positives en negatives) en vermindert de controleerbaarheid van de data.' Nadat de privacyvraagstukken met deze scan zijn geconcretiseerd zijn gerichte, concrete oplossingen benoembaar.

De stappen van deze privacyscan – de Smart Privacy Approach - zijn:

(1) beschrijving van het te onderzoeken privacyvraagstuk. In deze eerste stap worden de ketenopgave en de informatieverwerking daarbinnen benoemd. De informatiestroom van persoonsgegevens vormt het uitgangspunt, zoals 'het vastleggen van patiëntgegevens in een database' in het geval van het EPD. Net als bij de ketenaanpak is het scherp stellen van het vraagstuk belangrijk en kan een vraagstuk om meerdere analyses vragen;

(2) analyse van informatierisico's tijdens de informatieprocessen. In deze tweede stap analyseren we welke van de informatierisico's op kunnen treden. Vaak blijkt slechts een beperkt aantal van de zestien genoemde risico's een rol te spelen;

(3) verdieping in informatierisico's en actoren. In deze derde stap wordt de analyse van de risico's voor de betrokken actoren op drie manieren verdiept. Allereerst vraagt het om het privacyvraagstuk vanuit breder perspectief van een grootschalige toepassing te zien. Op individueel niveau is één camera geen probleem, voor een gemeenschap kunnen 50 of 1000 camera's dit wel vormen. Daarnaast vraagt het om actoren te benoemen die mogelijkerwijs niet direct bij het vraagstuk betrokken zijn, maar wel te maken krijgen met *gevolgen* van activiteiten. Tenslotte vraagt het de factor tijd mee te nemen en risico's voor actoren op langere termijn te benoemen;

(4) benoeming van de risicoverlagende maatregelen per privacyprobleem.

4 Resultaat

Het resultaat van de Smart Privacy Approach is een gestructureerde analyse en heldere benoeming van het privacyvraagstuk, toetsing op risico's voor de privacy van de betrokken personen en inzicht in de betrokken actoren en het niveau waarop zij acteren (lokaal, regionaal of landelijk). Pas hierna kunnen passende oplossingen en concrete acties worden benoemd. De scan voorkomt dat belangrijke aspecten van het privacyvraagstuk over het hoofd worden gezien.

Het leerstuk Keteninformatisering biedt de mogelijkheid zeer kritisch te kijken naar de noodzakelijkheid, proportionaliteit en doelbinding van de gegevensdeling. Als aanvulling op keteninformatisering biedt de voorgestelde privacyscan een hulpmiddel om de privacyrisico's van de ketensamenwerking te operationaliseren. Hiermee draagt het bij aan een zorgvuldiger toepassing van het leerstuk en verbetert de privacy binnen ketensamenwerking.

Biografie: Drs. M. (Martijn) van der Veen (1978) studeerde Bestuurskunde aan de Universiteit Twente en volgt de opleiding Nederlands Recht aan de Open Universiteit. Sinds 2006 is hij werkzaam bij Capgemini Consulting op het terrein van organisatieverandering en procesverbetering, sinds 2008 vooral in de veiligheidssector. Zijn speciale aandacht heeft privacy, de toetssteen van *good information governance.*

Literatuurverwijzingen

Grijpink, J.H.A.M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving*. Den Haag: Sdu Uitgevers.

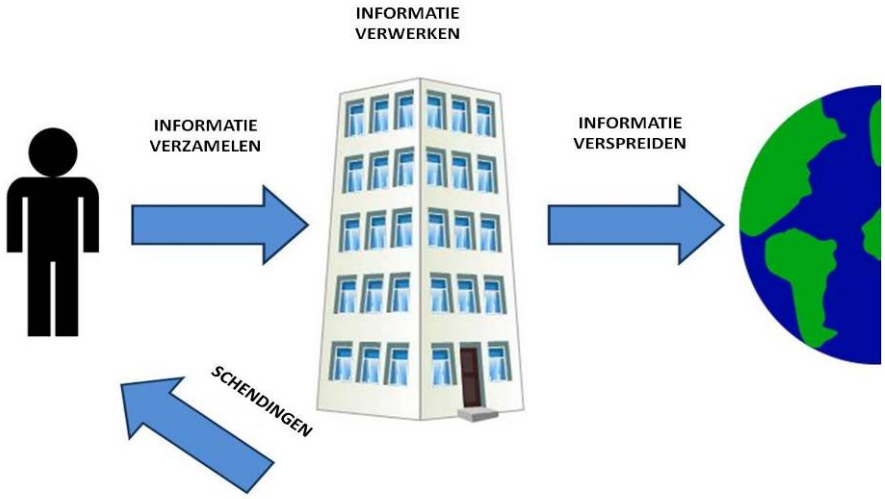
Grijpink, J.H.A.M. (2010). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling*. Den Haag: Boom/Lemma Uitgevers.

Kouwenhoven, R. & Binnekamp, R. (2007). Ketensamenwerking in de lokale veiligheidspraktijk. In J.H.A.M. Grijpink, T.A.M. Berkelaar, D.G.H. van Breemen, B.P.M.J. Dommisse & R.J. Steenkamp (red.), *Geboeid door ketens: Samen werken aan keteninformatisering*. Den Haag: Platform Keteninformatisering.

Solove, D.J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477.

Solove, D.J. (2008). *Understanding Privacy*. Cambridge MA: Harvard University Press.

A. Bijlage: Risico's van informatieverwerking



Risico's van informatieverwerking
Informatie verzamelen
Observatie
Bevraging
Informatie verwerken
Combineren
Identificatie
Onzorgvuldige omgang
Hergebruik
Rechteloosheid
Informatie verspreiden
Schending van vertrouwen
Onthulling
Blootstellen
Toegankelijkheid
Chantage
Vermomming
Vervorming
Schendingen
Indringing
Ongewenste besluitvorming