

Minister van Veiligheid en Justitie: waarborg privacy in Veiligheidshuizen!

Prof. mr. drs. M.R. Bruning en mr. J.J. Oerlemans*

4

1 Inleiding

Veiligheidshuizen zijn in Nederland als paddenstoelen uit de grond geschoten. In deze gebouwen komen allerlei instanties voor verschillende typen casusoverleg (zoals Veelplegers, Huiselijk Geweld en Nazorg) bij elkaar om informatie te delen en besluiten te nemen over de problematiek van een persoon. Hierbij is een tendens zichtbaar dat steeds meer gegevens tussen de domeinen zorg en strafrecht worden gedeeld teneinde optimaal te reageren in een concrete casus (bijvoorbeeld door hulpverlening aan te bieden of een passende handhavingsmaatregel op te leggen).

De regering en bij een casusoverleg betrokken professionals zijn enthousiast over het casusoverleg. Met de gegevensuitwisseling kan een gedetailleerd(er) beeld worden verkregen van de betrokkenen en kan zorg of afdoening op maat worden geleverd. Organisaties zijn op de hoogte van elkaars betrokkenheid bij een individu, waardoor efficiënter en effectiever kan worden gewerkt. Dit blijkt bijvoorbeeld uit het onderzoek 'Vastpakken niet meer loslaten' van onderzoeksbureau Nelissen uit juni 2010 (p. 24) en dit wordt benadrukt in de brochure 'Veiligheidshuizen' uit maart 2010 (p. 10).

Uit het onderzoek van het Integraal Toezicht Jeugdzaken (een samenwerkingsverband van vijf rijksinspecties die toezicht houden op organisaties en voorzieningen voor jongeren) in 2009 naar Veiligheidshuizen blijkt echter dat een gebrek aan kennis over privacywetgeving er vaak toe leidt dat onvoldoende informatie wordt uitgewisseld, terwijl die informatie van belang is voor hulpverlening aan jongeren. In hetzelfde onderzoek staat dat 'privacy als argument wordt gebruikt' om informatie niet te delen. Dit blijkt tevens bijvoorbeeld uit een onderzoek naar nazorg van ex-gedetineerden (*Justitiële Verkenningen* (33) 2007, nr. 4).

Wij zijn van mening dat het probleem bij dergelijk ketenoverleg juist omgedraaid is: er worden veelal te gemakkelijk gegevens voor brede doelen tussen private en publieke instellingen uitgewisseld en dit bedreigt het recht op de persoonlijke levenssfeer – de informationele privacy – van betrokkenen.

2 Beleid van het nieuwe kabinet

In 2003 introduceerde de commissie 'Veilig Samenleven' onder leiding van prof. Fijnaut het concept van het Veiligheidshuis. In de praktijk bleek dat meerdere organisaties (zoals het Openbaar Ministerie, de politie, Bureau Jeugdzorg, Raad voor de Kinderbescherming, verslavingszorg en het Leger des Heils) met eenzelfde persoon of gezin te maken hebben zonder dit van elkaar te weten. Het Veiligheidshuis beoogt hier een oplossing voor te bieden. In een Veiligheidshuis kunnen de betrokken organisaties samenkomen voor overleg, teneinde de betrokkene bijvoorbeeld de juiste zorg te verlenen of op een effectieve manier op strafbare feiten te reageren. Het inmiddels demissionaire kabinet nam het advies van Fijnaut en anderen ter harte en binnen een paar jaar tijd is een landelijk dekkend netwerk van Veiligheidshuizen ontstaan.

Het kabinet-Rutte/Verhagen ziet voor Veiligheidshuizen een 'belangrijke rol' weggelegd bij het terugdringen van overlast, huiselijk geweld en criminaliteit. De Veiligheidshuizen zullen onder hun bewind voortgezet en verder ontwikkeld worden. Daarnaast moet volgens het kabinet de informatieveiligheid en bescherming van persoonsgegevens worden verbeterd. Wat ons betreft moeten deze twee beleidsdoelstellingen worden gecombineerd: bij het overheidsbeleid ten aanzien van de uitwisseling van persoonsgegevens in een Veiligheidshuis moet voldoende rekening gehouden worden met privacy.

3 'Als er een convenant is, zit het wel goed met de privacy'

In de afgelopen jaren is binnen, maar ook buiten Veiligheidshuizen, een wildgroei aan casusoverleg ontstaan. Het is niet altijd duidelijk wat voor overleg, met welke partijen en voor welk doel deze precies plaatsvinden. De overheid lijkt hier geen richting aan te geven en zij vertrouwt voor de naleving van de privacyregelgeving op de professionals uit het werkveld. Het is de vraag of dat verstandig is. Uit het onderzoek 'Wat niet weet, wat niet deert' (2009) blijkt dat het hoge abstractieniveau van de Wet bescherming persoonsgegevens (Wbp), in combinatie met de vele wetten die van toepassing zijn naast de Wbp,

* Mariëlle Bruning is hoogleraar jeugdrecht Universiteit Leiden, Jan-Jaap Oerlemans is promovendus bij eLaw@Leiden, centrum voor recht in de informatiemaatschappij van de Universiteit Leiden.

een in de praktijk ondoorgrondelijk regelstelsel vormt. Hoe meer men van de relevante regelgeving af weet, hoe meer vragen er bij de respondenten opkomen. Verder blijkt uit dit onderzoek dat 'in de casusoverleggen privacybescherming geen onderwerp van gesprek is. De deelnemers aan de casusoverleggen geven aan dat het uitwisselen van gegevens noodzakelijk is om een bepaald maatschappelijk doel te bereiken. Op basis van professionaliteit wordt beslist of gegevens moeten worden uitgewisseld om het uiteindelijke doel te bereiken.' (p. 131). De professionals zullen hun eigen (sectorale) privacywet- en regelgeving echter zorgvuldig moeten blijven naleven bij het uitwisselen van gegevens met ketenpartners. Telkens zal daarbij opnieuw moeten worden gewogen of er een noodzaak bestaat voor het uitwisselen van specifieke gegevens. Dit vraagt om professionals die goed op de hoogte zijn van de privacyregels en de naleving daarvan. Gezien het hierboven aangehaalde onderzoek is het nog maar zeer de vraag of hierop vertrouwd kan worden.

Sommige professionals lijken te denken dat indien er een convenant wordt opgesteld 'het wel goed zit met de privacy' en verdere privacyafwegingen niet meer nodig zijn. Convenanten zijn echter slechts een weergave van de gemaakte afspraken tussen partijen. Zij bieden de burger een zekere transparantie, maar nemen de eigen verantwoordelijkheid van deelnemers aan casusoverleg niet weg. Daarnaast baart de kwaliteit van sommige reeds bestaande convenanten ons zorgen. Te vaak worden er te brede gronden voor de uitwisseling van persoonsgegevens in convenanten bepaald en worden verschillende convenanten nogal eens 'gemixt' teneinde de gewenste partijen bij elkaar te krijgen om gegevens uit te wisselen. Een vluchtige blik op privacyconvenanten die via internet beschikbaar worden gesteld, bevestigt dit beeld. Op de website <www.nogveiligghuis.nl> is bijvoorbeeld een wel heel algemeen, uitgebreide samenwerkingsovereenkomst te vinden, waar in een bijlage het 'privacyreglement' is opgenomen. Dit algemene reglement wordt gebruikt als basis voor verschillende typen casusoverleg, zoals Huiselijk Geweld of Veelplegers; 'waar dat nodig is' mogen instanties zoals gemeenten, politie, Bureau Jeugdzorg, maar ook verslavingsorganisaties en de GGZ aan een overleg deelnemen. Persoonsgegevens uit een ander casusoverleg kunnen verstrekt worden als dit bijvoorbeeld 'noodzakelijk is voor de uitvoering van de integrale persoonsgerichte aanpak'. Dergelijke formuleringen zijn te begrijpen vanuit het oogpunt van het stimuleren van gegevensuitwisseling, maar het is nog maar zeer de vraag of dit de toets van de huidige privacywet- en regelgeving kan doorstaan.

4 Privacy vooralsnog onvoldoende gewaarborgd: werk aan de winkel!

Het bovenstaande heeft uiteraard consequenties voor de informationele privacy van de betrokkene in een casusoverleg. Het kan echter ook ongewenste consequenties hebben voor de betrokken instanties. Onrechtmatig

verkregen gegevens die leiden tot identificatie van verdachten moeten bijvoorbeeld in principe worden uitgesloten van bewijs en dat kan vrijspraak tot gevolg hebben. Betrokken professionals of de overkoepelende organisaties kunnen bovendien door de betrokkene civielrechtelijk worden aangesproken.

Wij zijn van mening dat de privacywaarborgen in de dagelijkse praktijk van de Veiligheidshuizen door het Ministerie van Veiligheid en Justitie moeten worden gecontroleerd, gestimuleerd en ondersteund. Casusoverleg biedt veel voordelen, maar hierbij moet wel op een verantwoorde manier worden omgegaan met persoonsgegevens. De Minister van Veiligheid en Justitie zou als eindverantwoordelijke moeten worden aangemerkt, omdat Veiligheidshuizen grotendeels op initiatief van het Openbaar Ministerie zijn opgezet en het OM onder de verantwoordelijkheid van de Minister van Veiligheid en Justitie valt.

Op landelijk niveau – bij het Ministerie van Veiligheid en Justitie – zou volgens ons met betrekking tot Veiligheidshuizen gecontroleerd moeten worden welk casusoverleg op welke plek plaatsvindt. Dit zou vervolgens openbaar moeten worden gemaakt, zodat er voldoende duidelijkheid is voor de burger en de betrokkene weet welke organisatie kan worden aangesproken ter uitoefening van zijn of haar rechten. Bij twijfel zouden medewerkers van de betrokken organisaties hun eigen privacyjuristen moeten raadplegen over de vraag of een concrete gegevensuitwisseling door de beugel kan. De Helpdesk Privacy van het Ministerie van Veiligheid en Justitie zou voor vragen of overleg geraadpleegd moeten kunnen worden.

Kortom, de Minister van Veiligheid en Justitie zou zijn verantwoordelijkheid moeten nemen en bij het creëren van een landelijk netwerk van Veiligheidshuizen duidelijker beleid moeten scheppen met betrekking tot privacyaspecten. Ons inziens is het wenselijk dat de teugels worden aangetrokken en de privacy van de betrokkenen beter wordt gewaarborgd dan nu het geval is. Daarbij moet voor de langere termijn ook worden nagedacht over een wettelijke basis voor de Veiligheidshuizen.