SAMENVATTING .

HOOFDSTUK 1 INLEIDING

1.1 Aanleiding

1.2 Probleemstelling

1.3 Definities van Veiligheid en Persoonlijke Levenssfeer

1.4 Invulling van de opdracht

HOOFDSTUK 2 MAATSCHAPPELIJKE ONTWIKKELINGEN

2.1. De risicoloze samenleving – een utopie

2.2. Beleidstrends in het sociaal-veiligheidsbeleid

(A) Naast repressie veel meer aandacht voor preventie

(B) Preventie noopt tot nieuwe samenwerkingsverbanden

(C) In Samenwerkingsverbanden selecteren van risico's

2.3 Centraal – decentraal

2.4 Technologische ontwikkelingen

2.4.1 Typeren van personen

2.4.2 "Immutable me"

2.4.3 Identiteitsfraude

2.4.4 Slimme omgevingen

2.5 Overheid en bedrijfsleven

2.6 De private sector

2.7. Internationale ontwikkelingen

2.8 Waarheen, waarvoor

HOOFDSTUK 3 NAAR EEN RICHTINGGEVEND KADER

Richtinggevend kader voor informatieverwerking en veiligheid

3.1 Inleiding

3.2 Wettelijke kaders

3.2.1 Bestaand wettelijk kader veiligheid

3.2.2 Bestaand wettelijk kader omgang met persoonsgegevens

3.2.3. Kanttekeningen bij de wettelijke kaders

3.3 Wat komt er in de praktijk van de wetgeving terecht?

3.4 Diagnose

3.4.1 Niet in het werk ingebakken

3.4.2 Juridische dominantie

3.5 Veiligheid en persoonlijke levenssfeer als normaal beleidsterrein: richtinggevend kader

3.5.1 Inleiding: functies van het richtinggevende kader

3.5.2 Geadresseerden van het kader

3.5.3 Richtinggevend kader: grondslagen en handreikingen; kader en model

3.6 Handreikingen voor gegevensverwerking

3.6.1 Grondslagen voor de gegevensverwerking

3.6.2 Grondslagen voor de organisatie

3.7 Robuust extern toezicht en handhaving

3.8 Uitleiding

HOOFDSTUK 4 TOEPASSING VAN KADER OP ACTUELE CASES

4 Het richtinggevende kader in de praktijk

4.1 Kentekenherkenning met camera's

4.2 Registratie van etniciteit

4.3 Registeren van levensovertuiging

BIJLAGE 1: INSTELLINGSBESLUIT

BIJLAGE 2: DE AUTEURS VAN HET RAPPORT

BIJLAGE: 3: DE GESPREKSPARTNERS VAN DE COMMISSIE

BIJLAGE 4: SUMMARY

BIJLAGE 5: AFKORTINGENLIJST

BIJLAGE 6: AANBEVELINGEN

GEWOON DOEN, beschermen van veiligheid en persoonlijke levenssfeer

PROLOOG

Dit advies gaat over veiligheid en persoonlijke levenssfeer. Veiligheid en persoonlijke levenssfeer – de termen *'persoonlijke levenssfeer'*, *'privacy'* en *'privé-leven'* worden als synoniemen gebruikt – grijpen steeds vaker op elkaar in en zijn in diverse situaties elkaars voorwaarde.

Soms staan ze op gespannen voet met elkaar. Dit advies heeft als centrale boodschap dat de uitdaging van het zoeken naar de balans tussen veiligheid en de bescherming van de persoonlijke levenssfeer gewoon ter hand genomen moet worden. Dat we vooral niet weg moet lopen voor deze uitdaging. En, dat we daarbij gewoon, dat wil zeggen: niet krampachtig moeten doen om beide belangen zoveel als in een concrete situatie mogelijk is, recht te doen. Het advies presenteert daartoe een richtinggevend kader.

IN DE SCHIJNWERPERS

Een normaal beleidsterrein

Een van de centrale conclusies van dit advies is dat het juridische systeem voor de zorgvuldige omgang met persoonsgegevens ten behoeve van veiligheid vrijwel geen vertaling heeft gekregen naar de werkvloer. De organisaties waar 'professionals' werken aan de veiligheid van personen hebben hun 'professionals' vaak onvoldoende toegerust om handen en voeten te kunnen geven aan het juridische systeem van de omgang met persoonsgegevens. Met 'professionals' bedoelt de Commissie alle mensen die werkzaamheden verrichten ten behoeve van veiligheid. Sommigen bijna voortdurend, zoals politiemedewerkers, sommigen alleen incidenteel, zoals medewerkers van de GGZ of van scholen die soms veiligheidsdreigingen constateren. Zorgvuldige omgang met privacyregels is niet 'ingebakken' in het dagelijkse werk van de organisaties van deze 'professionals'. De discussie over zorgvuldig omgaan met persoonsgegevens blijkt sterk gedomineerd door een bijna exclusief juridische invalshoek. Vanuit deze diagnose adviseert de Commissie om het terrein waar veiligheid en de bescherming van de persoonlijke levenssfeer elkaar raken als een normaal beleidsterrein op te vatten. Dat wil zeggen, een beleidsterrein waarop afwegingen vanuit verschillende invalshoeken betekenis hebben en waarop voldoende aandacht is voor professionele, technologische en economische overwegingen. De centrale vragen zijn dan:

- Hoe in de dagelijkse praktijk de zorgvuldigheid te waarborgen bij het omgaan met persoonsgegevens door ‘professionals’ die werken op terreinen waar eisen worden gesteld in het belang van veiligheid?
- Met welke faciliteiten kunnen organisaties hun ‘professionals’ voldoende rugdekking geven?
- Met welke mechanismen kunnen we realiseren dat alle betrokkenen – ‘professionals’, leidinggevenden, bestuurders en politiek – hun verantwoordelijkheid nemen in het zoeken en realiseren van de balans tussen privacy en veiligheid?
- Hoe kunnen we de privacyregels zo goed en zo vroeg mogelijk inbouwen in technische systemen (*privacy by design*) en hoe kunnen we dit ‘inbouwen’ stimuleren?
- Wat kunnen we doen om de naleving te stimuleren?

De betrokken organisaties kunnen direct aan de slag met het faciliteren van hun ‘professionals’.

Ten behoeve van deze transformatie naar een normaal beleidsterrein ontwikkelt de Commissie een richtinggevend kader. Dit kader beoogt bij te dragen aan rationaliteit en consistentie bij beslissingen waar er spanning kan ontstaan tussen veiligheid en persoonlijke levenssfeer (‘evaluatie vooraf’). Ook kan het richtinggevende kader dienen als inspiratiebron om op een praktische manier de ‘professionals’ te faciliteren die dagelijks aan veiligheid en privacy werken. Het kader is ook een instrument om uitvoerders bij de implementatie van beslissingen over omgaan met persoonsgegevens tot alertheid op kwetsbaarheden te prikkelen. Tenslotte kan het richtinggevende kader dienen als toetsingsinstrument bij beleid en wetgeving dat privacy en veiligheid raakt.

Grondslagen voor een zorgvuldige omgang met persoonsgegevens

Een centraal uitgangspunt bij het richtinggevende kader is: “houd het eenvoudig, faciliteer en zorg dat veiligheid en persoonlijke levenssfeer elkaar zo veel mogelijk versterken.”
Het richtinggevende kader bestaat uit zes grondslagen met bijbehorende handreikingen:

1. ‘Transparantie, tenzij’;
2. ‘Selecteer voor je verzamelt’ en houd het sober (‘*select before you collect*’);
3. ´Indien noodzakelijk voor de veiligheid, moet je delen´;
4. Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers;
5. Zorg voor voorlichting en facilitering;

6. Zorg voor naleving en intern toezicht.

Met de voorgestelde grondslagen en handreikingen adviseert de Commissie niet meer en niet minder dan dat te doen wat al gedaan had moeten zijn: op een eenvoudige manier de ‘professionals’ helpen de benodigde zorgvuldigheid met het omgaan met persoonsgegevens in hun dagelijkse werk te verankeren en de passende prikkels in het leven roepen om dat te waarborgen.

Robuust extern toezicht en handhaving

Om de grondslagen en handreikingen kracht bij te zetten is het nodig dat er een onafhankelijke externe toezichthouder actief is. De toezichthouder moet zijn handen vrij hebben en geen bemoeienis hebben met advisering, facilitering of voorlichting. Op basis van de grootste nalevingsrisico’s en in samenhang met de ontwikkeling van zelfregulering stelt de toezichthouder cyclisch een programma op voor zijn werk. Wanneer nodig treedt de toezichthouder handhavend op met instrumenten als dwangsommen, bestuursdwang, *‘naming en shaming’* en bestuurlijke boetes.

Robuust toezicht betekent: op basis van een scherpe prioritering de feitelijke omgang met persoonsgegevens op de werkvloer aan toezicht onderwerpen. Kijken hoe het verzamelen en delen van persoonsgegevens in de praktijk feitelijk verloopt en of dat volgens de regels gaat. Dat wil zeggen: niet volstaan met beoordelen of de papieren werkelijkheid van codes en reglementen strookt met de wettelijke verplichtingen. Dat brengt ook mee: niet alléén op basis van signalen reageren, maar ook op basis van eigen prioritering pro-actief de praktijk induiken om bij te dragen aan de wisselwerking tussen praktijk, regels en de belangen en waarden die in de regels zijn vervat.

In de huidige situatie verricht het College bescherming persoonsgegeven zijn toezichtstaak naast andere taken zoals advisering over wetgeving, toetsing van gedragscodes en reglementen, voorlichting, bemiddeling, klachtbehandeling en internationale taken. Deze situatie is niet gewenst. De slagvaardigheid en geloofwaardigheid van extern toezicht is er bij gebaat dat de toezichthouder zijn handen vrij heeft en geen taken vervult als advisering, voorlichting of facilitering.

HET DECOR

Centraal in dit advies staan de maatschappelijke ontwikkelingen en de praktijk waarbinnen rechtshandhavers en hulpverleners afwegingen moeten maken ten behoeve van veiligheid en persoonlijke levenssfeer. Deze afwegingen zijn complexer geworden. Dat komt door de roep om een risicoloze samenleving, door nieuwe technologische mogelijkheden, door de vervlechting van private en publieke doelen en middelen, alsmede door internationale druk in verband met bestrijding van terrorisme en georganiseerde misdaad. Het wordt voor burgers steeds lastiger om te overzien wat er met persoonsgegevens gebeurt. Als er de afgelopen tien jaar op het gebied van informatie in het veiligheidsdomein iets fundamenteel is veranderd, is het wel de groei van het aantal databases, het aantal gegevens dat daarin is opgeslagen en de mogelijkheden om die databestanden te bevragen en te delen met andere instanties. Nu het kabinetsbeleid zwaarder inzet op voorzorg en preventie ontstaan nieuwe samenwerkingsverbanden tussen gemeente, politie en justitie met partijen die voorheen weinig met veiligheidsbeleid van doen hadden (netwerksamenleving).
Afgezien van het advies over het toezicht en over een enkele precisering komt de Commissie niet tot het advies de wetgeving op de schop te nemen. Prioritair is een hechtere verankering in het dagelijkse werk van kernbegrippen voor omgaan met persoonsgegevens bij het werken aan of ten behoeve van veiligheid, zoals ‘doelbinding’, ‘transparantie en voorzienbaarheid’ en ‘subsidiariteit en proportionaliteit’. Daarom is het nodig het maken van afwegingen in concrete gevallen te faciliteren op een manier die past bij de belangen die er spelen en die aansluit bij verantwoordelijkheden en het werk van de ‘professionals’ die de afwegingen maken. Daarom ook is het zaak meer werk te maken van verantwoordelijkheid voor en naleving van zorgvuldigheid in de omgang met persoonsgegevens bij het werken aan veiligheid. Het kan om allerlei situaties gaan. Om de docent die bij een van zijn leerlingen wel erg vaak blauwe plekken constateert. Om een luchtvaartmaatschappij die haar klanten een halalmaaltijd wil kunnen voorschotelen zonder dat deze bang hoeven te zijn als potentiële terroristen te worden aangemerkt. Om een burgemeester die burgers wel of niet informeert over het adres van een veroordeelde pedofiel. Over al dan niet een kentekenregistratiesysteem bijhouden. Of over de wenselijkheid om een landelijk elektronisch patiëntendossier in te voeren.

DE VOORSTELLING

Het richtinggevende kader bestaat uit 6 grondslagen die hieronder worden toegelicht.

1. ***'Transparantie, tenzij'***

   Daar waar de omgang met persoonsgegevens complexer wordt en burgers steeds afhankelijker worden van het gebruik van hun gegevens, is transparantie cruciaal. De grondslag *'transparantie, tenzij'* houdt in dat burgers in beginsel moeten weten wie wat met zijn persoonsgegevens doet. Ook wanneer het om gebruik van gegevens binnen ketens van organisaties gaat. Zo versterkt deze grondslag het streven naar een 'samenleving van vertrouwen'. Actief informeren over recht op inzage, correctie van gegevens en zonodig verweer draagt bovendien bij aan de juistheid van de gegevens. De Commissie acht het van groot belang dat (samenwerkende) organisaties het belang van transparantie serieus nemen en stevig werk maken van instrumenten die transparantie realiseren. Zo dienen ze onder meer direct te gaan werken aan het wegnemen van onnodige drempels voor burgers voor hun recht op inzage en correctie van hun gegevens. Zowel degene die besluit persoonsgegevens te doen verwerken als degene die dat feitelijk doet zijn verantwoordelijk voor het bewerkstelligen van 'transparantie'. De Commissie geeft organisaties in overweging een functionaris met het implementeren van deze grondslag te belasten.

2. ***'Selecteer voor je verzamelt' en houd het sober ('select before you collect')***

   Met de grondslag *'selecteer voor je verzamelt en houdt het sober'* beoogt de Commissie het werken met persoonsgegevens tot het noodzakelijke minimum te beperken en zo invulling te geven aan de open formulering van artikel 8, onderdelen e. en f. van de Wet bescherming persoonsgegevens. Bovendien adviseert de Commissie het kabinet in het licht van deze grondslag om bij wettelijke regelingen op het terrein van veiligheid en privacy steeds serieus te overwegen of een horizonbepaling tot de mogelijkheden behoort en gewenst is.

3. ***'Indien noodzakelijk voor de veiligheid, moet je delen´,***

   De Commissie wil de praktijk een nadrukkelijk signaal geven: wanneer risicobeoordeling uitwijst dat de veiligheid van individuen concreet wordt bedreigd en het delen van persoonsgegevens dat risico kan wegnemen móeten persoonsgegevens gedeeld worden. De Commissie adviseert het kabinet te bevorderen dat de 'professionals' die aan veiligheid werken zich kunnen wenden tot een externe vertrouwenspersoon voor hun beroepsgroep: een gezaghebbende persoon die fungeert als vraagbaak en klankbord met wie zij twijfels kunnen bespreken over hun risicobeoordeling of over de noodzaak persoonsgegevens te

delen. Zoals de Deken van de Orde van Advocaten deze functie voor advocaten vervult. Dat verwerking van persoonsgegevens achterwege moet blijven voor zover een geheimhoudingsplicht uit hoofde van beroep of wettelijk voorschrift aan delen van gegevens in de weg zou staan kan niet betekenen dat in een concrete situatie – bijvoorbeeld – een psychiater, die kennis neemt van levensbedreigende omstandigheden van of in de kring rond zijn cliënt, deze kennis onder zich houdt. De Commissie geeft in overweging deze grondslag in artikel 9 van de Wet bescherming persoonsgegevens te expliciteren.

4. ***Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers***

   Bij deze grondslag is het onder meer essentieel al bij het formuleren van de opdracht ontwikkeling van systemen privacyrisico's te ondervangen. De architectuur van de techniek bepaalt wat het systeem nu kan, maar ook wat de toekomstige mogelijkheden zullen zijn. Regie daarover is daarom noodzakelijk. Privacyoverwegingen kunnen zonder probleem een plaats krijgen in de ontwikkeling van technologie. Slimmere omgevingen stellen steeds hogere eisen aan het realiseren van de noodzakelijke privacywaarborgen. Passende deskundigheid zal bij (uitbesteding van) ontwikkeling van ICT-diensten binnen organisaties, waarbij de Commissie nadrukkelijk de overheid noemt, beschikbaar moeten zijn.

5. ***Zorg voor voorlichting en facilitering***

   Bij deze grondslag zijn modelcodes en protocollen voor de werkvloer onmisbaar. Ontwikkeling van *'good and best practices'* en simulaties kunnen bijdragen aan verankering van het privacybelang in het dagelijkse werk van 'professionals' die vanuit of met het oog op veiligheidsbelangen werken. De verantwoordelijkheid voor het ontwikkelen van codes en *'good and best practices'* ligt bij de instanties die met persoonsgegevens omgaan. De overheid speelt hierbij een faciliterende rol.

6. ***Zorg voor naleving en intern toezicht***

   Deze grondslag zorgt voor een permanente prikkel in de organisatie om de afwegingen binnen privacy en veiligheid, waaronder risicoanalyses en risicobeoordelingen op adequaat niveau te brengen en te houden. Het is in de visie van de Commissie noodzakelijk in iedere instelling of binnen ieder bedrijf een functionaris aan te wijzen die met voldoende gezag tot naleving kan aanzetten. Afhankelijk van onder meer de omvang van de organisatie zal dat soms wel, maar vaak ook niet een speciale functionaris zijn. De Commissie acht het in grotere organisaties zeer de moeite waard een gezaghebbende *'Functionaris voor de gegevensbescherming'* als bedoeld in de

Wet bescherming persoonsgegevens aan te stellen om concreet handen en voeten te geven aan de afwegingen en risicoanalyses die gemaakt moeten worden wanneer veiligheid en privacy elkaar raken. Deze functionaris kan tevens de zorg voor naleving van het binnen de organisatie afgesproken beleid kracht bijzetten.

DE EPILOOG

Op verzoek van de opdrachtgevers bespreekt het advies twee actuele dossiers. Het advies maakt aan de hand van het richtinggevende kader kanttekeningen bij:

- Kentekenherkenning met camera's;
- Registratie van etniciteit/levensovertuiging bij criminaliteitsbestrijding en de-radicaliseringsbeleid.

DE VESTIAIRE

Het advies herbergt verder verspreid in de tekst nog een aantal aanbevelingen. Bijlage 6 bij dit advies vermeldt alle aanbevelingen. Aanvullend op het bovenstaaande noemen we in deze samenvatting nog de volgende:

- Onderzoek hoe ontwikkeling en inrichting van privacyzorgsystemen en normalisatie en certificering kunnen bijdragen aan het slaan van een brug tussen praktijk en regelgeving op het gebied van veiligheid en persoonlijke levenssfeer;
- Zorg binnen de overheid voor voldoende deskundigheid om bij (uitbesteding van de) ontwikkeling van systemen ook het privacybelang een goede plaats te geven;
- Zorg in het geval dat de overheid gegevens van burgers vraagt deze burgers weten dat het de overheid is die om deze gegevens vraagt, ook wanneer de gegevens door tussenkomst van private partijen bij de overheid komen; dit speelt bijvoorbeeld bij verkeersgegevens in de luchtvaart: luchtvaartmaatschappijen verzamelen passagiersgegevens ter uitvoering van verplichtingen die hen door de overheid zijn opgelegd. Het moet burgers duidelijk zijn of een verplichting van de overheid afkomstig is en het is de taak van de overheid daar voor te zorgen;
- De Commissie adviseert het er toe te leiden dat met recht overheidscampagnes zoals '*Wij werken aan uw veiligheid'* aangevuld kunnen worden met de toevoeging *'en aan uw privacy'* .

HOOFDSTUK 1 INLEIDING

1.1. Aanleiding

Het afgelopen decennium is het aantal wetten en beleidsvoorstellen ter bevordering van de veiligheid van personen aanzienlijk toegenomen. De overheid heeft de strijd tegen kleine en grote criminaliteit geïntensiveerd. De wereldwijde strijd tegen terrorisme fungeert als aanjager voor wetten waarin het belang van een veilige samenleving voorop staat. Verder vragen ook burgers en bedrijven steeds sneller en vaker aandacht voor potentieel onveilige situaties. Zij dringen aan op daadkrachtig handelen door de overheid. Daarnaast hebben de toenemende complexiteit van informatiestromen en de sociale-netwerksamenleving alsook de snel groeiende ontwikkeling van nieuwe technologieën een belangrijke invloed op de persoonlijke levenssfeer. Als er de afgelopen tien jaar op het gebied van informatie in het veiligheidsdomein iets fundamenteel is veranderd, is het wel de groei van het aantal databases, het aantal gegevens dat daarin is opgeslagen en de mogelijkheden om die databestanden te bevragen en te delen met andere instanties.

De bescherming van de persoonlijke levenssfeer is bij deze ontwikkelingen niet altijd van begin af aan gelijkwaardig meegewogen. Wanneer discussie plaatsvindt worden privacy en veiligheid in het concrete geval dikwijls lijnrecht tegenover elkaar gezet. Een publieke discussie over een eigentijdse visie op 'de balans tussen veiligheid en de persoonlijke levenssfeer' is geboden, zo stelt het kabinet in reactie op het advies '*Data voor Daadkracht*'[1] Alle reden voor een nadere beschouwing.

In het politieke en publieke debat over veiligheid en persoonlijke levenssfeer verschuilt men zich veelal achter onheldere begrippen en daarachter liggende onnauwkeurige concepten. Veiligheid en persoonlijke levenssfeer worden vaak als containerbegrippen gebruikt en vanuit een open formulering zonder nadere inkleuring in het debat ingezet. Het belang van veiligheid lijkt te worden opgeëist door diegenen die de samenleving en het publieke domein willen beschermen tegen alle soorten inbreuken zoals terrorisme, criminaliteit, risicogedrag en misbruik van gegevens. Het belang van de persoonlijke levenssfeer lijkt te worden voorbehouden aan degenen die zich opwerpen als verdedigers van de waarden van de rechtsstaat (en zijn afzonderlijke burgers) en de daarbij behorende ruimte voor het individu,

[1] TK 2006-2007, 30 800, VI en VII, nr. 65, brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties mede namens de ministers van Justitie en Defensie over het rapport *'Data voor daadkracht'*, 30 augustus 2007.

de privacy en de rechtsbescherming. Deze stand van zaken lijkt mede debet aan de verstarring van de posities in het debat over een waaier aan concrete maatschappelijke vraagstukken, zoals de bestrijding van terrorisme en criminaliteit, maar ook de werkwijze in de jeugdzorg, de zorg om sociale veiligheid, de waarborgen rondom nieuwe technologieën, het gebruik van gegevens die in het veiligheidsbelang zijn verzameld in de private sector (zoals door banken en internet-providers) en de maatregelen ter bevordering van integriteit. Bescherming van de persoonlijke levenssfeer wordt vaak beschouwd als eenzijdig gericht op de bescherming van het individu en diens rechten, met veronachtzaming van belangen van de samenleving. Maatregelen tot bevordering van veiligheid worden omgekeerd vaak beschouwd als angstmaatregelen tot stand gekomen onder oneigenlijke maatschappelijke druk, invloed van de media en de roep van politici en bestuur om steeds maar meer bevoegdheden. Gevolg van de eenzijdige benadering van belangen is dat 'veiligheid' en 'persoonlijke levenssfeer' ogenschijnlijk tegenover elkaar zijn komen te staan.[2] Discussies gaan over afzonderlijke maatregelen en te weinig over zowel het grotere geheel als de zoektocht naar de balans tussen veiligheid en de bescherming van de persoonlijke levenssfeer.

Pas recent is het maatschappelijke debat over een eigentijdse visie op de persoonlijke levenssfeer geactiveerd, onder meer door wetenschappers en maatschappelijke organisaties.[3] Begrijpelijk, nu de persoonlijke levenssfeer niet alleen bij de bestrijding van terroristische activiteiten, maar ook bij de aanpak van sociale onveiligheid in wijken en buurten onder druk staat. Ook in het politieke discours namen fracties in zowel de Tweede als de Eerste Kamer het afgelopen jaar een kritischere houding aan tegen kabinetsvoorstellen op dit terrein. In die zin is, althans in het debat, sprake van een pendulebeweging. Veiligheid is topprioriteit van beleid. En wanneer dan de overheid meer veiligheidsmaatregelen neemt en de gevolgen daarvan in de samenleving meer bekend en merkbaar worden, dan blijkt dat burgers naast hun veiligheid ook prijs stellen op hun persoonlijke levenssfeer. Naar de indruk van de Commissie beweegt de pendule zich nu weer in de richting van meer aandacht voor de bescherming van de persoonlijke levenssfeer.

1.2. Probleemstelling

[2] Zie ook *E.R. Muller, H.R.B.M. Kummeling en R.P. Bron, Veiligheid en privacy: Een zoektocht naar een nieuwe balans, Den Haag 2007.*

[3] Onder meer *E.R. Muller, H.R.B.M. Kummeling en R.P. Bron, Veiligheid en privacy: Een zoektocht naar een nieuwe balans, Den Haag 2007;* Vedder, Van der Wees, Koops, De Hert, *Van privacyparadijs tot controlestaat,* Rathenau-instituut 2007.

Een samenleving kan alleen functioneren wanneer de veiligheid van burgers in voldoende mate is gewaarborgd. Burgers, bedrijven, maatschappelijke instellingen en overheid hebben een verantwoordelijkheid bij het streven naar een veilige samenleving. Daarnaast is het voor het functioneren van een samenleving essentieel dat er vertrouwen is. Vertrouwen tussen mensen, vertrouwen in instanties en vertrouwen als basis voor het handelen in ons maatschappelijk verkeer. In beginsel heeft iedereen het recht met rust te worden gelaten en zich onbespied te weten. Dat recht op de bescherming van de persoonlijke levenssfeer kent verschillend aspecten, zoals de bescherming van persoonsgegevens, en ook de onaantastbaarheid van het lichaam, het huisrecht en het briefgeheim. Dit recht is niet absoluut, inmenging in de persoonlijke levenssfeer kan zijn gerechtvaardigd. Evenzogoed als het nastreven van veiligheid is begrensd. Het gaat er om dat zowel bij het werken aan veiligheid als bij de bescherming van de persoonlijke levenssfeer waarborgen voor een vrije ruimte voor de burger worden geëerbiedigd. Zo geformuleerd dragen inspanningen voor veiligheid en de bescherming van de persoonlijke levenssfeer bij aan dezelfde doelstelling.[4]

Intussen ondervinden overheden, overheidsinstellingen en hun medewerkers die waken over onze veiligheid, spanning tussen veiligheid en persoonlijke levenssfeer. De Commissie richt zich in haar advies juist op het omgaan met deze spanning en zij beoogt handvatten te geven om hiermee om te gaan.
De burgers zullen in zijn relatie tot de overheid vooral een tegenstelling ervaren. Maatregelen ter bevordering van sociale cohesie, welbevinden en een veilige publieke en private ruimte en veel maatregelen op het gebied van veiligheid, zorg, welzijn ervaren zij voor zichzelf soms als knellend. Soms staan veiligheid en privacy gewoon tegenover elkaar. Dan vraagt het voorkomen van grof geweld, terreur of kindermishandeling inmenging in de persoonlijke levenssfeer van iedereen, van een bepaalde groep of van bepaalde personen.

De Commissie illustreert haar advies met concrete voorbeelden op terreinen[5] waar de spanning tussen het scheppen van een zo veilig mogelijke samenleving en het beschermen van de persoonlijke levenssfeer voor burgers, bedrijven en instellingen duidelijk zichtbaar zijn. Rechtshandhavers en hulpverleners worden het meest met die spanning geconfronteerd in het

[4] *E.R. Muller, H.R.B.M. Kummeling en R.P. Bron, Veiligheid en privacy: Een zoektocht naar een nieuwe balans, Den Haag 2007.*
[5] Met uitzondering van specifieke wet- en regelgeving gericht op de aanpak van terrorisme. De ministers van Justitie en Binnenlandse Zaken en Koninkrijksrelaties hebben 11 juli 2008 de commissie evaluatie antiterreurmaatregelen aangekondigd (TK 2007-2008, 29 754, 31200, VII, nr. 132).

sociale veiligheidsdomein waaronder het jeugdbeleid en bij de uitwisseling van gegevens tussen private en publieke partijen.

De Commissie beziet hoe doelstellingen met betrekking tot veiligheid alsook ter zake van de bescherming van de persoonlijke levenssfeer zo goed mogelijk in samenhang met elkaar gerealiseerd kunnen worden. Overeenkomstig het instellingsbesluit besteedt de Commissie daarbij aandacht aan wat er nodig is aan regulering van, voorlichting over, werkwijzen bij en indien nodig protocollisering en handhaving van de omgang met persoonsgegevens, met het oog op het belang van de veiligheid van personen en het maatschappelijke verkeer (het gaat immers toch ook om andere veiligheidsbelangen dan alleen de veiligheid van personen). Concreet besteedt de Commissie ook aandacht aan de belemmeringen die rechtshandhavers en hulpverleners ondervinden. Verder wordt ingegaan op de vraag hoe technologische ontwikkelingen benut kunnen worden op het gebied van de bescherming van persoonlijke levenssfeer en veiligheid en wordt kort stilgestaan bij deze begrippen in internationaalrechtelijke context.

Om de doelstellingen op het gebied van veiligheid alsook op het terrein van de bescherming van de persoonlijke levenssfeer zo goed mogelijk in samenhang met elkaar te realiseren, presenteert de Commissie in hoofdstuk 3 van dit rapport een praktisch richtinggevend kader voor een verantwoorde en in de dagelijkse praktijk in te bedden omgang met persoonsgegevens op het terrein van veiligheid. De uitwerking van dit richtinggevende kader wordt met voorbeelden geïllustreerd. Daarnaast geeft de Commissie in hoofdstuk 4 op verzoek van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie aandacht aan kentekenregistraties gekoppeld aan cameratoezicht en aan registratie van etniciteit en levensovertuiging.

1.3 Definities van Veiligheid en Persoonlijke Levenssfeer

Veiligheid en persoonlijke levenssfeer zijn veelomvattende begrippen. De Commissie ziet in dit rapport af van een nadere analyse van deze begrippen, maar hanteert in plaats daarvan algemene werkdefinities. De Commissie benadert veiligheid en persoonlijke levenssfeer daarbij als volgt:

Het bieden van veiligheid vormt in de rechtsstaat van oudsher een centrale taak van de overheid. Ook bedrijven, instellingen en niet in de laatste plaats de burger zelf hebben een

verantwoordelijkheid ten aanzien van hun eigen veiligheid. De bescherming die daarbinnen moet worden gerealiseerd door de overheid is altijd tweeledig: de bescherming tegen andere burgers en dreigingen van buitenaf maar ook bescherming tegen te grote macht van de staat zelf. Veiligheid ziet op de bescherming van de burger, diens leven maar ook eer, lijf en goederen. Recht op veiligheid is geen beginsel of een anderszins grondwettelijk of verdragsrechtelijk gewaarborgd recht maar ligt besloten in onder meer het recht op leven en het recht op ongestoord genot van eigendom die wel als zodanig zijn gewaarborgd. De Commissie vat het begrip veiligheid ruim op. Ook sociale veiligheid, het tegengaan van criminaliteit, overlast in de openbare ruimte en onveiligheidsbeleving, wordt hieronder begrepen.[6]

De persoonlijke levenssfeer omvat het recht om met rust te worden gelaten en het recht om zich te beschermen tegen handelingen of beslissingen die van invloed zijn op de levensomstandigheden en dus op de vrijheid van betrokkene.[7] De persoonlijke levenssfeer vindt bescherming in artikel 10 van de Grondwet. Ook wordt wel gesproken over privacy of privé-leven; deze termen worden vaak als synoniemen gebruikt. Specifieke aspecten ervan betreffen onder andere de onaantastbaarheid van het lichaam, het huisrecht en het briefgeheim, die alle onder een specifiek grondwettelijk beschermingsregiem vallen (respectievelijk de artikelen 11, 12 en 13 Grondwet).

De kern van het recht is de bescherming van persoonlijke vrijheid en individuele autonomie, zowel in relatie tot de overheid - in de afbakening van de privé-sfeer tot de publieke sfeer - als in relatie tot rechten en vrijheden van anderen. Het recht op privacy is een essentiële voorwaarde voor een menswaardig bestaan en een van de grondslagen van onze rechtsorde. Het gaat om ‘het recht zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf’ en ‘de reeks situaties waarin de mens onbevangen zich zelf wil zijn.’ Internationaal vindt het recht bescherming in onder andere de artikelen 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR).

[6] L. van Noije en K. Wittebrood, Sociale veiligheid ontsleuteld: Veronderstelde en werkelijke effecten van veiligheidsbeleid, Sociaal en Cultureel Planbureau, Den Haag: 2008.
[7] De Hert en Gutwirth 2004, p.588-589.

Ook persoonsgegevens maken deel uit van de persoonlijke levenssfeer. Volgens artikel 10, tweede lid, van de Grondwet, stelt de wet regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Volgens artikel 10, derde lid, van de Grondwet, stelt de wet ook regels met betrekking tot de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens. Mede ter uitvoering van deze opdracht van de Grondwet, alsook van diverse Europese regelingen (zie bijlage), zijn onder andere de Wet bescherming persoonsgegevens (Wbp), de Wet justitiële en strafvorderlijke gegevens en de Wet politiegegevens tot stand gebracht.

Bij zowel de bescherming van veiligheid als van de persoonlijke levenssfeer gaat het om concepten die bezien vanuit de overheid verplichtend zijn en, bezien vanuit de burger, aanspraak bieden op een recht. Met het oog daarop moet de overheid instrumenten en bevoegdheden creëren om een en ander daadwerkelijk te kunnen realiseren. Tegelijkertijd betekent dat, dat de overheid moet garanderen dat die aanspraken kunnen worden afgedwongen. Een democratische rechtsstaat blijft daarbij binnen de grenzen die hij en de internationale gemeenschap zichzelf hebben opgelegd. Het gaat meestal niet om de vraag óf de overheid moet optreden, maar om de vraag hoever hij daarbij mag gaan en welke instrumenten en bevoegdheden hij daarbij mag inzetten. De grondrechten van de burger spelen daarbij een fundamentele rol. Zij vormen de basis van de verhouding tussen overheid en burger en in toenemende mate ook voor de verhouding tussen burgers onderling. De burger verwacht van de overheid maatregelen ter bescherming van zijn veiligheid, maar diezelfde burger verwacht ook dat de overheid - en zijn medeburgers - zijn vrijheden eerbiedigt en hem met rust laat. Veiligheid nastreven zonder recht te doen aan de balans tussen collectieve veiligheid en individuele vrijheid, ondermijnt de essentie van elke open en pluriforme samenleving. Overheidscampagnes zoals *'Wij werken aan uw veiligheid'* zouden dan ook heel goed kunnen worden vergezeld van campagnes met de toevoeging *'en aan uw privacy'* Immers, het bevorderen van veiligheid en eerbiediging van de vrijheidsrechten zijn geen competitieve waarden, maar elkaars voorwaarde.[8]

1.4. Invulling van de opdracht

[8] Vedder e.a 2007, p. 62.

De Commissie is van mening dat de spanning tussen veiligheid en persoonlijke levenssfeer en de omgang met deze spanning het meest pregnant tot uitdrukking komt in de dagelijkse context waarin rechtshandhavers, hulpverleners, instellingen, bedrijven en andere betrokkenen afwegingen hebben te maken. Het is hier dat de noodzaak tot een richtinggevend kader zeer nadrukkelijk wordt gevoeld. De Commissie kiest er daarom voor om bij de invulling van haar opdracht de maatschappelijke ontwikkelingen en context waarbinnen rechtshandhavers en hulpverleners afwegingen moeten maken centraal te stellen. Dit vanuit de ambitie om vermeende en werkelijke belemmeringen die op de 'werkvloer' bestaan, te helpen wegnemen. In het rapport wordt dan ook veel nadruk gelegd op de maatschappelijke context en beoogt de Commissie een voor rechtshandhavers en hulpverleners toepasbaar kader te schetsen.
De Commissie heeft in het licht van deze ambitie gesproken met deskundigen op het terrein van de bescherming van persoonsgegevens en deskundigen op het terrein van de integrale veiligheid. Zij heeft expertsessies belegd over privacy en veiligheid in de sector welzijn en zorg, over de visie van het bedrijfsleven op veiligheid en persoonlijke levenssfeer, over nieuwe technologieën en over de wijze waarop jongeren met hun 'privacy' omgaan.[9]
De interviews en expertsessies hebben de Commissie gesterkt in haar opvatting dat er behoefte is aan een richtinggevend kader voor een verantwoorde omgang met persoonsgegevens. De Commissie heeft de expertsessies mede benut om de uitgangspunten van het hierna te presenteren richtinggevend kader zowel te inventariseren als te bediscussiëren.

.

[9] Zie bijlage 3: 'De gesprekspartners van de Commissie'.

HOOFDSTUK 2 MAATSCHAPPELIJKE ONTWIKKELINGEN

Inleiding

De vraagstukken waarin veiligheid en persoonlijke levenssfeer elkaar raken zijn, zo bleek al, niet slechts van deze tijd. Toch zijn er in onze samenleving ontwikkelingen waarin de spanning tussen beide waarden sterker dan voorheen tot vragen en discussie leidt. De belangrijkste ontwikkelingen worden hier kort besproken.

2.1. De risicoloze samenleving – een utopie

Het bevorderen van veiligheid is een kerntaak van de overheid. Rechtshandhavers en hulpverleners die proberen incidenten te voorkomen, kinderen en ouders op het juiste pad te houden of te brengen, overlast en verloedering te voorkomen, criminaliteit aan te pakken en iets willen doen met signalen van radicalisering, hebben in hun dagelijks werk niet alleen te maken met wetten en regels, maar ook met de maatschappelijke context waarbinnen zij hun werk moeten doen. Het is moeilijk ‘het goede’ te doen. De samenleving heeft heel wat wensen en verlangens. Daarvoor moeten soms gegevens juist wel en in andere gevallen juist niet uitgewisseld kunnen worden. Wij hoeven volgens de Wet eenmalige gegevensuitvraag maar één keer onze gegevens op te geven met betrekking tot werk en inkomen voor het digitale klantdossier voor het UWV en de gemeente. Wij willen dat de politie op basis van gegevens optreedt tegen groepjes jongeren die een buurt onveilig maken en daarbij openlijk overtredingen en misdrijven plegen. Wij willen dat tijdig wordt gesignaleerd dat kinderen in de knel komen en dat de betrokken hulpverleners daarbij goed kunnen samenwerken en dat ook doen. Van gegevensuitwisseling om potentiële drama’s en menselijk leed te voorkomen is iedereen voorstander. Tegelijkertijd willen we niet dat meer gegevens van ons worden gevraagd en uitgewisseld dan strikt noodzakelijk.

Op het brede terrein van ‘veiligheid’ en ‘persoonlijke levenssfeer’ zijn er veel actoren die - ieder voor zich gestuurd vanuit onderscheiden taken en met verschillende bevoegdheden - allemaal op deelterreinen hun wettelijke taak uitvoeren. Dat maakt het kader waarbinnen geopereerd moet worden onoverzichtelijk. Bovendien is de wereld waarop het beleid zich richt steeds complexer geworden. De gedachte dat de overheid zich kan opstellen als een alwetende regisseur die in detail kan voorschrijven welk gedrag vereist is, stuit daardoor in

de huidige sociale-netwerksamenleving met tal van samenwerkingsverbanden waarbij niemand de eindverantwoordelijkheid heeft, op grenzen.[10]

De samenleving wil enerzijds niet dat de overheid alles voorschrijft en preventief beïnvloedt, maar anderzijds wel dat zij (absolute) veiligheid realiseert. Hoewel er altijd een bepaalde mate van onveiligheid in een samenleving is, lijkt bij burgers het begrip daarvoor af te nemen.[11] Burgers, bedrijven en maatschappelijke instellingen nemen jegens de overheid een dubbele houding aan. Zij willen graag een grote keuzevrijheid en menen dat de overheid zich niet (teveel) met zijn of haar persoonlijk leven en met de onderneming of de organisatie heeft te bemoeien. Regels zijn er vooral voor de ander. Tegelijkertijd vragen burgers steeds sneller aandacht voor potentieel onveilige situaties en om daadkrachtig optreden van diezelfde overheid. Het verwachtingspatroon bij de burger uit zich meer en meer in een roep om een risicovrije samenleving. De media spelen daarin een grote rol. Zij zijn een belangrijke aanjager in het maatschappelijke en politieke discours over veiligheid. Bij elk incident, groot of klein, komt de vraag op welke rol de media hebben gespeeld in het positioneren van het incident als signaal van een mogelijk structureel verschijnsel. Niet zelden bepalen de media, gevoed door maatschappelijke groeperingen en actiegroepen, de politieke agenda. De dynamiek van publiciteit rond een incident leidt vaak tot het resultaat dat de overheid nieuwe maatregelen voorstelt om dergelijke incidenten voor de toekomst te voorkomen.

2.2. Beleidstrends in het sociaal-veiligheidsbeleid

Achtereenvolgende kabinetten hebben de nadruk gelegd op een evenwichtige verantwoordelijkheidsverdeling tussen overheid, burgers, bedrijfsleven en maatschappelijke instellingen. Momenteel is sprake van een overheid die verder dan voorheen, tot achter de voordeur, ingrijpt in het leven van burgers. Daarmee geeft de overheid - vaak onder politieke en maatschappelijke druk - zelf voeding aan de wens om en de mogelijkheid tot het realiseren van een vrijwel risicovrije samenleving. Maar een risicoloze samenleving is en blijft een utopie.

(A) Naast repressie veel meer aandacht voor preventie

De algemene staat van de leefomgeving en de aanpak van overlast en van verloedering in het publieke domein vormen sinds eind jaren negentig speerpunt van beleid. Er is een

[10] Wetenschappelijke Raad voor her Regeringsbeleid, *'Onzekere Veiligheid'*, 1 oktober 2008.
[11] H. Boutellier, *De Veiligheidsutopie*, Den Haag 2002.

verschuiving van delict naar risico en van repressie naar voorzorg en preventie. Beter gezegd, het beleid ten aanzien van voorzorg en preventie heeft lange tijd geen gelijke tred gehouden met het repressieve beleid en is daarom de afgelopen jaren geïntensiveerd. Ook van oudsher meer repressieve middelen, die vroeger als straf werden opgelegd na een overtreding of misdrijf, worden nu preventief gebruikt. Hierbij kan bijvoorbeeld worden gedacht aan de gebieds- of contactverboden. Er is fors geïnvesteerd in nieuw beleid, waarbij veel meer dan voorheen kan worden ingegrepen in de persoonlijke levenssfeer van burgers. Het gewicht is daarbij deels verschoven naar het lokale bestuur. De burgemeester heeft naast en in samenspraak met de officier van justitie de afgelopen jaren extra bevoegdheden gekregen, zoals preventief fouilleren, het opleggen van gebiedsverboden en samenscholingsverboden en het mogen ophouden van groepen personen die de openbare orde dreigen te verstoren (‘bestuurlijke ophouding’). Veel instrumenten worden ingezet jegens burgers die nog geen kwaad hebben verricht of overtredingen of misdrijven hebben begaan en dat – op een enkele uitzondering na – ook niet van plan zijn. Het leidende beginsel is nu: vroegtijdig signaleren en tijdig ingrijpen.

(B) Preventie noopt tot nieuwe samenwerkingsverbanden

De afgelopen jaren is een stelsel van samenwerkingsrelaties ontstaan tussen gemeentebestuur, politie, justitie, onderwijs, horeca, winkeliersverenigingen, woningbouwcorporaties, verslavingszorg, GGD’s, jeugdzorg en buurtwerkers. Op dit terrein van preventief veiligheidsbeleid wordt informatie niet altijd adequaat geselecteerd en indien noodzakelijk gedeeld met andere partijen. Een voorbeeld: burgemeesters krijgen van het Openbaar Ministerie niet alle informatie aangaande verlofbewegingen of vrijlatingen van ex-gedetineerden en TBS-ers. Dit terwijl gemeenten wel de wettelijke zorg hebben voor enerzijds het nazorgtraject; huisvesting, uitkering, begeleiding en anderzijds de zorg voor de openbare orde.

Om de samenwerking op lokaal niveau meer structuur te geven, worden in heel Nederland *Veiligheidshuizen* opgericht. Dit gebeurt meestal op instigatie van de gezagsdriehoek (burgemeester – officier van justitie – districtschef van politie). Het casusoverleg vormt de kern van het Veiligheidshuis. Meerdere partijen voeren op reguliere basis met elkaar overleg over een specifieke casus. Bijvoorbeeld het casusoverleg ‘huiselijk geweld’, het casusoverleg ‘jeugd’ of het casusoverleg ‘veelplegers’.Veelal wordt gewerkt met actuele en historische persoonsgegevens vanuit één of meer databases van het OM en de politie. Het persoonlijke dossier bevat informatie over onder meer het criminele verleden, verslavingsproblematiek,

schulden en schuldsanering, inkomens- en uitkeringssituatie, de gezins- en woonsituatie, scholing en het zorgverleden van de cliënt.

(C) In Samenwerkingsverbanden selecteren van risico's

In het rapport *'Politie in Ontwikkeling'* van de Raad van Hoofdcommissarissen wordt de opgave van de politie toegelicht om, als de verkeersagent op een kruispunt, tientallen informatiestromen te herkennen en te volgen. De politie staat daarbij vaak voor een dilemma. Enerzijds wordt zij gestimuleerd om innovaties toe te passen om niet achter de feiten aan te lopen. Anderzijds leidt het gebruik van innovatieve technieken in de perceptie van veel burgers soms tot een 'controle-politie'. Het gaat erom een doelgericht controlemechanisme te ontwikkelen waarmee in de massaliteit van (mensen)stromen een adequate selectie kan worden gemaakt van personen die een bedreiging voor de veiligheid kunnen vormen.[12] Die selectie leidt ertoe dat overheidshandelen in de lijn van vroegtijdig signaleren en tijdig ingrijpen voornamelijk is gericht op uitgaanscentra, openbaarvervoer-knooppunten zoals vliegvelden en grote stations en op achterstandswijken, waar kwetsbare groepen verblijven. Overlast, verloedering en kleine criminaliteit komen op die plekken het meeste voor. Veel wijken laten zich vanwege hun fragiele sociale structuren lastig door de 'overheid' en overheidsdienaren kennen. Om misstanden te bestrijden, zullen rechtshandhavers en hulpverleners zich meer in de persoonlijke levenssfeer van de burgers mengen. Als het gaat om bijvoorbeeld mógelijk huiselijk geweld of mógelijke zedendelicten, is het van belang dat relevante gegevens beschikbaar zijn en op tafel komen voordat zich ernstige drama's voordoen.

Samenvattend: nu zowel nationaal als lokaal sterk wordt ingezet op voorzorg en preventie, ontstaan nieuwe samenwerkingsverbanden tussen gemeente, politie en OM met partijen die voorheen weinig met veiligheidsbeleid van doen hadden. In die nieuwe samenwerkingsverbanden is het zaak om op basis van risico-analyses te komen tot een geselecteerde groep van personen of gebieden (zoals OV-knooppunten) die extra aandacht verdienen.

2.3. Centraal – decentraal

[12] TK 2005-2006, 29628, nr. 25, brief van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Justitie, 14 oktober 2005.

Het huidige kabinetsbeleid bevordert decentralisatie. Soms heeft dit als onbedoeld effect dat de verkokering in Den Haag zich verplaatst naar het decentrale niveau.[13] Bij digitalisering is dat niet anders. Gemeenten hebben in onze gedecentraliseerde eenheidsstaat een betrekkelijk autonome positie en kunnen vaak hun eigen plan trekken. Dit wordt nog versterkt doordat voornemens op rijks- en op lokaal niveau vaak sneuvelen door te grote ICT-ambities, rommelige aanbestedingen en een stapeling van wensen van maatschappelijke en politieke partijen. Zo is bij de coördinatie van de zorg om jongeren niet alleen een bonte schakering aan instanties tot stand gekomen, maar ook een kleurrijk digitaal landschap ontstaan.

Gemeenten, politieregio's en tal van samenwerkingsverbanden spelen zoals gezegd een grote rol in het domein van veiligheid en persoonlijke levenssfeer. Werken aan de oplossing van écht lastige problemen zal dikwijls plaatsvinden in samenwerkingsverbanden van publieke en private partijen. Daarbij zal regelmatig uitwisseling van persoonsgegevens plaatsvinden op basis van verschillende wettelijke regiems.

2.4. Technologische ontwikkelingen

Het doordenken van een nieuw richtinggevend kader is des te meer noodzakelijk nu in hoog tempo gebruik wordt gemaakt van nieuwe technologieën. Zij bieden kansen, maar ook bedreigingen. Nieuwe technologieën worden enerzijds ingezet om de persoonlijke levenssfeer en de veiligheid te realiseren en te waarborgen, anderzijds bieden zij ook instrumenten die de persoonlijke levenssfeer en de veiligheid bedreigen.

Technologieën die recentelijk in ontwikkeling zijn gekomen, zoals nanotechnologie of RFID-technologie (*radio frequency identification*), zullen in de zeer nabije toekomst op grote schaal worden gebruikt. Nieuwe technologieën zorgen voor nieuwe mogelijkheden enerzijds en een vergroting van de reikwijdte van bestaande mogelijkheden anderzijds. De agent die langs de snelweg staat te controleren wordt bijvoorbeeld vervangen door camera's en computerprogramma's die de kentekens van al het passerende verkeer registeren. In beide gevallen kan worden gesproken over het uitoefenen van controlebevoegdheden maar de camera's hebben een veel groter bereik dan de controlerende agent en computerprogramma's hebben een welhaast onbeperkt geheugen. Door de toepassing van nieuwe technologieën kunnen overheden maar ook bedrijven en instellingen zich meer en meer begeven in de levenssfeer van burgers die voorheen als privé werd aangemerkt. Als gevolg daarvan lijken

[13] Raad voor Maatschappelijke Ontwikkeling, *Ontkokering en Verkokering*, september 2008.

zowel die ‘inmenging’ als de aard en omvang van de persoonlijke levenssfeer anders te worden gepercipieerd dan bijvoorbeeld tien jaar geleden.
Wanneer de Commissie - vanuit haar ambitie te komen tot een richtinggevend kader voor de omgang met veiligheid en persoonlijke levenssfeer - kijkt naar die technologieën die het mogelijk maken gemakkelijker meer gegevens te verzamelen, te koppelen en te delen, verdienen vier belangrijke ontwikkelingen aandacht.

2.4.1. Typeren van personen

Doordat over steeds meer personen steeds meer gegevens worden verzameld en opgeslagen wordt typering van personen door middel van profilering en datamining op grotere schaal mogelijk. Nieuwe technologieën spelen ook daarom een steeds grotere rol in het veiligheidsbeleid. Politie en justitie beschikken in toenemende mate over mogelijkheden om met behulp van nieuwe technologieën persoonsgegevens te analyseren. Onder invloed van technologie is de aandacht van de overheid verschoven van een handelen gericht op een individu, naar handelen gericht op groepen van en typen van individuen.[14] Ook in de private sector is een dergelijke trend waar te nemen en worden door middel van datamining en profilering categorieën van individuen en groepen gecreëerd. Op basis van deze informatie wordt bijvoorbeeld bepaald wie welke lening, beveiliging of reclame krijgt. De wijk waarin iemand woont kan op deze wijze meer en meer bepalend zijn voor de maatschappelijke mogelijkheden van individuen.

2.4.2. “Immutable me”

Een ander gevolg van een toename van (gekoppelde) databestanden is dat de relevantie van de broncontext van verkregen gegevens afneemt. Door de toenemende intensiteit van samenwerken binnen de overheid en nieuwe uitgangspunten zoals het eenmalig uitvragen bij burgers worden steeds meer gegevens voor uiteenlopende doeleinden opgeslagen. Het gevaar dat daardoor ontstaat is de zogenaamde “immutable me”. Doordat gegevens zonder broncontext wordt opgeslagen kunnen er beelden van personen worden gecreëerd die niet of niet meer kloppen. Waar een jeugdhulpverlener ten aanzien van een jongere een risico signaleert omdat zijn broer het criminele pad opgaat kan deze jaren lang geregistreerd blijven als risicojongere. Maar ook de informatie die mensen over zichzelf op het internet zetten kan bijdragen aan het ontstaan van de “immutable me”. Het is immers vaak onmogelijk om

[14] J.E.J. Prins, “Technocratie en de toekomstagenda van de Nationale Ombudsman”, *Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context*, Den Haag 2007, pp. 130-131.

informatie die eenmaal op het internet is gezet nog te verwijderen, terwijl men zich hiervan niet ten volle bewust is.

2.4.3. Identiteitsfraude

Een van de andere risico's van het opslaan en koppelen van steeds meer gegevens is identiteitsfraude. Een goed en betrouwbaar beeld van de omvang van identiteitsfraude in Nederland ontbreekt maar identiteitsfraude is een groeiend probleem. Deze groei neemt toe naarmate er meer gegevens geautomatiseerd kunnen worden gewisseld. Identiteitsfraude kan verschillende gedaanten aannemen en vervelende gevolgen hebben, van het aangaan van een lening of afsluiten van een verzekering op naam van het slachtoffer tot het plegen van een strafbaar feit onder gebruikmaking van de identiteit van het slachtoffer.

Een recent rapport van de Nationale ombudsman (21 oktober 2008, nummer 2008/232) beschrijft het schrijnende voorbeeld van iemand die op naam van een ander (de verzoeker) talloze strafbare feiten gepleegd had. Als gevolg daarvan werd verzoeker tot ongewenst vreemdeling verklaard, werd hem een verklaring van geen bezwaar geweigerd en werd hij onderworpen aan een huiszoeking door de FIOD. Verzoeker probeerde de gevolgen van de diefstal van zijn identiteit al dertien jaar tevergeefs ongedaan te maken.

Naarmate meer gegevens over personen beschikbaar zijn, kunnen ook meer gegevens worden misbruikt voor identiteitsfraude. Bovendien kan er bij identiteitsfraude een omgekeerde bewijslast ontstaan, alle bewijzen leiden immers naar het slachtoffer die zich geconfronteerd ziet met valse beschuldigingen.[15]

Ter voorkoming van identiteitsfraude zijn goede voorlichting over omgang met gegevens en een goede bescherming van de systemen waarin de gegevens zijn opgeslagen onmisbaar.[16]

2.4.4. Slimme omgevingen

Techniek wordt steeds "slimmer" en geïntegreerd in allerhande producten die burgers in hun dagelijks doen en laten gebruiken. Hierdoor ontstaan "slimme omgevingen" oftewel "ambient intelligence omgevingen" waarbij de technologie steeds meer wordt verweven met de

[15] J.HA.M. Grijpink, Biometrie, veiligheid en privacy: enkele opvallende, richtinggevende ontwikkelingen, Privacy en informatie, 2008, afl. 1, p. 12.
[16] J.E.J. Prins en N.S. van der Meulen, Identiteitsdiefstal: lessen uit het buitenland in Identiteitsfraude, Justitiële verkenningen 2006/07, Den Haag 2006.

omgeving.[17] De ambient intelligence omgeving wordt gekenmerkt door een onzichtbaar netwerk van intelligente computers, sensoren en andere ICT-middelen. Deze intelligente, onzichtbare ICT-infrastructuur anticipeert en reageert op personen die zich in de omgeving bevinden. Naarmate de toepassing van dit soort technologieën toeneemt, wordt het steeds moeilijker voor individuen om zich hieraan te onttrekken.
Deze ontwikkelingen brengen mee dat beveiliging en integriteit van systemen en de gebruikers daarvan steeds belangrijker worden. Dat geldt evenzeer voor transparantie. Alleen zo kunnen burgers nog zicht houden op het gebruik van hun gegevens door overheid en bedrijfsleven. Omdat door het voortschrijden van de technologie gegevens steeds gemakkelijker worden uitgewisseld kan de informatieplicht uit de Wbp niet langer een voldoende waarborg bieden. Aldus bestaat er slechts zicht op wat er in eerste instantie met de gegevens gebeurt maar niet wat een volgende organisatie ermee doet.
Die steeds slimmere omgevingen stellen steeds hogere eisen aan de overheid. Die moet goed toegerust zijn om haar weg te kunnen vinden.

2.5. Overheid en bedrijfsleven

Niet alleen de overheid, ook de private sector verzamelt, verwerkt en analyseert op grote schaal persoonsgegevens. De mate en het karakter van de uitwisseling van persoonsgegevens tussen de private en de publieke sector is om verschillende redenen sterk veranderd. Door de grote vlucht die ICT genomen heeft en de groeiende verwevenheid tussen het private en publieke domein vinden thans gegevensuitwisselingen en -koppelingen plaats met een snelheid en op een schaal die tien jaar geleden niet waren voorzien.

Mag ik even een foto van u maken?

Camerabewaking door winkels voor de veiligheid, de regeling dat de caissière in uw tas mag kijken en de taxichauffeur die een foto van u maakt als u mee wilt rijden. De private sector kan deze maatregelen allemaal nemen als ‘algemene voorwaarden’ uit het privaatrecht. En als u hiertegen bezwaren heeft, dan bezoekt u de winkel maar niet of neemt u toch een andere taxi.
De overheid is bij vergelijkbare handelingen echter altijd gebonden aan democratisch controle en verantwoording en heeft (nog) niet de vrijheid om vergelijkbare ‘algemene voorwaarden’ te stellen.

De overheid verplicht private partijen ook steeds vaker tot het verstrekken van gegevens aan overheidsinstanties, voor een niet onbelangrijk deel met het oog op veiligheid. Bekende

[17] E. Aarts en S. Marzano, The new everyday view on ambient intelligence, Rotterdam 2003; B.W. Schermer, Ambient intelligence, persoonsgegevens en consumentenbescherming, ECP.nl 2008.

voorbeelden zijn verkeers- en locatiegegevens bij elektronische communicatie en passagiergegevens uit de burgerluchtvaart. Daarbij gaat het om gegevens die bedrijven in eerste instantie om een andere reden van hun klanten hebben gekregen. Uit gesprekken die de Commissie heeft gevoerd blijkt dat het bedrijfsleven dat als problematisch ervaart omdat daarmee een inbreuk wordt gemaakt op de vertrouwensrelatie die bedrijven met hun klanten onderhouden.

Dat roept wel belangrijke vragen op. Enkele daarvan zijn: hebben burgers, bedrijven en instellingen ook de mogelijkheden (gekregen) om preciezer en sneller op de hoogte te geraken van welke instantie over welke gegevens beschikt, aan welke andere instantie deze gegevens worden doorgeleverd, welke andere instantie om die gegevens heeft gevraagd; bestaan er nog adequate mogelijkheden om die gegevens en gegevensstromen te controleren en zo nodig te corrigeren? Ook is de vraag wie verantwoordelijk is voor de transparantie en het informeren van burgers in het geval de overheid gegevens van burgers in een later stadium opvraagt bij de private sector.

Een ander aandachtspunt is de verwevenheid publiek-privaat bij de ontwikkeling van nieuwe technologische instrumenten. Zo beschikken bijvoorbeeld lang niet alle gemeenten over de noodzakelijke kennis voor het ontwikkelen van complexe digital systemen, zoals een verwijsindex risicojongeren of een elektronisch kinddossier. De publieke instellingen zien zich vaak genoodzaakt de ontwikkeling van digitale systemen aan een externe organisatie over te laten, veelal een private partij. Er ontstaan dan vormen van samenwerking waarin niet alleen organisaties met een publieke taak participeren, maar ook particuliere bedrijven en adviesbureaus een steeds wezenlijker rol gaan vervullen. Technologie dwingt als het ware tot arrangementen van publiek-private samenwerking. Passende deskundigheid zal ook – en wellicht vooral – bij ICT-diensten binnen de overheid beschikbaar moeten zijn. Het is de moeite waard na te gaan of in de initiatieven om ICT-projecten meer geconcentreerde aandacht te geven, ook het privacybelang een passende plaats kan krijgen.

Een en ander zou de waarborgen zoals neergelegd in de regels ter bescherming van de persoonlijke levenssfeer onder druk kunnen zetten. Er zou dus meer helderheid moet komen over de vraag waar exact bepaalde verantwoordelijkheden rondom de invulling van de bescherming van persoonsgegevens belegd moeten worden. Wanneer de overheid bedrijven verplicht tot het verstrekken van gegevens over hun klanten zou het dan niet ook de overheid moeten zijn die voor de transparantie daarover moet zorgen? En zou het ook niet de overheid

moeten zijn die uitlegt waarom de te verstrekken gegevens nodig zijn, of ze daadwerkelijk worden gebruikt en waarvoor dan en of het niet met minder kan. En moet ook de overheid zich met behulp van een in de wet neergelegde horizonbepaling niet tot geregelde heroverweging van nut en noodzaak van gegevensverwerking verplichten?

2.6 De private sector

Met wisselende accenten beogen bedrijven winst te maken, de continuïteit te verzekeren en belangen van aandeelhouders en werknemers veilig te stellen. Vertrouwen van klanten, van aandeelhouders en werknemers en vertrouwen van bedrijven met wie zaken worden gedaan domineren de gang van zaken binnen de private sector. Inspelen op dat vertrouwen biedt mogelijkheden om algemene belangen in het primair proces van een bedrijf goed te verankeren. Dat gebeurt op beleidsterreinen als milieuzorg, arbeidsomstandigheden en kwaliteitszorg door aan te zetten tot private normalisering en certificering. Waar de overheid dan soms weer gebruik van maakt door naar die private normen en certificering te verwijzen.

Het vertrouwen dat de gang van zaken in de private sector domineert kan ook het belang van privacy ondersteunen. Zo geven kritische volgers van omgang met persoonsgegevens aan dat banken en verzekeraars over het geheel genomen zorgvuldig omgaan met persoonsgegevens omdat zij het vertrouwen van hun klanten niet willen verspelen. Dat roept de vraag op of het mogelijk zou zijn ook in andere sectoren dan banken en verzekeraars met vaak kleinere bedrijven in te spelen op ‘vertrouwen’. Het privacybelang lijkt heel wel te kunnen worden verankerd in door bedrijven zelf op te zetten zorgsystemen. Certificering daarvan kan ‘privacy’ zo tot een *unique selling point* maken.

2.7. Internationale ontwikkelingen

Ook in internationaal verband is de afgelopen jaren een beweging zichtbaar geworden waarin veiligheids- en anti-terrorismemaatregelen zijn getroffen waarbij de bescherming van de persoonlijke levenssfeer niet van het begin af aan gelijkwaardig is meegewogen. Omdat internationale instrumenten, maar dat geldt ook voor nationale instrumenten, veelvuldig los van elkaar en daardoor versnipperd tot stand komen, wordt het zicht op de samenhang tussen de verschillende maatregelen en de verhouding van deze maatregelen tot de bestaande privacyinstrumenten nog eens extra bemoeilijkt. Er zijn velerlei doelen waarvoor op internationaal en Europees niveau persoonsgegevens worden geregistreerd, uitgewisseld, gebruikt en bewaard. Enkele voorbeelden zijn het Schengeninformatiesysteem (gegevens van

ongewenst verklaarde vreemdelingen), Eurodac (vingerafdrukken voor de identificatie van asielzoekers), het Ecrissysteem (geautomatiseerde uitwisseling tussen EU-lidstaten uit nationale strafregisters) en gegevensuitwisseling met derde landen (onder andere passagiersgegevens die aan de Verenigde Staten worden verstrekt).

Daarnaast zijn er diverse internationale verdragen, Europese richtlijnen en kaderbesluiten die gedeeltelijk zien op de bescherming van de persoonlijke levenssfeer. De belangrijkste daarvan zijn artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR), het Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981 (Dataprotectieverdrag; Trb. 1988, 7) en de Richtlijn nr. 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Privacyrichtlijn; Pb EU 2003, 284). Opvallend is dat deze instrumenten aanzienlijk ouder zijn dan de in de vorige alinea beschreven veiligheidsinstrumenten en de wettelijke normen hierin bovendien veelal open zijn geformuleerd. Daardoor biedt de regeling ruimte voor nadere inkleuring en de flexibiliteit om mee te bewegen met ontwikkelingen en behoeften op het terrein van veiligheid.

De belangrijkste conclusie is dat in internationaal verband de aandacht voor veiligheidsmaatregelen niet gelijk op is gegaan met de aandacht voor privacybescherming. Daar waar wel aan de bescherming van de persoonlijke levenssfeer is gedacht, diende dat vooral om de veiligheidsmaatregelen te accommoderen. Internationaal blijkt niet van de aanwezigheid van een algemene visie op de balans tussen veiligheid en de persoonlijke levenssfeer.

2.8. Waarheen, waarvoor

Alle beschreven maatschappelijke ontwikkelingen zetten de spanning tussen veiligheid en persoonlijke levenssfeer meer ‘op scherp’. Wij hebben als samenleving heel wat verlangens en wensen op het terrein van veiligheid en persoonlijke levenssfeer. Het willen voorkomen van risico’s, het overzien en voorzien van mogelijkheden en bezwaren van technische ontwikkelingen, de vervlechting van private en publieke doelen en middelen, alsmede de internationale druk leiden ertoe dat de vragen die betrekking hebben op de spanning tussen veiligheid en persoonlijke levenssfeer steeds vaker in een vroeg stadium moeten worden

beantwoord. Het is voor rechtshandhavers en hulpverleners complexer om ‘het goede te doen’.
De ene hulpverlener mag gegevens wel verzamelen, de andere niet. Soms moeten gegevens worden gedeeld, dan weer mag het niet. Hetzelfde geldt voor de vervlechting tussen het publieke en private domein. De burger die zijn gegevens aan een bedrijf geeft kan daar later in een heel ander kader door de overheid mee worden geconfronteerd. Het wordt voor de burger steeds lastiger om te overzien wat er met persoonsgegevens kan gebeuren. Ook technologische ontwikkelingen maken het belang van transparantie voor burgers pregnanter. De ontwikkelingen onder paragraaf 2.4 laten immers zien dat het steeds gemakkelijker zal worden om meer gegevens te verzamelen en misschien nog wel belangrijker om daar vervolgens conclusies uit te trekken. Bovendien is tussenkomst van de betrokken burger of instelling zelf daar steeds minder voor nodig, waardoor beelden van die burger of instelling kunnen worden gecreëerd die niet of niet meer kloppen. Het is de vraag of zij zich daar voldoende van bewust zijn en of er voldoende middelen zijn om nadelige gevolgen adequaat te voorkomen respectievelijk tegen te gaan.

De roep om potentieel onveilige situaties te voorkomen en de voortschrijdende technologische ontwikkeling maken dat steeds vaker de vraag wordt voorgelegd: wanneer verzamelen we informatie, wanneer delen we die met anderen, wanneer grijpen we op basis daarvan in? De oplossing is niet gelegen in meer wet- en regelgeving, die nu al voor rechtshandhaver, hulpverlener, burger en bedrijfsleven moeilijk te volgen is. Op basis van zowel de eigen analyse, als de gesprekken met deskundigen constateert de Commissie dat bestaande wet- en regelgeving veelal op hoofdpunten voldoende ruimte biedt voor het realiseren van een goede balans tussen privacy en veiligheid, maar dat het moeilijk is de brug te slaan naar de praktijk.

Daar zijn meerdere redenen voor. Afhankelijk van het tijdsframe wordt er kort gezegd of meer waarde gehecht aan veiligheid of meer waarde gehecht aan privacy. Het is moeilijk om uit die patstelling te komen, is men voor het bevorderen van veiligheid dan is men tegen privacybescherming en andersom. Daar komt nog bij dat privacy vaak vanuit een strikt juridisch oogpunt op zichzelf wordt bekeken, hetgeen een open discussie verder bemoeilijkt. De Commissie meent dat privacy als een normaal beleidsterrein moet worden gezien. Het spreekt voor zich dat de bestaande internationale en nationale juridische randvoorwaarden daarbij – net als bij andere beleidsterreinen – van groot belang zijn. Maar dat neemt niet weg dat ook andere overwegingen (zoals efficiency, financiën, politiek, professionaliteit) een

belangrijke rol horen te spelen. Met andere woorden, door privacy als een normaal beleidsterrein of een onvermijdelijk facet van vele beleidsterreinen te zien, kan de discussie op basis van meer overwegingen gevoerd worden dan alleen de (schijnbare) tegenstelling tussen veiligheid en privacy. De Commissie is van mening dat een kader voor het omgaan met de balans tussen privacy en veiligheid ertoe kan bijdragen om uit de “verstarring” van het huidige debat te komen.

Een andere reden waarom de bestaande wet- en regelgeving in de praktijk onvoldoende werkt is het hoge abstractieniveau daarvan. Belangrijke uitgangpunten van de Wet bescherming persoonsgegevens als doelbinding, subsidiariteit en proportionaliteit bieden weliswaar de mogelijkheid voor het realiseren van een zorgvuldige balans tussen privacy en veiligheid maar zijn soms moeilijk te vertalen naar een concreet geval. Het wringt zich dat vaak strikt naar regels wordt gekeken zonder echt te kijken naar wat in het concrete geval noodzakelijk en wenselijk is. De Commissie is van mening dat een duidelijke handreiking voor het maken van concrete afwegingen noodzakelijk is. De praktijk moet daarbij ruim worden opgevat. Het kan gaan om een restauranthouder die zichzelf en collega’s wil hoeden voor niet betalende klanten of om de docent die ziet dat een van zijn leerlingen wel erg vaak blauwe plekken heeft. Het kan ook een luchtvaartmaatschappij betreffen die haar klanten een halalmaaltijd wil kunnen voorschotelen zonder dat deze bang hoeven te zijn als potentiële terroristen te worden aangemerkt. De praktijk kan ook overheidsorganen of -instellingen betreffen. De burgemeester die moet afwegen of hij burgers al dan niet op de hoogte brengt van het feit dat er een veroordeelde pedofiel in hun wijk woont. Of bij het toepassen van kentekenherkenning met camera’s.

Om die afwegingen te vergemakkelijken, is er naar het oordeel van de Commissie een kader nodig voor een verantwoorde omgang met persoonsgegevens. De rode draad in dit kader zou naar het oordeel van de Commissie moeten zijn “houd het eenvoudig, faciliteer**,** verlang dat de balans voorop staat en maak werk van een robuuste handhaving”. Het volgende hoofdstuk laat zien hoe dit kader er naar het oordeel van de Commissie uit zou moeten zien.

HOOFDSTUK 3 NAAR EEN RICHTINGGEVEND KADER

Richtinggevend kader voor informatieverwerking en veiligheid

3.1. Inleiding

"Moeten we een bepaald systeem voor uitwisseling van persoonsgegevens voor de veiligheid wel willen ontwikkelen? En als we zo'n systeem hebben, wanneer moeten we dan de beschikbare persoonsgegevens uitwisselen? Wat kunnen we doen om de zorgvuldigheid bij de omgang met persoonsgegevens ten behoeve van de veiligheid zo goed mogelijk te waarborgen?"

Om bij te dragen aan rationaliteit en consistentie bij het beantwoorden van dit type vragen ontwikkelt de Commissie in dit hoofdstuk een richtinggevend kader voor het omgaan met persoonsgegevens ten behoeve van de veiligheid. Naast deze functie als middel tot 'evaluatie ex ante' kan het richtinggevende kader ook dienen als inspiratiebron voor het ontwikkelen van op specifieke werkplekken toegesneden eenvoudige *'do's en dont's'* voor de mensen die dagelijks met persoonsgegevens met betrekking tot veiligheid omgaan. Ook biedt het richtinggevende kader aanknopingspunten voor de uitvoering van beslissingen om persoonsgegevens voor de veiligheid te benutten: het kader prikkelt uitvoerders tot alertheid bij de implementatie van beslissingen om veiligheid te beschermen door met persoonsgegevens te werken.

3.2 Wettelijke kaders

3.2.1 Bestaand wettelijk kader veiligheid

De zorg voor de veiligheid van de burgers is één van de klassieke taken van de overheid. Het wettelijke kader voor 'veiligheid' in samenhang met uitwerking van klassieke grondrechten is verspreid geregeld in wetten als de Politiewet 1993, de Wet op de bijzondere opsporingsdiensten, de Gemeentewet, de Wet op de rechterlijke organisatie, de Wet op de inlichtingen- en veiligheidsdiensten 2002, het Wetboek van Strafrecht, het Wetboek van Strafvordering en vele andere. Rond de millenniumwisseling heeft de wetgever de bestaande wetgeving met een aantal onderwerpen aangevuld, zoals DNA-onderzoek en DNA/databank[1], cameratoezicht[2], bijzondere opsporingsbevoegdheden[3], identificatieplicht[4] en het vorderen van gegevens[5].

---

[1] Wet DNA-onderzoek bij veroordeelden, Stb. 2004, 465.

3.2.2 Bestaand wettelijk kader omgang met persoonsgegevens

Het eerste hoofdstuk van dit advies beschreef de verschillende aspecten van ´persoonlijke levenssfeer´. Een aspect daarvan, de verwerking van persoonsgegevens, is geregeld in het tweede en derde lid van artikel 10 van de Grondwet, die opdracht geven tot wetgeving ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens respectievelijk tot wetgeving voor de aanspraken van personen op kennisneming, gebruik en verbetering van over hen vastgelegde gegevens.

Artikel 8 van de Wbp vormt een kernbepaling.[6] Wetten voor specifieke terreinen geven aan dit artikel nadere invulling, zoals de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens, de Wet op de Inlichtingen- en veiligheidsdiensten, de Wet Gemeentelijke basisadministratie persoonsgegevens, de Kieswet en vele andere.
De Wbp hanteert enkele ‘open normen’, zoals ‘behoorlijke en zorgvuldige verwerking van persoonsgegevens’. De wetgever beoogt zo ruimte te geven aan nadere invulling en concrete toepassing van de wettelijke normen met behulp van codes en protocollen door branches, (organisaties van) instellingen en sectoren.

Leidende beginselen van de Wbp zijn:

- Legitieme doelbinding

---

[2] Wet cameratoezicht op openbare plaatsen, Stb. 2005, 392.
[3] Wet bijzondere opsporingsbevoegdheden, Stb. 1999, 245. Per saldo wetgeving ter codificering van het vervolg op de Commissie Van Traa.
[4] Wet op de uitgebreide identificatieplicht, Stb. 2004, 300.
[5] Wet bevoegdheden vorderen gegevens, Stb. 2005, 390.
6 Artikel 8 Wbp: Persoonsgegevens mogen slechts worden verwerkt indien:
a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Het doel waarvoor gegevens mogen worden vastgelegd en verwerkt of verstrekt moet legitiem zijn en de gegevens mogen niet voor een ander doel worden gebruikt dan waarvoor ze zijn verkregen.

- Transparantie en voorzienbaarheid

  In het concrete geval moet de burger over voldoende informatie kunnen beschikken over wat er met zijn persoonsgegevens gebeurt. Het gaat er om dat de burger kan weten waarom gegevens worden verzameld, welke gegevens worden verzameld en welke gegevens aan derden worden verstrekt.
  Uitzonderingen op het beginsel van transparantie zijn mogelijk, maar de uitzonderingsgronden moeten strikt worden geïnterpreteerd. De burger heeft in beginsel het recht tot inzage en correctie van zijn gegevens.
  In meer algemene zin geldt dat de burger zijn gedrag moet kunnen afstemmen op de regels die gelden voor het omgaan met zijn persoonsgegevens. Die regels moeten voldoende precies zijn, zodat de burger kan voorzien wat er met zijn gegevens gebeurt.

- Proportionaliteit en subsidiariteit

  Afgezien wordt van de verwerking van persoonsgegevens, indien hetzelfde doel ook langs andere weg en met minder ingrijpende middelen kan worden gerealiseerd. Wordt desondanks tot gegevensverwerking overgegaan, dan is van belang dat degene die gegevens wil verwerken in redelijkheid alle eventuele bestaande mogelijkheden benut om inmenging in de persoonlijke levenssfeer van de betrokkenen te beperken. Er moet een noodzaak zijn in relatie tot een welbepaald, concreet aangeduid of nader aan te duiden doel.[7]
  Deze beginselen schrijven in combinatie met de doelbinding ook voor dat geen bovenmatige gegevensverwerking plaatsvindt.

3.2.3. Kanttekeningen bij de wettelijke kaders

Bij de wettelijke kaders zoals hierboven beschreven maakt de Commissie de volgende kanttekeningen:

a. Wettelijk kader veiligheid is actueel, wettelijk kader bescherming persoonsgegevens is

[7] Uit de memorie van toelichting Wbp, p. 8.

deels verouderd.

In vervolg op het werk van de Commissie bijzondere opsporingsmethoden en in reactie op bedreigingen vanuit zware georganiseerde criminaliteit en terrorisme zijn de afgelopen tien jaar vele nieuwe wetten van kracht geworden. Zo is het wettelijke kader voor de veiligheid actueel gehouden. Politieke en maatschappelijke wensen hebben hun weg naar het Staatsblad gevonden.

Geen actualisering daarentegen vond plaats van het algemene wettelijke kader voor de bescherming van persoonsgegevens. Men zou verwachten dat nieuwe technologieën, globalisering en verdergaande overheidsbevoegdheden bij wetgeving ter bevordering van veiligheid, de wetgever zouden hebben aangezet tot actualisering van de bestaande regels op dit terrein. Dat blijkt niet het geval. De Wbp die in 2001 van kracht werd als opvolger van de Wet persoonsregistraties, strekte primair tot de implementatie van de Europese privacyrichtlijn. Bij deze gelegenheid was er minder aandacht voor aanpassing van het wettelijke kader met het oog op de omgang met persoonsgegevens in de dagelijkse praktijk.[8] Zowel over de toekomst van het bredere begrip privacy als de (feitelijke) omgang met persoonsgegevens werd overigens wel geregeld gerapporteerd en vond evaluatieonderzoek plaats.[9] Tot op heden hebben de uitkomsten hiervan niet in aanpassing van wetgeving geresulteerd.

b. *Praktisch afwegingskader privacy ontbreekt.*

Er is geen overkoepelend kader beschikbaar aan de hand waarvan concrete afwegingen over omgang met gegevens op het raakvlak van veiligheid en persoonlijke levenssfeer op een systematische manier plaats kunnen vinden. Leidend in het denken over een dergelijk kader zijn de beginselen die in de Wbp zijn gecodificeerd, zoals legitieme doelbinding, transparantie en voorzienbaarheid, resp. subsidiariteit en proportionaliteit. Maar als zodanig vormen deze beginselen en de concrete uitwerking daarvan in de wettelijke

[8] Zie voor evaluatie van de Wet persoonsregistraties:
- J.E.J. Prins, W.B.H.J. van de Donk, e.a., *Zon, Maan of Ster? In het licht van de Wet persoonsregistraties*, Den Haag: Ministerie van Justitie, 15 december 1995;
- G Overkleeft-Verburg, *De Wet persoonsregistraties Norm toepassing en evaluatie*, diss. KUB, Zwolle 1995.

[9] Vgl. de respectieve commissies Franken (*Grondrechten in het digitale tijdperk*, Den Haag 2000) en Bosma (*Data voor daadkracht*, Den Haag 2007). En verder: G-J. Zwenne, A.W. Duthler e.a., *Eerste fase evaluatie Wet bescherming persoonsgegevens, Literatuuronderzoek en knelpuntenanalyse*, Leiden 2007; en E.R. Muller, H.R.B.M Kummeling, en R.P. Bron, *Veiligheid en privacy Een zoektocht naar een nieuwe balans*, Den Haag 2007.

bepalingen van de Wbp naar hun aard niet een kader om een systematische afweging mogelijk te maken over de wenselijkheid tot introductie of juist beëindiging van specifieke vormen of systemen van persoonsgegevensverwerking. Dat is nu eenmaal niet de functie van een wet. Of het opzetten – dit ter illustratie – van een VerwijsIndex Antillianen gerechtvaardigd is hangt in eerste instantie niet af van een bestaande wet, maar van een politiek oordeel dat mogelijk tot wetswijziging moet leiden. De rationaliteit van dat oordeel is gebaat bij een afwegingskader dat uitnodigt tot een systematische, interdisciplinaire en intersubjectieve benadering.

3.3 Wat komt er in de praktijk van de wetgeving terecht?

'Professionals'[10] hebben in de dagelijkse praktijk behoefte aan houvast bij de toepassing van de algemene beginselen voor de bescherming van de persoonlijke levenssfeer. Hun organisaties moeten hun dat houvast geven. Zeker wanneer instellingen samenwerken om tot een effectieve aanpak van een maatschappelijk probleem te kunnen komen, blijken de 'professionals' verschillende werkwijzen te hanteren bij de uitwisseling van gegevens. Soms moet dat ook. Zo is bijvoorbeeld op gegevensuitwisseling door een psychiater een ander regiem van toepassing dan op gegevensuitwisseling door een jeugdhulpverlener. Hoe ingewikkelder het voor de 'professionals' op de werkvloer wordt – grote veiligheidsbelangen voor individuele burgers, verschillende samenwerkingspartners met allemaal een eigen cultuur – des te meer komt het bij de toepassing van regels aan op eenvoud en verankerde mechanismen. Maar in de praktijk ontbreekt het daar aan:

- 'De privacywet' heeft de reputatie erg ingewikkeld te zijn. 'Professionals' ervaren privacywetgeving dikwijls als een 'ver-van-mijn-bedshow'. Privacyspecialisten zitten

[10] Alle functionarissen die werkzaamheden verrichten ten behoeve van veiligheid noemt de Commissie in dit advies 'professional'. Het gaat om een zeer diverse groep: politiemedewerkers, psychiaters, jeugdhulpverleners, toezichthouders, artsen, gezinsvoogden, therapeuten, officieren van justitie en vele anderen zoals medewerkers van uitvoeringsorganisaties, dienstverleners aan balies en loketten. Zij allen werken in wisselende samenstelling en intensiteit aan het waarborgen van de veiligheid van mensen en doen zeer uiteenlopend werk. Sommige 'professionals' werken elke dag met mensen van wie de veiligheid is bedreigd, terwijl anderen slechts incidenteel en in de eigen beleving nauwelijks persoonlijk contact met hen hebben. Ook beschikken zij over zeer uiteenlopende competenties en werken zij vanuit zeer verschillende disciplines. Hun gemeenschappelijk kenmerk is dat ze soms werken met persoonsgegevens ten behoeve van veiligheid. Hun diversiteit is van belang: hen helpen de goede afwegingen te maken bij omgaan met persoonsgegevens moet op hun opleidingsniveau en type werk zijn toegesneden.

vaak ver weg van de werkvloer en hebben weinig gelegenheid zich te verdiepen in de dynamiek van die werkvloer. 'Professionals' op die werkvloer voelen zich daardoor weinig geprikkeld de privacyspecialisten te raadplegen.

- 'Dat mag niet van de privacywetgeving' fungeert nogal eens als dooddoener om gegevens niet te hoeven delen. In weer andere situaties worden gegevens weer te gemakkelijk gedeeld als gevolg van onbekendheid met de regels. 'Niemand in de buurt die weet hoe het precies zit en dan moet je toch wat…!'
- Het ontbreekt soms aan inzicht bij de partners over en weer in elkaars belangen bij en mogelijkheden tot al dan niet uitwisselen van gegevens. Dit leidt tot onzekerheid bij het wel of niet delen van persoonsgegevens. Zo kan een medisch beroepsgeheim in z'n algemeenheid aan delen van gegevens in de weg staan. Bij een belang als dat van de veiligheid van kinderen zien we echter dat het beroepsgeheim in een concrete situatie soms behoort te wijken[11].
- Zelfregulering in de vorm van gedragscodes in de zin van de Wbp is nog niet of nauwelijks tot stand gekomen; de website van het College bescherming persoonsgegevens maakt momenteel melding van zeven goedgekeurde gedragscodes, waarvan er twee zijn verlopen[12]. De evaluatie van de Wbp laat ook een grote mate van onbekendheid met de zelfreguleringsinstrumenten zien. Er staat eerder rem dan prikkel op zelfregulering: goedkeuring van codes door het College bescherming persoonsgegevens duurt lang, vergt van alle partijen heel veel tijd en aandacht en levert uiteindelijk zeer gedetailleerd commentaar op met weinig empathie voor de dagelijkse praktijk.
- Van kleinere bedrijven en organisaties in een veranderende wereld met steeds nieuwe uitdagingen kan nauwelijks worden verwacht dat zij de '*state of the art*' van de omgang met persoonsgegevens nauwgezet bijhouden. Er bestaat niet veel aandacht voor de vraag hoe zij daarbij gefaciliteerd kunnen worden.
- Het recht op inzage en correctie van persoonsgegevens kent vaak een hoge drempel en de ingang bij organisaties en met name samenwerkende instanties in ketens, om deze rechten te effectueren is nauwelijks kenbaar noch transparant voor burgers en hun organisaties.

[11] Om goede redenen is de GGZ terughoudend met uitwisselen van persoonsgebonden informatie. Maar ook weer om goede redenen zit er beweging in dat veld. Zo roemt de Inspectie Gezondheidszorg de "duidelijke afspraken" in Gelderland waar ook de GGZ bij betrokken is over de uitwisseling van informatie bij vermoedens van kindermishandeling.
[12] Peildatum 7 januari 2009.

De centrale conclusie is dat het juridische systeem voor zorgvuldige omgang met persoonsgegeven vrijwel geen vertaling heeft gekregen naar de werkvloer. 'Professionals' die werken aan de veiligheid van personen blijken onvoldoende toegerust om handen en voeten te kunnen geven aan het juridische systeem van de omgang met persoonsgegevens.

3.4 Diagnose

Zoals hierboven al uiteengezet hangt een gebrekkige omgang met persoonsgegevens samen met twee onderling samenhangende factoren:

a. Zorgvuldige omgang met privacyregels is niet "ingebakken" in het dagelijkse werk van de 'professionals' en hun organisaties, en
b. de discussie over zorgvuldige omgang met persoonsgegevens wordt sterk gedomineerd door een bijna exclusief juridische invalshoek.

3.4.1 Niet in het werk ingebakken

Een politieagent staat vaak voor situaties waarin direct optreden nodig is. Gezinsvoogden, psychiaters, jeugdhulpverleners willen in concrete situaties gemakkelijk kunnen bepalen of gegevens wel of niet gedeeld moeten worden. Daarvoor moet het niet nodig zijn dat deze 'professionals' beschikken over gespecialiseerde kennis van de privacywetgeving. Zij zijn het meeste geholpen met een aantal '*do's and dont's'* voor de meest voorkomende situaties en een helpdesk of vraagbaak voor de overige gevallen. Juist op het moment dat men voor dilemma's komt te staan moet men op zekerheden kunnen terugvallen en zijn verankerde en verinnerlijkte protocollen nodig voor goede toepassing van de wet.

3.4.2 Juridische dominantie

Op elk terrein van het overheidsbeleid spelen politieke, economische, professionele en juridische aspecten een rol.[13] Op een 'normaal beleidsterrein' is er voorlichting, zijn er financiële prikkels, zijn er uit oogpunt van machtsverdeling '*checks*' en '*balances*' en proberen de mensen die op dat terrein werken alle relevante aspecten van hun werk evenwichtig in dat werk te incorporeren. Dat resulteert soms in normering door NEN en ISO[14] van zorgsystemen op milieugebied, fysieke veiligheid, arbeidsomstandigheden en kwaliteit van bijvoorbeeld bouwmaterialen. Overheidsregelgeving verwijst vervolgens soms

[13] Vgl. Ig Snellen, Grondslagen van de bestuurskunde, Meppel 2008, p. 80 e.v.,
[14] Nederlands centrum voor normalisatie resp. International Organisation for Standardization

weer naar deze privaat tot stand gekomen normen. Een ‘privacyzorgsysteem’ is daarentegen nog niet ontwikkeld. Beleid over ‘zorgvuldige omgang met persoonsgegevens’ kenmerkt zich door een sterk juridisch accent, waarbij eigenlijk alleen juridische instrumenten in het leven geroepen zijn om de zorgvuldige omgang met persoonsgegevens te waarborgen. Vele aspecten blijven als gevolg daarvan onderbelicht, zoals:

- hoe te waarborgen dat de ‘professionals’, die met persoonsgegevens werken, de regels in hun dagelijkse werk goed toepassen?
- hoe te organiseren dat deze ‘professionals’ voldoende rugdekking van hun organisaties krijgen?
- welke beleidsmatige en economische overwegingen spelen in de praktijk van ‘professionals’ op de werkvloer bij gegevensverwerking een rol; hoe kunnen deze overwegingen de zorgvuldige omgang met persoonsgegevens versterken?
- is er sprake van machtsverschuivingen als gevolg van toegang tot, alsmede verwerking, beschikbaarheid en uitwisseling van persoonsgegevens en wat zijn daar de gevolgen van?
- hoe kunnen we de privacyregels zo goed en zo vroeg mogelijk inbouwen in technische systemen en organisatorische praktijken (*privacy by design)* en hoe kunnen we dit ‘inbouwen’ stimuleren?

Dergelijke aspecten blijven in de discussies rond de verhouding veiligheid en persoonlijke levenssfeer momenteel te veel op de achtergrond. Als gevolg daarvan komen de privacyregels in de praktijk onvoldoende tot leven en krijgt privacy niet de ruimte zich te ontwikkelen tot een ´normaal´ beleidsterrein dan wel een vanzelfsprekend aspect van alle relevante beleidsterreinen. Het gaat er om in een meer afgewogen ‘mix’ overwegingen van veiligheid en privacy met elkaar in verband te brengen. Een juridische benadering vervult in die mix onmiskenbaar een wezenlijke functie. Maar om organisaties die aan veiligheid werken te prikkelen tot een op de werkvloer afgestemde zorgvuldige balans tussen veiligheid en persoonlijke levenssfeer is meer nodig.

3.5 Veiligheid en persoonlijke levenssfeer als normaal beleidsterrein: richtinggevend kader

3.5.1 Inleiding: functies van het richtinggevende kader

De Commissie formuleert hieronder in een richtinggevend kader grondslagen en handreikingen voor zorgvuldige omgang met persoonsgegevens in de situaties dat er spanning kan ontstaan met het werken aan de veiligheid. Voor wie op de werkvloer van

veiligheid en persoonsgegevens vreest dat er nu heel veel nieuws op hem afkomt: dit kader vloeit rechtstreeks voort uit al bestaande verplichtingen. Het geeft aan wat – als het goed is – al gebeurt en anders wat al gebeurd had moeten zijn. Het beoogt er aan bij te dragen om informatieverstrekking ten behoeve van veiligheid als een normaal beleidsterrein te kunnen opvatten.

De grondslagen en handreikingen maken het mogelijk langs systematische weg tot een oordeel te komen over de wenselijkheid van een specifiek voorgesteld of bestaand geheel van voorzieningen waarbinnen persoonsgegevens worden verwerkt om veiligheid te waarborgen. Het kader versterkt de rationaliteit van de beslissing of men een bepaalde verwerking van persoonsgegevens wel of niet zou moeten willen: toepassing van het kader op een concrete casus brengt de spanning die er kan zijn tussen veiligheid en privacy in beeld en faciliteert het nadenken over de diverse te maken afwegingen. Dat maakt het mogelijk een weloverwogen beslissing te nemen over wenselijkheid en uitwerking van een systeem. Tegelijk draagt het richtinggevende kader bij aan risicobeheersing: de kwetsbare elementen van een systeem van omgaan met persoonsgegevens worden inzichtelijk, zodat maatregelen kunnen worden genomen om de risico's te beperken en te beheersen. Tenslotte geven de algemeen geformuleerde grondslagen en handreikingen van het richtinggevende kader de koers aan voor het ontwerpen van concrete instructies voor mensen op een specifieke werkvloer. Dit kader kan alleen functioneren binnen de randvoorwaarden van artikel 8 EVRM en de Europese privacyrichtlijn. Inmenging in de persoonlijke levenssfeer kan alleen plaatsvinden als de noodzaak daarvan vaststaat en de beginselen van proportionaliteit en subsidiariteit in acht zijn genomen.

3.5.2 Geadresseerden van het kader

Het kader richt zich in de eerste plaats tot de opdrachtgevers van de Commissie en het kabinet, de ministers van Justitie en BZK. De Commissie adviseert hen dit kader over te nemen en er mee aan de slag te gaan. Onder meer door er in de Aanwijzingen voor de regelgeving naar te verwijzen. Maar ook zonder hun tussenkomst hoopt de Commissie dat de inzichten van het richtinggevende kader hun weg vinden. De Commissie doet een beroep op opdrachtgevers en systeemontwerpers om privacyoverwegingen al in de allereerste plannen en ontwerpen voor systemen te verankeren. Alle betrokken organisaties zouden direct aan de slag moeten gaan met het faciliteren van hun 'professionals'. En met het waarborgen van voldoende rugdekking voor die 'professionals'. Terwijl organisaties die op het

veiligheidsterrein met persoonsgegevens omgaan direct van start zouden moeten gaan met het heel concreet wegnemen van de huidige drempels voor burgers voor hun recht op inzage en correctie van hun gegevens.

3.5.3 Richtinggevend kader: grondslagen en handreikingen; kader, model en toelichting

Figuur 1 hieronder zet de grondslagen en bijbehorende handreikingen voor de informatieverwerking op het specifieke gebied van de veiligheid bij elkaar. De eerste drie grondslagen richten zich tot degenen die met gegevens omgaan en zijn op dat omgaan als zodanig van toepassing. Indien niet is voldaan aan deze grondslagen valt de ‘basis’ onder de rechtmatigheid van de omgang met gegevens weg. Zo is de grondslag ‘indien noodzakelijk voor de veiligheid, moet je delen’ pas aan de orde wanneer voldaan is aan alle aspecten van ‘selecteer voor je verzamelt’. Ook moet bij het uitwisselen van specifieke gegevens over een persoon steeds een risicobeoordeling voorafgaan aan toepassing van de grondslagen ‘transparantie, tenzij’, ‘selecteer voor je verzamelt en houdt het sober’ en ‘delen, tenzij’.
De andere grondslagen hebben betrekking op de organisatie, d.w.z. zijn van toepassing op systemen, het materiaal waarmee en de context waarbinnen gegevens worden verwerkt. Deze grondslagen richten zich op de organisatie waarbinnen ‘professionals’ werken en de omgeving daarvan: hun werkgever, opdrachtnemers van ICT-projecten, de beroepsverenigingen van ‘professionals’, branches en de overheid als organisatie die de zorgvuldige omgang met persoonsgegeven faciliteert.

Grondslag 1. 'Transparantie, tenzij'

a. Maak de burger duidelijk of verstrekking van zijn gegevens wettelijk verplicht is of niet. Maak de burger duidelijk om welke andere reden dan een wettelijke plicht zijn gegevens worden verwerkt.

b. Maak duidelijk met welk doel de persoonsgegevens worden verzameld en gebruikt zonder daarbij – mogelijke toekomstige – doelen te verzwijgen.

c. Bied inzicht in wat er met de gegevens gebeurt en zeg ook duidelijk aan wie de gegevens worden doorverstrekt.

d. Maak het de persoon om wie het gaat mogelijk en gemakkelijk de gegevens te controleren en te corrigeren en daar waar wettelijk toegestaan verzet aan te tekenen.

Grondslag 2. 'Selecteer voor je verzamelt' en houd het sober ('select before you collect')

e. Verzamel alleen persoonsgegevens met een rechtmatig doel, rekenschap gevend van de belangen van proportionaliteit en subsidiariteit.

f. Stel voorafgaand aan de verzameling een concrete risicoanalyse op en maak daarin duidelijk wat met het oog op de voorgestelde aanpak de rol van de verzamelde persoonsgegevens is.

g. Verzamel niet meer persoonsgegevens dan je op basis van de vooraf op te stellen risicoanalyse nodig hebt en zult gebruiken.

h. Scherm persoonsgebondenheid zo veel mogelijk af.

i. Bewaar gegevens niet langer dan nodig en zorg voor vernietiging daarna ('horizon').

j. Gebruik persoonsgegevens alleen voor het wettelijk geregelde doel of – bij vrijwillige verstrekking – het doel waarvoor toestemming is verleend (doelbinding) of wanneer sprake is van een vitaal belang van betrokkene.

Grondslag 3. ´Indien noodzakelijk voor de veiligheid, moet je delen´

k. Persoonsgegevens moet je delen als uit een risicobeoordeling blijkt dat delen noodzakelijk is voor de veiligheid.

l. Wanneer de noodzaak van delen voor de veiligheid niet vaststaat:

- deel persoonsgegevens in geval van vrijwillige verstrekking alleen wanneer de verstrekker daar uitdrukkelijk toestemming voor geeft en de gevolgen van die toestemming kan overzien.
- deel in geval van wettelijk verstrekte persoonsgegevens deze alleen met anderen als de wet het toelaat.

Grondslag 4. Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers

m. Zorg steeds voor correcte, actuele, volledige gegevens uit oogpunt van bron- en gebruikscontext.

n. Zorg voor veilige systemen.

o. Zorg dat de systemen voor de gegevensverwerking precies zijn toegerust op de doelen van verwerking.

p. Zorg voor integere omgang van de 'professionals' met de systemen.

Grondslag 5: Zorg voor voorlichting en faciliteiten

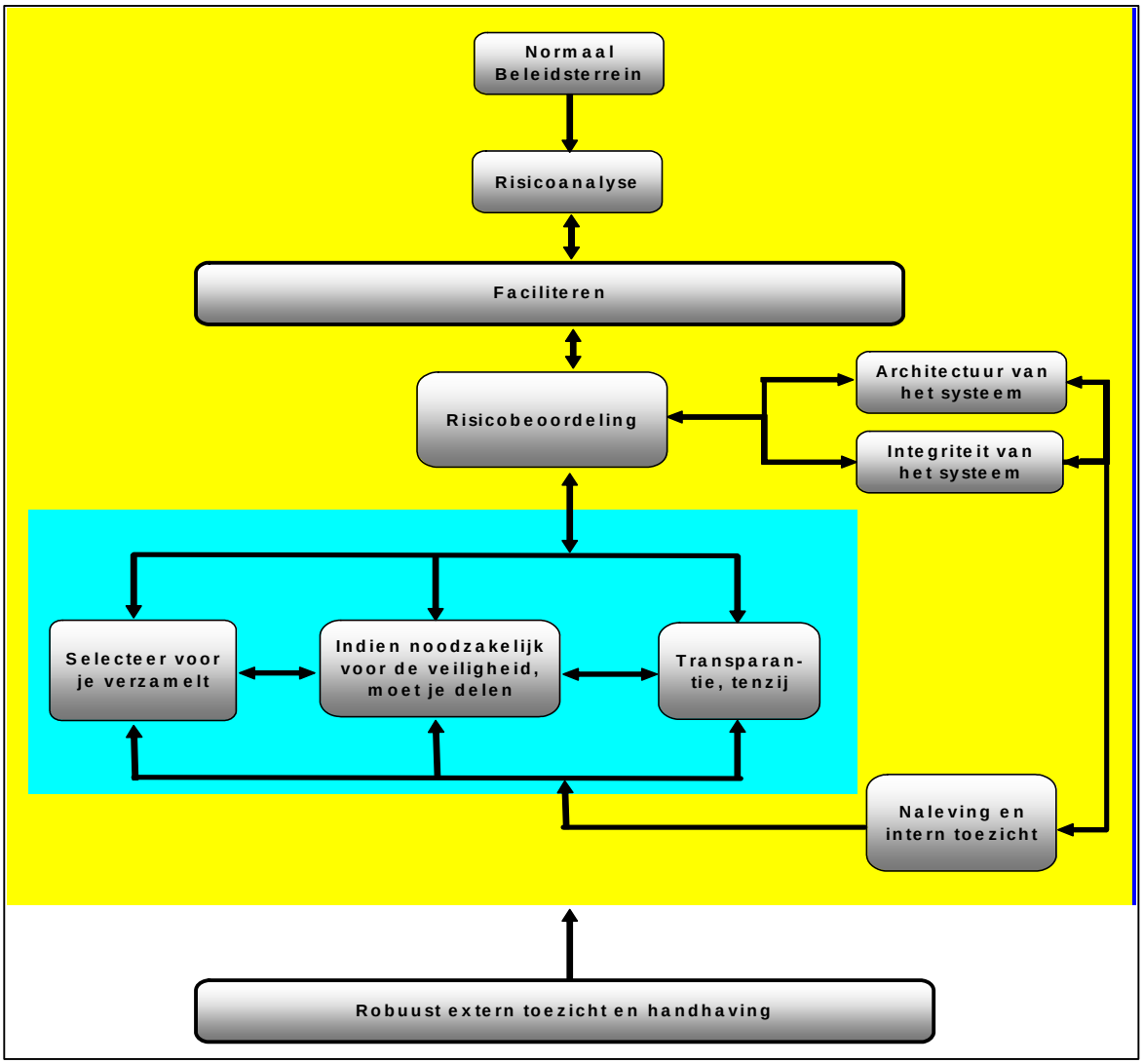
q. Waarborg dat de mensen die aan veiligheid werken steeds weten hoe zij met persoonsgegevens om moeten gaan.

r. Faciliteer de mensen die aan veiligheid werken in hun omgang met persoonsgegevens.

Grondslag 6: Zorg voor naleving en intern toezicht

s. Waarborg dat de mensen die aan veiligheid werken de regels naleven en zorg voor goed intern toezicht.

t. Overweeg een 'functionaris voor de gegevensverwerking' zoals genormeerd in de Wet bescherming persoonsgegevens aan te stellen



Het model in figuur 2 geeft een grafische weergave van de verhouding tussen de grondslagen. Het model vloeit voort uit de ambitie om het omgaan met persoonsgegevens op het gebied van veiligheid tot een ‘normaal’ beleidsterrein – zie paragraaf 3.4 – te transformeren, waarbij ook andere dan juridische overwegingen de passende aandacht moeten krijgen. De risicoanalyse vormt de kern van de balans tussen veiligheid en de persoonlijke levenssfeer en domineert het model. De afweging of verwerking van persoonsgegevens nodig is, start met de vraag welk veiligheidsrisico het werken met persoonsgegevens kan helpen wegnemen of beheersen. En tegelijk met de vraag welk risico het afzien van werken met persoonsgegevens tot gevolg heeft. Vervolgens is de vraag aan de orde met welke elementen het systeem gefaciliteerd kan worden. Architectuur en integriteit van het systeem moeten bijdragen aan wegnemen en beheersen van de gesignaleerde risico´s en aan de zorgvuldigheid van de

feitelijke omgang met persoonsgegevens. Vóór concrete persoonsgegevens worden verwerkt is steeds een risicobeoordeling nodig. De feitelijke omgang met persoonsgegevens speelt zich af binnen de lichtblauwe achtergrond van figuur 2 en komt tot uitdrukking in de grondslagen ´selecteer voor je verzamelt`, ´indien noodzakelijk voor de veiligheid, moet je delen' en ´transparantie tenzij'. De grondslagen zijn iteratief: na elke stap is het nodig opnieuw te kijken wat de gevolgen van die stap zijn voor de alle andere grondslagen resp. het stelsel als geheel.
Op het veiligheidsterrein is de overheid verantwoordelijk voor het functioneren van het stelsel. Verder heeft de overheid een stelselverantwoordelijkheid voor het faciliteren van voorlichting en advisering en is zij ten volle verantwoordelijk voor de uitoefening van robuust extern toezicht op de naleving van de wettelijke regels voor het omgaan met persoonsgegevens en de handhaving daarvan.

3.6. Handreikingen voor gegevensverwerking

Deze paragraaf geeft een toelichting bij de ´grondslagen´ en bijbehorende ´handreikingen´. Eerst komen de grondslagen voor gegevensverwerking als zodanig, daarna de grondslagen die zich richten op de organisatie. Daarbij komen de volgende vragen steeds terug:
- Wat houdt de grondslag in?
- Welk doel dient de grondslag?
- Wie is verantwoordelijk voor een juiste toepassing van de grondslag?
- Welke uitzonderingen zijn gerechtvaardigd?

3.6.1 Grondslagen voor de gegevensverwerking

Grondslag 1. 'Transparantie, tenzij'

a. Maak de burger duidelijk of verstrekking van zijn gegevens wettelijk verplicht is of niet. Maak de burger duidelijk om welke andere reden dan een wettelijke plicht zijn gegevens worden verwerkt.
b. Maak duidelijk met welk doel de persoonsgegevens worden verzameld en gebruikt zonder daarbij - mogelijk toekomstige - doelen te verzwijgen.
c. Bied inzicht in wat er met de gegevens gebeurt en zeg ook duidelijk aan wie de gegevens worden doorverstrekt.
d. Maak het de persoon om wie het gaat mogelijk en gemakkelijk de gegevens te controleren en te corrigeren en daar waar wettelijk toegestaan verzet aan te tekenen.

Doorgifte van passagiersgegevens aan Verenigde staten (PNR)

Het door luchtvaartmaatschappijen verstrekken van passagiersgegevens aan de Verenigde Staten werd pas duidelijk toen dit al enige tijd geschiedde. En tot op heden wordt het aan de luchtvaartmaatschappijen overgelaten om de passagiers hierover te informeren. Hoewel dit verstrekken een treffend voorbeeld is van gegevensverwerking die volledig van overheidswege (VS) verplicht gesteld wordt en waar overheden (VS en Europa) al enige jaren met elkaar over discussiëren, hebben die overheden er aan de burger nauwelijks uitleg aan of toelichting over gegeven. Het waarom en het hoe van de verstrekking van passagiersgegevens blijkt in de praktijk een zaak te zijn van de private partijen die aan deze herendienst onderworpen zijn. De grondslag van 'transparantie, tenzij' is een waarborg om de duidelijkheid vooraf te verschaffen.

Wat betekent ' transparantie, tenzij':

Transparantie betekent dat het in beginsel – zie hieronder het kopje 'uitzonderingen' – voor betrokkene duidelijk moet zijn wie zijn gegevens verzamelt, met welk doel zijn gegevens worden verzameld en wat er vervolgens met zijn gegevens gebeurt. Transparantie heeft dus betrekking op alles wat er met persoonsgegevens gebeurt, van verzamelen tot en met vernietigen. Transparantie kent twee aspecten. Een generiek aspect dat voorschrijft actief te communiceren over doelstelling, middelen, proportionaliteit, subsidiariteit etc. van een systeem voor het omgaan met persoonsgegevens. Juist op het moment van verzamelen immers is het nodig de burger te informeren over doel van verzameling en gebruik, zoals beoogd op het moment van verzamelen van gegevens.[15] Daarnaast kent transparantie een specifiek aspect dat voorschrijft degene wiens gegevens verwerkt worden actief te informeren over de doelstellingen van de verwerking, welke gegevens het betreft, met welke instanties voor welk doel wordt uitgewisseld en te wijzen op diens rechten en verplichtingen. Aan beide aspecten van deze grondslag moet zijn voldaan.

[15] Vgl. Rapport Gemeentelijke Ombudsman Amsterdam, Almere e.a. , 30 januari 2006, RA0611457. Deze oordeelde dat het onbehoorlijk was dat de Gemeentelijke Belastingdienst de incasso voor vorderingen van een semi-publiek gezondheidscentrum ter hand was gaan nemen, terwijl het instellingsbesluit voor de dienst dat uitdrukkelijk uitsloot en er geen waarborgen waren tot strikte scheiding van gegevens voor de incassotaak ten behoeve van anderen dan die van de Belastingsdienst zelf.

Het elektronisch kinddossier (EKD)

De toepassing van het EKD wordt een wettelijke verplichting. In die zin is de toepassing kenbaar en is het doel van het EKD duidelijk omschreven. Er is ook veel maatschappelijke en politieke discussie over. Maar het is wel de vraag of het voor iedereen ook duidelijk is welke gegevens zullen worden verzameld en uitgewisseld, aan wie de gegevens worden doorverstrekt en welke gevolgen dit uiteindelijk kan hebben. Het feit dat 'een ieder geacht wordt de wet te kennen' leidt nog niet tot daadwerkelijke transparantie voor de burger. De grondslag van transparantie is een waarborg dat ook bezien wordt of de beschikbare informatie wel informatief genoeg is, dat duidelijk wordt gemaakt dat het recht op inzage bestaat en dat ook daadwerkelijk de gelegenheid geboden wordt om inzage te krijgen in de vastgelegde gegevens.

Welk doel dient 'transparantie, tenzij':

Alleen als de omgang met gegevens transparant is, kan de persoon over wie de gegevens gaan, weten wat er bij wie over hem bekend is. Transparantie waarborgt ook dat gebruik kan worden gemaakt van eventueel inzage- en correctierecht. Verder kan transparantie bijdragen aan het voorkomen van in paragraaf 2.4 besproken ontwikkelingen als identiteitsfraude en "*the immutable me*". Het eveneens in paragraaf 2.4 besproken typeren van personen kan er toe leiden dat transparantie in de toekomst ook zal verplichten tot openheid over welke typeringen of categorieën van personen worden bijhouden en in welke categorieën betrokkene is ingedeeld. Het is immers niet alleen van belang om te weten wat de overheid, instanties en instellingen over iemand weten, maar ook hoe zij de persoon op grond van die gegevens zien en beoordelen.

Het elektronisch patiëntendossier (EPD)

Over het EPD hebben alle gezinnen in Nederland een brief ontvangen. Dat het EPD aanstaande is, is daardoor wel duidelijk geworden. In die zin is de brief een treffend voorbeeld van het informeren van burgers. Maar het is nog maar de vraag of de term 'patiëntendossier' niet verwarrend was of is. In de praktijk gaat het immers niet om één enkel dossier dat er van iedereen zal komen, maar gaat het veeleer om een infrastructuur om gegevensuitwisseling tussen de vele verschillende dossiers van de zorgverleners mogelijk te maken. Ook bood de brief geen zicht op welke gegevens dan vastgelegd worden of welke gegevens uitgewisseld worden. Als met al is voor velen niet (meer) duidelijk wat het EPD nu precies wel of niet is.

Wie is verantwoordelijk voor ' transparantie, tenzij':

De verantwoordelijkheid voor het realiseren van transparantie berust om te beginnen bij de instantie die de gegevens verzamelt. Wanneer deze dat in opdracht doet van een andere instantie die met de verzamelde gegevens gaat werken, ontslaat dat de verzamelende instantie

niet van haar verplichting om te handelen conform de grondslag ‘transparantie, tenzij’. Het steeds meer koppelen van bestanden zorgt er voor dat gegevens die onjuist worden ingevoerd in één systeem ook deel uitmaken van andere systemen. Voor betrokkene is het moeilijk te overzien dat zijn gegevens verkeerd zijn ingevoerd maar ook in welke andere bestanden bij andere verwerkers de onjuiste informatie terecht is gekomen. Per saldo ontstaat dan als het ware een omkering van de bewijslast waarbij betrokkene steeds bij elke verwerker opnieuw moet aantonen dat de over hem opgenomen gegevens niet juist zijn. Daarom is van het belang dat elke instantie die met persoonsgegevens aan de slag gaat transparantie in acht neemt.

Ook werkgevers googelen

Ongeveer een kwart van de Nederlandse werkgevers zoekt op sociale netwerksites zoals Hyves naar informatie over sollicitanten. In bepaalde gevallen is de inhoud van die sites reden om de sollicitant niet aan te nemen. In andere gevallen kan een sollicitant met een sterke Hyves-site ook voordeel hebben bij zijn Hyves. Maar waarschijnlijk weten lang niet alle sollicitanten dat ook de werkgever googelt.

Zeker de overheid moet transparantie verwerkelijken. In de specifieke context van werken aan de veiligheid lopen belangen van burgers, bedrijven en overheid rond transparantie niet steeds parallel. De burger zal vaak meer informatie willen wat er met zijn gegevens gebeurt, terwijl de overheid die burger en zichzelf soms weinig tijd gunt voor informeren in de haast om een veiligheidsdreiging het hoofd te bieden. Echter, op langere termijn zal de overheid er wel degelijk baat bij hebben de burger zo goed mogelijk te informeren en transparantie als leidraad te nemen. In acht nemen van transparantie vergroot de kans dat foutieve gegevens gecorrigeerd worden. Draagt ook bij aan het vertrouwen van burgers in de overheid. Actief informeren is bovendien veel efficiënter dan steeds moeten reageren op al dan niet terechte klachten van wantrouwende burgers. Dat vertrouwen is bovendien ook weer nodig om goed aan veiligheid te kunnen werken.

Vooral met het oog op de in hoofdstuk 2 geschetste ontwikkelingen is er geen gerede aanleiding de publieke sector uit te sluiten van de grondslag van transparantie.

Registratie van (risico)jongeren

Bij meldingen over (risico)jongeren die in een verwijsindex worden opgenomen is in de praktijk vaak sprake van het actief informeren van betrokkenen. Het project Stedelijk Instrument Sluitende Aanpak (SISA) in Rotterdam is daar een treffend voorbeeld van. Iedere jongere waarvan een (eerste) melding wordt vastgelegd, krijgt daarover bericht.

Transparantie en het informeren kan bij specifiek beleid gericht op risicojongeren overigens ook contraproductief zijn. De risicojongere of zijn ouders die te horen krijgen dat er over hen meldingen zijn binnengekomen, zullen misschien minder snel geneigd zijn om hulpverleners of politieagenten in vertrouwen te nemen. In dat geval kan er sprake zijn van een situatie van *'transparantie, tenzij'*.

Uitzonderingen:

Het uitgangspunt is dat 'transparantie' moet worden betracht, maar de toevoeging 'tenzij' biedt ruimte voor uitzonderingen. Een zeer beperkte ruimte, die eigenlijk alleen benut kan worden in evidente situaties: bij voorbeeld bij het werk van inlichtingen- en veiligheidsdiensten of in het kader van een strafrechtelijk onderzoek. En ook zou het onwerkbaar worden wanneer nooit een beleidsverandering doorgevoerd zou kunnen worden zonder toestemming van alle mensen van wie persoonsgegevens verzameld zijn. Nieuwe, gezaghebbende, conclusies van wetenschappelijk onderzoek moeten in sommige gevallen toch echt op bestaande persoonsgegevens kunnen worden toegepast zonder de instemming van alle verstrekkers van die gegevens. Aan de andere kant vraagt een wijziging, naarmate deze ingrijpender gevolgen heeft, een des te steviger rechtvaardiging voor het maken van een uitzondering op de plicht tot transparantie.

Grondslag 2. 'Selecteer voor je verzamelt'[16] en houd het sober ('*select before you collect*')

e. Verzamel alleen persoonsgegevens met een rechtmatig doel, rekenschap gevend van de belangen van proportionaliteit en subsidiariteit.[17]

f. Stel voorafgaand aan de verzameling een concrete risicoanalyse op en maak daarin duidelijk wat met het oog op de voorgestelde aanpak de rol van de verzamelde persoonsgegevens is.

g. Verzamel niet meer persoonsgegevens dan je op basis van de vooraf op te stellen risicoanalyse nodig hebt en zult gebruiken.

[16] B. Jacobs, Select before you Collect, Ars Aequi, jaargang 54, dec. 2005, p. 1006 -1009.

[17] Dat wil zeggen: zet het lichtste middel in om je doel te bereiken en zorg er voor dat het middel in een passende relatie tot het beoogde doel staat.

h. Scherm persoonsgebondenheid zo veel mogelijk af.

i. Bewaar gegevens niet langer dan nodig en zorg voor vernietiging daarna (‘horizon’).

j. Gebruik persoonsgegevens alleen voor het wettelijk geregelde doel of – bij vrijwillige verstrekking – het doel waarvoor toestemming is verleend of wanneer sprake is van een vitaal belang van betrokkene (doelbinding).

De Baby-kipppi (Kort Instrument voor Psychologische en Pedagogische Probleem Inventarisatie)
De baby-kipppi is een lijst die door consultatiebureaus gebruikt wordt om informatie over de baby en de ouders te verzamelen als de baby ongeveer één jaar oud is. In de lijst zijn gestandaardiseerde vragen opgenomen die variëren van de eetlust van de baby tot de eventuele geestelijk malaise van de ouders als gevolg van de geboorte. Daarbij wordt men uitgenodigd om uitgebreid verhaal te doen van ingrijpende gebeurtenissen, zoals overlijden van een familielid, problemen met een ander kind, psychische problemen van de ouders of conflicten en ruzies binnen en buiten het gezin. En of men dan ook aan wil geven of die gebeurtenissen als niet zorgelijk of juist als ernstig zorgelijk ervaren zijn. Er lijkt bij het formulier een tendens te zijn om de (volledige) lijst van gestandaardiseerde vragen dan ook maar meteen als de standaard vragenlijst te gebruiken. Het is niet eenvoudig de baby-kipppi te zien als een vragenlijst die zich beperkt tot de noodzakelijke gegevens en waarbij soberheid van informatieverzameling voorop staat.

Wat betekent ‘selecteer voor je verzamelt’:

Selecteer voor je verzamelt betekent dat niet méér persoonsgegevens mogen worden verzameld dan echt nodig en dat ook overigens zo sober mogelijk moet worden omgegaan met persoonsgegevens. Deze selectie moet worden gebaseerd op de uitkomsten van een risicoanalyse. In hoeverre zijn de gegevens die zijn geselecteerd noodzakelijk voor de veiligheid? En is daarbij voldaan aan de beginselen van proportionaliteit en subsidiariteit? Met andere woorden, is het nodig om persoonsgegevens te verzamelen of kan de veiligheid in de voorliggende situatie ook op een andere, minder ingrijpende, manier worden gewaarborgd? Is het nodig gegevens van iedereen te verzamelen of kan worden volstaan met een bepaalde groep? De grondslag “selecteer voor je verzamelt” omvat mede de eis van doelbinding uit artikel 7 van de Wbp en het verbod van bovenmatige verwerking van artikel 11 van de Wbp. Dat betekent goed nadenken over het doel van gegevensverzameling, goed nadenken over het type gegeven dat nodig is en goed nadenken of het doel met verzameling van persoonsgegevens bereikt kan worden. En steeds nadenken of met verzamelen doorgegaan moet worden gelet op de aard van de veiligheidsbedreiging. De verzamelaar moet de gegevens ook feitelijk gebruiken. ‘*Nice to know’* is niet genoeg, ‘*need to know*’ is een minimumvoorwaarde. Het is van belang te onderkennen dat een ‘doel’ van tijdelijke aard kan zijn. Soms valt de noodzaak voor het eerder gekozen doel weg: een bedreigende situatie kan zich zo lang niet hebben voorgedaan dat er geen noodzaak meer is tot gegevensverzameling met het oog daarop. Een horizonbepaling in wettelijke regelingen en

uitvoeringsbepalingen dient naar de mening van de Commissie serieus te worden overwogen. ‘Niet gebruiken’ verplicht – met uitzondering van de situaties waarin de wet een bewaarverplichting kent – tot vernietiging van de gegevens. Immers, hoe minder gegevens, des te minder zal de integriteit van systemen – zie hieronder grondslag 4 – op de proef worden gesteld. De Commissie beoogt hiermee invulling te geven aan de open formulering van artikel 8, onderdelen e. en f. van de Wbp. Op grond daarvan mag gegevensverwerking plaatsvinden in het geval deze “noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt respectievelijk wanneer deze noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het recht op de persoonlijke levenssfeer prevaleert.”

Tanken zonder te betalen

De toepassing van deze grondslag *‘Selecteer voor je verzamelt’* zal in de praktijk geen sinecure zijn. De discussie over de noodzaak om gegevens vast te leggen is soms een lastige discussie waarbij zelfs tegenovergestelde keuzes mogelijk blijken. Een voorbeeld is het ‘tanken zonder te betalen’. In Nederland hebben pompstations via een intermediair (deurwaarders) indirect toegang gekregen tot informatie uit het kentekenregister om zo hun schade te kunnen verhalen op automobilisten die na het tanken wegrijden zonder te betalen. Een slagboom of eerst betalen en dan pas kunnen tanken of wegrijden (zoals in Luxemburg of Frankrijk) zou ook hebben gekund.

Welk doel dient ‘selecteer voor je verzamelt’:

´Handig voor later’ is een te magere rechtvaardiging voor het verzamelen van gegevens. Voor verzameling van persoonsgegeven dient een op basis van een risicoanalyse onderbouwde noodzaak te bestaan, ook in het veiligheidsdomein. Door te waarborgen dat er niet meer gegevens worden verzameld dan noodzakelijk wordt voorkomen dat een onevenredige inmenging in de persoonlijke levenssfeer van betrokkene plaatsvindt. Ook zorgt de grondslag ‘selecteer voor je verzamelt’ er voor dat de gegevens die wél noodzakelijk zijn niet als een speld in een hooiberg verdwijnen. Ook de efficiency is gebaat bij een zorgvuldige selectie. Zo versterkt deze grondslag niet alleen de persoonlijke levenssfeer maar ook de veiligheid.

Doorgifte van passagiersgegevens (PNR)

Een blik op de lijst van gegevens die luchtvaartmaatschappijen dienen te verstrekken aan overheden, bijvoorbeeld of een passagier een halalmaaltijd wenst of alle betalingsinformatie betreffende het ticket, zal bij de lezer van die lijst niet snel tot de conclusie leiden dat er sprake is van strenge selectie en soberheid bij het verzamelen van gegevens.
Maar wellicht staan selectie of soberheid ook niet voorop. The Electronic System for Travel Authorization van the U.S. Department of homeland Security geeft bij bezoeken van de site automatisch de voorwaarden weer. Voor wat privacy betreft gaat het dan om de mededeling: “There is no expectation of privacy when you use this computer system”.

Wie is verantwoordelijk voor ‘selecteer voor je verzamelt’:

De verantwoordelijke instantie of instelling moet kunnen verantwoorden waarom risicoanalyse heeft uitgewezen dat het nodig is deze gegevens te verzamelen.

Ongebruikelijke transacties

Financiële instellingen en beroepsbeoefenaren zoals notarissen en accountants zijn wettelijk verplicht zogenaamde ongebruikelijke transacties aan de overheid te melden. Welke transacties gemeld moeten worden hangt dan af van objectieve (de hoeveelheid geld die contant gestort of betaald wordt) en subjectieve (de omstandigheden van de financiële transacties) criteria. Deze meldingen worden vervolgens verder onderzocht waarbij bezien wordt of de ongebruikelijke transactie ook aan te merken valt als een verdachte transactie. Enkel de verdachte transacties van voldoende zwaarte worden vervolgens aan de politie gemeld voor strafrechtelijk onderzoek.
Het melden en beoordelen van ongebruikelijke transacties is een voorbeeld waarbij wetgeving voorziet in een selectiemechanisme.

Uitzonderingen:

Selecteer voor je verzamelt kan soms ook betekenen dat juist álle beschikbare gegevens moeten worden verzameld. Bij bijvoorbeeld een zeer ernstig misdrijf met grote kans op recidive kan het proportioneel zijn alles in het werk te stellen na te gaan wie zich op het moment van dat misdrijf bevonden in het gebied waar het gepleegd werd. Ook kan het soms nodig zijn gegevens te verzamelen voordat een selectie kan plaatsvinden. Uitzonderingen op de grondslag “selecteer voor je verzamelt” zijn dus mogelijk, maar ook in dat geval geldt dat gegevens moeten worden vernietigd zodra blijkt dat ze niet meer nodig zijn.

De slimme meter

In het kader van de zorg voor het milieu en als middel voor energiebesparing komt er de zogenaamde 'slimme' meter voor het energieverbruik. Deze meter geeft periodiek en automatisch de meterstanden door aan de energieleverancier. Het gebruik van een 'slimme' meter zal verplicht zijn. Bij de perioden waarover automatisch gegevens worden doorgegeven gaat het om kwartier/uurwaarden die aan netbeheerders doorgegeven worden en om dagwaarden die aan netbeheerders en aan leveranciers doorgegeven worden. Men kan zich afvragen of er bij deze korte perioden wel sprake is van voldoende 'soberheid' bij het selecteren en verzamelen van gegevens. Bij het doorgeven van kwartierwaarden wordt het energieverbuik van gezinnen toch al snel bijna 100 maal per dag doorgegeven.

Grondslag 3. 'Indien noodzakelijk voor de veiligheid, moet je delen'

k. Persoonsgegevens moet je delen als uit een risicobeoordeling blijkt dat delen noodzakelijk is voor de veiligheid.

l. Wanneer de noodzaak van delen voor de veiligheid niet vaststaat:

- deel persoonsgegevens in geval van vrijwillige verstrekking alleen wanneer de verstrekker daar uitdrukkelijk toestemming voor geeft en de gevolgen van die toestemming kan overzien;
- deel in geval van wettelijk verstrekte persoonsgegevens deze alleen met anderen als de wet het toelaat.

De peuter of de ouder?

De behandelende psycholoog die een ouder behandelt en daarbij kennis heeft van (vermoedelijke) kindermishandeling (fysiek geweld), maar die toch geen signaal afgeeft (eventueel via een intermediair) aan de peuterspeelzaal waar het kind verblijft om alert te zijn op mogelijke mishandeling, is een voorbeeld dat zicht biedt op het dilemma of de bescherming van iemands privacy (de ouder) een reden kan zijn om iets niet te doen als de veiligheid van een kind in gevaar is. Dat de veiligheid van jonge kinderen prevaleert boven de belangen die ouders of verzorgers kunnen hebben en prevaleert boven het beroepsgeheim is een standpunt dat past bij het delen van gegevens als dit voor de veiligheid van jonge kinderen ook echt noodzakelijk is.

Wat betekent ' indien noodzakelijk voor de veiligheid, moet je delen':

'Indien noodzakelijk voor de veiligheid, moet je delen' betekent dat, als aan de gestelde randvoorwaarden is voldaan, delen niet meer ter discussie kan staan. Onbekendheid met privacywetgeving en, als gevolg daarvan, angst om privacyregels te schenden zorgen er soms voor dat gegevens ten onrechte niet worden gedeeld. Ook worden privacyregels soms als excuus gebruikt om niet te hoeven delen. Dat is niet terecht, privacywetgeving geeft weliswaar *randvoorwaarden* voor de omgang met gegevens maar staat zeker niet in de weg

aan het delen van gegevens als dat noodzakelijk is voor de veiligheid. Die randvoorwaarden zijn van groot belang. Uit onder meer artikel 8 EVRM vloeit voort dat de *noodzaak* van het verstrekken van gegevens voor de veiligheid vast moet staan. Ook moet zijn voldaan aan de beginselen van *proportionaliteit en subsidiariteit*. Daarom moet aan toepassing van de derde grondslag altijd een *risicobeoordeling* vooraf gaan. Proportionaliteit vereist ook dat goed wordt gekeken naar *met wie* wordt gedeeld. Daarvoor is het belangrijk dat er aandacht is voor het specifieke domein waarbinnen de gegevensverstrekking plaatsvindt. De verplichting om gegevens te delen met degenen die aan veiligheid kunnen bijdragen is niet eenvoudig in algemene zin - en dus met álgemene regels – af te grenzen. De risicobeoordeling moet uitwijzen óf gegevens gedeeld moeten worden en met wíe gegevens gedeeld moeten worden. Het moet duidelijk zijn op basis van welke criteria de beoordeling plaatsvindt of sprake is van een bedreiging van de veiligheid en met wie in dat kader moet worden gedeeld. En op basis van welke criteria beoordeeld wordt of het 'delen' van gegevens bijdraagt aan de veiligheid in het specifieke geval. Een duidelijke afbakening van het domein waarbinnen 'delen indien noodzakelijk voor de veiligheid' is daarbij essentieel. Ter toelichting, dat houdt in dat nagegaan wordt welk doel de verschillende 'professionals', organisaties en instellingen nastreven. Binnen het domein van de jeugdzorg is dat doel onder meer het waarborgen van de veiligheid van kinderen en jongeren. Delen van gegevens met een andere 'professional' die binnen dat domein werkt en dus datzelfde doel nastreeft is eerder gerechtvaardigd dan het delen van gegevens met een 'professional' die een ander doel nastreeft, zoals een verzekeringsmaatschappij of een werkgever. Degene die voor verwerking van gegevens verantwoordelijk is heeft de plicht deze criteria voor 'indien noodzakelijk voor de veiligheid, moet je delen' vooraf te formuleren. In de praktijk moet dit betekenen dat de organisatie waarvoor de 'professional' werkt of de beroepsgroep waar de 'professional' deel van uitmaakt de risicobeoordeling faciliteert. Dat kan door vaak voorkomende situaties op een handzame manier voor de 'professional' te beschrijven en voor gevallen van twijfel een tweedelijnsvoorziening in het leven te roepen. In de eerste plaats binnen de eigen organisatie. Maar ook verdient het soms overweging buiten de organisatie een vertrouwenspersoon voor de beroepsgroep aan te stellen. De Commissie adviseert het kabinet te bevorderen dat de 'professionals' die aan veiligheid werken zich kunnen wenden tot een externe vertrouwenspersoon voor hun beroepsgroep: een gezaghebbende persoon die fungeert als vraagbaak en klankbord met wie zij twijfels kunnen bespreken over hun risicobeoordeling of over de noodzaak persoonsgegevens te delen. Zoals de Deken van de Orde van Advocaten

deze functie voor advocaten vervult. Bij die vertrouwenspersoon zou de ‘professional’ zijn twijfels vertrouwelijk kunnen voorleggen en om advies kunnen vragen.
Ook gaat het er om dat de ‘professional’ voldoende rugdekking voelt van zijn organisatie. Scherp zijn op wat wel en niet met anderen gedeeld moet worden en zorgvuldig met persoonsgegevens omgaan lukt alleen door voldoende zelfbewuste en competente ‘professionals’ die zich door hun organisatie gesteund voelen en gefaciliteerd weten. “Indien noodzakelijk voor de veiligheid, moet je delen” kan overigens worden toegepast in twee te onderscheiden categorieën van verstrekkingen: verstrekking van gegevens in concrete gevallen en verstrekking door middel van het koppelen van bestanden. Zowel de verstrekking in een concreet geval als de koppeling van bestanden is een verwerking in de zin van de Wbp. Bij beide categorieën moet zijn voldaan aan de eerder beschreven randvoorwaarden. Een concrete invulling van het beginsel van proportionaliteit bij het koppelen van bestanden kan overigens zijn dat niet wordt overgegaan tot koppeling van bestanden met concrete gegevens maar slechts tot koppeling van bestanden met verwijsgegevens. De verwijsgegevens geven aan wie er allemaal beschikken over gegevens over een bepaalde persoon maar niet wat die gegevens inhouden. Wanneer naar aanleiding van het bestand met verwijsgegevens inhoudelijke gegevens nodig blijken te zijn moet opnieuw worden getoetst aan noodzakelijkheid, proportionaliteit en subsidiariteit. Ook hierbij geldt dat een positieve toets aan de randvoorwaarden ertoe leidt dat gegevens moeten worden gedeeld.

Veiligheidshuis

Een treffend voorbeeld van samenwerking en het delen van informatie zijn de zogenaamde veiligheidshuizen. In een veiligheidshuis werken gemeenten, jeugd- en zorginstellingen, politie en justitie samen bij de aanpak van criminaliteit en overlast. Niet de dossiers, maar de persoon of een gebied staan daarbij centraal. Waarom gaat iemand opnieuw in de fout? Wat is er nodig om dat te voorkomen? Hoe vergroten we de veiligheid in deze buurt? Allemaal vragen die in het veiligheidshuis behandeld worden en waarvoor delen van informatie noodzakelijk is. De verantwoordelijkheid voor de verstrekking van persoonsgegevens is daar uitdrukkelijk belegd.

Welk doel dient ‘indien noodzakelijk voor de veiligheid, moet je delen’:
‘Indien noodzakelijk voor de veiligheid, moet je delen’ beoogt ervoor te zorgen dat privacyregels niet onnodig de veiligheid belemmeren. Door duidelijk te maken dat - als aan de noodzakelijke randvoorwaarden is voldaan – gegevens *moeten* worden gedeeld kunnen instellingen en instanties die niet willen delen zich niet langer achter privacywetgeving verschuilen. De commissie geeft in overweging dit ‘indien noodzakelijk voor de veiligheid, moet je delen’ in artikel 9 van de Wbp te expliciteren. Dat verwerking van persoonsgegevens

achterwege moet blijven voor zover een geheimhoudingsplicht uit hoofde van beroep of wettelijk voorschrift aan delen van gegevens in de weg zou staan, zoals onderdeel d. van artikel 9 van de Wbp formuleert, kan niet betekenen dat – bijvoorbeeld – een psychiater die kennis neemt van levensbedreigende omstandigheden van of in de kring rond zijn cliënt deze kennis onder zich houdt. De Commissie beoogt daarbij uitdrukkelijk niet het beroepsgeheim uit te hollen. Het moet gaan om concrete verstrekkingen waaraan altijd een risicobeoordeling vooraf is gegaan. De hulpverlener moet zich afvragen of het delen nodig is, of de veiligheid van betrokkene door het delen versterkt wordt en of delen proportioneel is. En ook of het delen voldoet aan het subsidiariteitsbeginsel en welke overige risico´s er zijn.

Delen voor een veilig plein

Het delen van camerafaciliteiten of het delen van camerabeelden zal voor een goede veiligheid in de openbare ruimte noodzakelijk kunnen zijn op plaatsen waar cameratoezicht door de overheid (het openbare plein) naadloos en ongemerkt overgaat in camerabewaking door de private sector (het aangrenzende treinstation of het winkelcentrum). Alleen het delen van de camera-informatie maakt het mogelijk om voor het gehele aaneensluitende gebied van plein, station en winkelpassage zorg te dragen voor een adequate beveiliging met adequaat toezicht.

Wie is verantwoordelijk voor ' indien noodzakelijk voor de veiligheid, moet je delen':
Vooraf moet vast komen te staan wie er verantwoordelijk is voor de gegevens en daarmee ook voor het delen van de gegevens. Eindverantwoordelijkheid berust altijd bij de leiding van de organisatie waar de 'professional' werkt. Deze moet een verantwoordelijke aanwijzen, deze functionaris faciliteren en er op toezien dat deze zijn verantwoordelijkheid ook draagt. Wanneer delen plaatsvindt door een koppeling van bestanden of het werken in een samenwerkingsverband, zoals in een veiligheidshuis moet duidelijk zijn wie de eindverantwoordelijkheid heeft.

Het hoeft niet allemaal tegelijk

Het delen van informatie behoeft niet altijd allemaal tegelijk. De inrichting van een verwijsindex 'sec' is een goed en sober middel om meldingen vast te leggen en om samenwerkende instanties de mogelijkheid te geven om te zien of ook een andere instantie een melding gedaan heeft over dezelfde persoon. Bij zo'n verwijsindex 'sec' wordt weinig of geen feitelijke informatie vastgelegd: het is eerder een "piepsysteem" waarbij vastgelegd wordt dat er meldingen zijn en dat iemand bij een bepaalde instantie bekend is.

Uitzonderingen:

De uitzonderingen zijn al ingebed in (de randvoorwaarden van) de grondslag zelf. “Moeten delen” kan alleen na een voorafgaande risicobeoordeling en een toets aan de beginselen van proportionaliteit en subsidiariteit.

De handreikingen bij de derde grondslag maken verder uitdrukkelijk onderscheid tussen situaties waarin sprake is van noodzakelijk in het kader van de veiligheid en situaties waarin hiervan geen sprake is. In dat laatste geval kan geen sprake zijn van *moeten* delen. Wel kan er – weer na een risicobeoordeling en een toets aan de beginselen van proportionaliteit – sprake zijn van *mogen* delen.

Betrek een derde partij

Het inschakelen van een intermediair bij de uitwisseling van gegevens is een middel om de uitwisseling te stroomlijnen en om de uitwisseling beperkt te houden of juist uit te breiden tot dat wat noodzakelijk is. Bij gebruik van een intermediair stellen alle vragende partijen hun vraag aan één instantie. Die instantie zoekt het antwoord of de informatie op in de eigen database of in de databases van de andere partijen en geeft het relevante antwoord aan de vragende partij. Een dergelijk intermediair is ook nuttig in het kader van conflictvermindering. Alle deelnemende en uitwisselende organisatie behoeven immers enkel te overleggen met die (objectieve) intermediaire organisatie. Ze hoeven dan niet iedere keer met “elkaar in de slag” en allerlei discussie over “wat wel en wat niet noodzakelijk is” hoeven niet gevoerd te worden binnen het geheel van al die samenwerkende partijen. Het intermediair kan als een aan de hand van vooraf gemaakte afspraken de gegevensuitwisseling verzorgen en als een soort scheidsrechter optreden bij discussies.

3.6.2 Grondslagen voor de organisatie

Grondslag 4. Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers

m. Zorg steeds voor correcte, actuele en volledige gegevens uit oogpunt van bron- en gebruikscontext.

n. Zorg voor veilige systemen.

o. Zorg dat de systemen voor de gegevensverwerking precies zijn toegerust op de doelen van verwerking.

p. Zorg voor integere omgang van de ‘professionals’ met de systemen.

Gegevens en hun betekenis / Kijk maar: "er staat niet wat er staat"

De betekenis en de impact van gegevens in de praktijk hangt vaak af van de context van die gegevens. Zo is het een heel verschil of de vermelding dat er sprake is van de stoornis "schizofrenie" afkomstig is uit de rapportage van een arts of alleen ontleend is aan mededelingen van familieleden. Het opnemen van een indicatie over de bron van gegevens of over de betrouwbaarheid ervan is een mogelijkheid om verkeerde of ongelukkige interpretatie van gegevens tegen te gaan.

Wat betekent de 'zorg voor integriteit van gegevens, systemen en het handelen van gebruikers':

Elke instantie die met persoonsgegevens omgaat heeft een zorgplicht voor het werken met de juiste gegevens. Gegevens moeten juist, actueel en volledig zijn. De gebruikscontext moet gekoppeld zijn aan de broncontext, de context waarin de gegevens zijn verzameld. Deze plicht voort onder meer voort uit artikel 11 van de Wbp. Daarbij moet onderscheid worden gemaakt naar de integriteit van de systemen waarin de gegevens worden opgeslagen, de juistheid van de gegevens zelf en de integriteit van omgang ermee door de personen die met de gegevens en systemen werken. Een belangrijke manier om goede omgang met persoonsgegevens op de werkvloer van de veiligheid te bevorderen is gelegen in het maken en goed gebruiken van de passende technische voorzieningen. Veiligheid van het systeem staat daarbij voorop. Technische voorziening moeten zo goed mogelijk worden beveiligd tegen inbrekers, hackers en het lekken van informatie. Daarnaast moeten systemen goed worden toegerust op de doelen van verwerking. "*Privacy by design*" en "*privacy enhancing technologies*" verdienen actievere aandacht. Het is essentieel al bij het formuleren van de opdracht tot het ontwerpen van applicaties en infrastructuren rekening te houden met privacyrisico's en daar bij het feitelijke ontwerpen steeds aandacht aan te geven. De architectuur van de techniek bepaalt wat het systeem nu kan maar ook wat de toekomstige mogelijkheden zullen zijn.[18] Privacyoverwegingen kunnen een prima plaats krijgen in de ontwikkeling van technologie. Multidisciplinaire samenwerking – al vanaf de beginfase – tussen ICT´ers en juristen is daarvoor essentieel, maar helaas nog bepaald niet vanzelfsprekend. De praktijk geeft vaak blijk van belemmeringen: ander jargon, andere perceptie van de problemen, verschillende doelen, nog geen precies inzicht in wat het systeem zou moeten kunnen en wat de opdrachtgever precies wil, ontijdige betrokkenheid. De juistheid van de gegevens kan deels worden gewaarborgd door een integer systeem. Burger en instanties hebben een vrijwel parallel belang bij de juistheid van gegevens.

[18] J.R. Roepman, *Revocable privacy*, in: Privacy & Informatie, 2008 afl. 3, p. 114-118.

Belangrijk is echter ook dat betrokkene zelf zoveel mogelijk de juistheid van zijn gegevens kan controleren. Daarom is transparantie zoals beschreven onder grondslag 1 van wezenlijk belang. Maar integere systemen en gegevens hebben geen betekenis zonder integer gebruik. Incidenten met verloren *memorysticks* en zoekgeraakte cd-roms spreken daarbij voor zich.

Beveiliging en de menselijke factor

Beveiliging van gegevens wordt nog te vaak als een zaak van vooral 'de techniek' gezien. Zo laten de recente onderzoeksrapporten van het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg over de beveiliging van gegevens in ziekenhuizen zien dat er op het gebied van instructie, opleiding en bewustwording van medewerkers nog veel te verbeteren valt.

De aandacht die een journalist van TV-West in november 2008 trok toen hij op vrij eenvoudige medische gegevens van diverse ziekenhuizen gefaxt kon krijgen werpt eveneens een blik op de menselijke factor. Hetzelfde geldt voor het verlies van vele bankgegevens (creditcard betalingen) van de Landesbank Berlin in december 2008 toen een pakket met microfiches niet bij de bank, maar bij een dagblad werd afgeleverd. Ook het gebruik van de 'ouderwetse' microfiches daarbij wekte bevreemding bij Duitse privacytoezichthouders: waarom was geen databestand met encryptie gebruikt vroegen zij zich af.

Welk doel dient de 'zorg voor integriteit van gegevens, systemen en het handelen van gebruikers':

Integriteit van systemen, gegevens en de gebruikers van de systemen zorgt ervoor dat zoveel mogelijk wordt gewaarborgd dat gegevens correct zijn en goed beveiligd worden. Zo kan worden voorkomen dat gegevens verder worden verstrekt dan nodig is maar ook dat ontwikkelingen als omschreven in paragraaf 2.4. (identiteitsfraude, "*immutable me*") zoveel mogelijk worden voorkomen.

Nieuwsgierig?

Tegen het onjuist gebruik van gegevens en tegen het raadplegen van gegevens uit nieuwsgierigheid kan logging (vastleggen) van het raadplegen en daadwerkelijke controle van die log-gegevens als middel ingezet worden. De brief die het Rotterdamse politiekorps aan enkele honderden agenten zond met de vraag waarom zij nu allemaal (tevergeefs) geprobeerd hadden het dossier van een gearresteerde voetballer te bekijken is een treffend voorbeeld. Hetzelfde geldt voor het loggen en controleren welke patiëntgegevens door plaatsvervangende artsen bij avond- en weekenddienst opgevraagd zijn.

Wie is verantwoordelijk voor de 'zorg voor integriteit van gegevens, systemen en het handelen van gebruikers':

De organisaties die met persoonsgegevens ten behoeve van de veiligheid werken zijn

verantwoordelijk voor correcte, actuele en volledige gegevens waarvan het gebruik is beperkt door de context waarin de gegevens zijn verzameld. Opdrachtgevers voor de bouw van systemen zijn verantwoordelijk voor integere systemen. Dat laat onverlet dat de opdrachtnemers enorm aan de integriteit van systemen kunnen bijdragen, bijvoorbeeld door er zorg voor te dragen dat ICT-toepassingen correcties in de gegevens gemakkelijk verwerken. Ook kan handig gebruik van ICT veroudering van gegevens het hoofd bieden: vaak is het mogelijk vooraf te bepalen hoe lang gegevens actueel zijn en dus ook het vernietigen van de gegevens na dat tijdstip in de systemen in te bouwen. Integriteit betekent ook het waarborgen van de veiligheid van de systemen. De kans op slordigheden kan ook met behulp van ICT worden beperkt. En ICT moet 'hackers' zo veel mogelijk buiten de deur houden. Daarvoor is het noodzakelijk dat de opdrachtgevers beschikken over de kennis om integriteit en een goede architectuur van systemen te waarborgen. Ook de overheid moet beschikken over de daartoe benodigde deskundigheid. Er zijn te veel aanwijzingen – ook de Commissie kwam het bij herhaling tegen – dat het aan die deskundigheid nog ontbreekt. Juist omdat goede samenwerking niet vanzelf van de grond komt, ligt het voor de hand dat de overheid nagaat hoe zij deze samenwerking kan faciliteren. Daarin past het te waken voor te hoge ambities en vooral veel aandacht te geven aan de transparantie. Uiteindelijk blijft de instantie of de organisatie die het systeem beheert verantwoordelijk voor de integriteit van haar systemen en medewerkers.

Uw unieke persoonlijke inlogcode

Als u met uw persoonlijke code op de klantensite van een bedrijf inlogt, worden uw gegevens vaak al automatisch ingevuld. Dat is handig, want dan hoeft u dat niet steeds zelf te doen. Maar soms gaat het automatisch invullen niet helemaal goed. Begin december 2008 waren korte tijd de gegevens van bijna 1 miljoen abonnees van Veronica Magazine op de site van de Lotto te vinden. De abonnees hadden een brief met een unieke en persoonlijke inlogcode van de Lotto gekregen. Bij het inloggen met die code werden de adresgegevens dan automatisch ingevuld. Maar door de ontvangen inlogcode een beetje te wijzigen konden de automatisch ingevulde adresgegevens van andere abonnees ook te voorschijn getoverd worden.

Uitzonderingen:

Integriteit van gegevens, systemen en het handelen van gebruikers moet altijd zoveel mogelijk worden gewaarborgd. Uitzonderingen op dat uitgangspunt zouden niet mogelijk moeten zijn. Dat is overigens iets anders dan de ogen te sluiten voor de realiteit. De realiteit is dat waar mensen werken ook fouten worden gemaakt. Integriteit zoals bedoeld met deze grondslag impliceert passende aandacht voor vergroten van de kans dat fouten gesignaleerd

worden en de mogelijkheid fouten te herstellen. Daarbij helpt het de betrokkene zo gemakkelijk mogelijk te maken op fouten te wijzen. Bijvoorbeeld door correctie op één plaats (‘*one-shop-stop*’) voldoende te laten zijn voor alle andere systemen waar de (afgeleide) foute informatie in is opgenomen.

Grondslag 5: Zorg voor voorlichting en faciliteiten

q. Waarborg dat de mensen die aan veiligheid werken steeds weten hoe zij met persoonsgegevens om moeten gaan.

r. Faciliteer de mensen die aan veiligheid werken in hun omgang met persoonsgegevens.

Vooraf opleiden

De vuistregel dat gebruikers van systemen en databases eerst een afdoende opleiding gevolgd moeten hebben en pas daarna een autorisatie tot gebruik kunnen krijgen is een voorbeeld van het zorg dragen voor voorlichting en faciliteiten. De voorwaarde van ‘vooraf opleiden en dan pas autoriseren voor gebruik‘ wordt in de praktijk gehanteerd door bijvoorbeeld politiekorpsen en het ministerie van Defensie.

Wat betekent de ‘zorg voor voorlichting en faciliteiten’:

Onbekendheid met en ingewikkeldheid van privacywetgeving is een van de redenen waarom de brug tussen privacy en veiligheid in de praktijk moeilijk is te slaan. Het streven naar privacy als een normaal beleidsterrein behoeft nog een concrete vertaling naar de praktijk. Codes en protocollen voor de werkvloer zijn daarvoor onmisbaar. De overheid zou daarin een faciliterende rol moeten spelen, maar primair moeten de (overheids-)instanties hun medewerkers faciliteren in het omgaan met regels over privacy en veiligheid. Eerder – in paragraaf 2.6 – signaleerde de Commissie dat de private sector op beleidsterreinen als productkwaliteitszorg, zorg voor arbeidsomstandigheden, milieuzorg is overgegaan tot normalisatie en certificering om de achterliggende belangen in de organisatie te borgen. De Commissie beveelt aan na te gaan of met behulp van normalisatie en certificering ook de zorg voor privacy geborgd kan worden als onderdeel van de bedrijfsvoering van de organisaties die werken aan de veiligheid. Vanzelfsprekend zijn verder opleidingen, simulaties, ontwikkelingen van ‘*good’* en ‘*best practices*’ potentieel belangrijke faciliteiten.

Onbekend maakt onbemind

In de praktijk blijkt keer op keer dat de personeelsleden die daadwerkelijk met systemen en gegevens werken vaak niet of nauwelijks bekend zijn met de regels en voorschriften. Ook bij cursisten blijkt dat de bekendheid met de eigen Wbp-gedragscodes nog al eens beperkt is tot “ja, ik weet dat er wel zoiets is, ja”.

Welk doel dient de ‘zorg voor voorlichting en faciliteiten’:

Voorlichting en facilitering dienen als prikkel tot de naleving van de privacywetgeving en om bij te dragen aan de veiligheid. Bieden van een handreiking voor het werken aan privacy en veiligheid aan ‘professionals’, instanties, bedrijven en instellingen dient beide belangen. De omgang met persoonsgegevens verdient het serieus te worden genomen op de werkvloer. Dat is nodig om schade voor individuele personen te voorkomen en het primaire werk van organisaties niet te frustreren. En dat is ook nodig om bij te dragen aan het vertrouwen tussen de deelnemers aan de samenleving als geheel. Een samenleving van wantrouwen schaadt uiteindelijk ook de veiligheid.

Zeker bij complexere samenwerkingsverbanden is het nauwkeurig beleggen van de verantwoordelijkheid voor goede omgang met persoonsgegevens cruciaal. In de praktijk blijkt juist in die situaties het op eenduidige wijze beleggen lastig. Terwijl het er juist dan vaak op aankomt dat wat gedeeld moet worden ook daadwerkelijk wordt gedeeld. Het ligt voor de hand om bij een aantal concrete samenwerkingsverbanden – te denken valt aan veiligheidshuizen of de jeugdgezondheidszorg – na te gaan hoe ‘professionals’ in hun samenwerken verder gefaciliteerd kunnen worden. Wellicht helpt een wettelijke voorziening om samenwerking tussen deelnemers aan samenwerkingsverbanden op veiligheidsterrein te vergemakkelijken, mogelijk volstaat een modelcode of gaat het er vooral om handzame instructies door ‘professionals’ en hun organisaties tot stand te brengen.

De kleine ondernemer

Het voorlichten en faciliteren van personeelsleden is een taak voor de werkgever is een veel gehoorde mening. Het lijkt ook een vanzelfsprekende mening. Maar zonder ondersteuning van overheid of van branches is die voorlichting voor ondernemers in het midden- en kleinbedrijf welhaast ondoenlijk. Voorlichtingsmateriaal wordt door kleine ondernemers ook node gemist.

Wie is verantwoordelijk voor de 'zorg voor voorlichting en faciliteiten':
Voldoen aan de grondslagen voor de zorgvuldige omgang met persoonsgegeven op het gebied van veiligheid is de verantwoordelijkheid van de organisatie voor wie de 'professional' werkt. Deze organisatie zal veel afwegingen aan de 'professional' moeten overlaten. Een competente 'professional' zal zijn werk goed willen doen en om dat mogelijk te maken moet de organisatie de 'professional' actief faciliteren en rugdekking geven. Zowel de 'professional' als zijn organisatie hebben er baat bij de algemene uitgangspunten voor zorgvuldige omgang met persoonsgegevens in het dagelijkse werk te incorporeren. De 'professional' heeft behoefte aan de uitwisseling van ervaringen met collega's, aan ontwikkeling en uitwisseling van *´good´* en *´best practices´*. Deelnemen aan simulaties kan goed helpen. De organisatie heeft er belang bij dat de '*state of the art*' op adequaat niveau is.

De stelselverantwoordelijkheid voor voorlichting en facilitering behoort los te staan van het 'externe toezicht en de handhaving' en berust bij de verantwoordelijke bewindspersonen. Invulling geven aan deze stelselverantwoordelijkheid zal veelal vooral bestaan in het in het leveren van de juiste prikkels om koepelorganisaties, bedrijfstakken, organisaties van 'professionals', onderdelen van de overheidsorganisatie etc. aan te zetten voorlichting en facilitering ter hand te nemen.

Uitzonderingen:
Facilitering en voorlichting als onderdeel van de stelselverantwoordelijkheid vormen kerntaken van de overheid. Dat betekent echter niet dat bedrijven, organisaties en instellingen met de armen over elkaar kunnen gaan zitten. Op hen rust de verantwoordelijkheid voor het naleven van privacyregels binnen hun organisatie. Daartoe kunnen zij zelf gedragscodes, cursussen en richtlijnen ontwikkelen. Indien nodig kunnen zij daarvoor de hulp van de overheid inroepen.

Grondslag 6. Zorg voor naleving en intern toezicht
s. Waarborg dat de mensen die aan veiligheid werken de regels naleven en zorg voor goed intern toezicht.
t. Overweeg een 'functionaris voor de gegevensverwerking' zoals genormeerd in de Wet bescherming persoonsgegevens aan te stellen.

Externe beoordeling en keurmerk

Het laten uitvoeren van privacyaudits of het laten certificeren van verwerkingen zijn mogelijkheden om een onafhankelijk oordeel te verkrijgen over de naleving van wetgeving. In de Wet gemeentelijke basisadministraties persoonsgegevens en in de Wet politiegegevens zijn audits al verplicht gesteld. Instrumenten daarvoor zijn de compliance instrumenten van het College bescherming persoonsgegevens en de certificering door externe auditors zoals ontwikkeld door NIVRA en NOREA.

Wat betekent de 'zorg voor naleving en intern toezicht':

Zorg voor naleving betekent op basis van risicoanalyse nagaan waar de kwetsbare risico's voor de zorgvuldige omgang met persoonsgegevens schuilgaan en de nodige maatregelen in gang zetten om deze risico's te voorkomen of te beheersen. Hoe een bedrijf of instelling de zorg voor de naleving vormgeeft zal afhangen van factoren als de aard en omvang van de risico's, de omvang van het bedrijf of de (overheids-)instelling, de competenties van de 'professionals' die met persoonsgegevens werken en vele andere.

Zorgvuldig omgaan met persoonsgegevens is op het veiligheidsterrein geen vanzelfsprekendheid. Er kunnen zich vele omstandigheden voordoen die er toe leiden dat 'professionals' het met de regels niet erg nauw nemen. Daarom is het noodzakelijk binnen iedere instelling of binnen ieder bedrijf een functionaris aan te wijzen die met voldoende gezag tot naleving kan aanzetten. Soms voor deze taak vrijgesteld, soms naast andere taken. De werkvloer van veiligheid en persoonlijke levenssfeer is te veelvormig om precies voor te schrijven hoe de zorg voor naleving en intern toezicht moet worden ingevuld. Wel zal steeds een passende voorziening operationeel moet zijn. Er zijn gerede aanwijzingen dat in organisaties waar een 'functionaris voor de gegevensbescherming' is aangewezen – in het jargon: een FG – het niveau van zorgvuldigheid bij het omgaan met persoonsgegevens adequater is[19]. De commissie acht dit zeer aannemelijk. De aanwezigheid van zo'n relatief onafhankelijke functionaris die belast is met intern toezicht op de naleving van zorgvuldigheidsregels voor omgaan met persoonsgegevens op voldoende hoog niveau in de organisatie kan een belangrijke prikkel voor zorgvuldigheid genereren. De Commissie acht het in grotere organisaties zeer de moeite waard een gezaghebbende '*functionaris voor de*

[19] Vgl. College bescherming persoonsgegevens, Informatieblad 16, juni 2004, te raadplegen op website Cbp; aanwijzingen dat een functionaris voor de gegevensbescherming inderdaad bijdraagt aan een adequater zorgvuldigheidsniveau ontleent de Commissie aan het nog te publiceren rapport van de tweede fase evaluatie Wet bescherming persoonsgegevens, "Wat niet weet, wat niet deert."

gegevensbescherming' als bedoeld in de Wet bescherming persoonsgegevens aan te stellen om intern toezicht te houden op de zorgvuldige omgang met persoonsgegevens.

Verantwoording en rapportages

Rapportages en de verplichting tot rapporteren kunnen ook bijdragen aan zorg voor zorgvuldige gegevensverwerking. Voorbeelden van verplichte rapportages zijn te vinden in de gedragscode Financiële instellingen in de Wet politiegegevens (de rapportageplicht van de privacyfunctionaris). Ook het jaarverslag van de functionaris voor de gegevensbescherming is een voorbeeld van een rapportageplicht. De milieu-rapportages zijn inmiddels bekend; zouden privacyrapportages eenzelfde ontwikkeling door kunnen maken?

Welk doel dient de ' zorg voor naleving en intern toezicht':

Alleen wanneer regels, grondslagen en handreikingen worden nageleefd hebben deze nut. Het lijdt geen twijfel dat zorgvuldig omgaan met persoonsgegevens belangrijke doelen dient en dat de realisering van deze doelen afhankelijk is van naleving. Zonder actief toezicht en zonder een uitdrukkelijk belegde verantwoordelijkheid voor naleving en toezicht zal de prikkel om conform regels, grondslagen en handreikingen te werken snel wegvallen. Bovendien is het de moeite waard om steeds na te gaan of technologische of andere ontwikkelingen verder kunnen bijdragen aan de zorgvuldigheid bij het omgaan met persoonsgegevens.

Wie is verantwoordelijk voor de 'zorg voor naleving en intern toezicht':

Het bevoegde gezag van bedrijf of instelling dat ten behoeve van de veiligheid met persoonsgegevens werkt is onder alle omstandigheden verantwoordelijk voor verwerkelijking van de regels. Dus ook voor het waarborgen van prikkels tot naleving. Bij het aangaan van samenwerkingsverbanden is het altijd nodig afspraken over de verantwoordelijkheid te maken.

Voor naleving en intern toezicht is wel iemand nodig

Het aanstellen van privacyfunctionarissen of het aanstellen van een functionaris voor de gegevensbescherming is een middel om aandacht voor zorgvuldige gegevensverwerking te creëren. Ook kan aandacht voor zorgvuldige gegevensverwerking verbeterd worden door dit als taakonderdeel op te nemen van bijvoorbeeld compliance-officers (financiële instellingen) of van beveiligingsfunctionarissen. Het toepassen van de grondslagen in de praktijk zal zeker gediend zijn bij aanstelling van dergelijke functionarissen of dergelijk taakaccenten.

Uitzonderingen:
Mogen zich niet voordoen. Waarborgen van naleving is altijd verplicht net als het feitelijk uitoefenen van intern toezicht.

3.7 Robuust extern toezicht en handhaving [20]
Toepassing van het richtinggevende kader spoort de organisaties van 'professionals' aan tot goede omgang met persoonsgegevens. Het richtinggevende kader legt een belangrijk accent bij de gemarkeerde eigen verantwoordelijkheid van de organisaties waar 'professionals' aan veiligheid werken. Door risicoanalyse, faciliteren en voorlichten, de zorg voor architectuur en integriteit van systemen alsmede het uitoefenen van intern toezicht maken de organisaties die werken aan veiligheid – ook de overheidsorganisaties – de geldende wettelijke regels pasklaar voor hun eigen praktijk. Zo vergemakkelijken zij toepassing van de eerste drie grondslagen die toezien op het feitelijk omgaan met persoonsgegevens. Idealiter relativeert dit de rol van wettelijke regels ten gunste van bij de 'professionals' passende handreikingen die de wettelijke regels naar de praktijk vertalen.
Intussen moet wel worden nagegaan of de vereiste en wettelijk voorgeschreven zorgvuldigheid via toepassing van de grondslagen daadwerkelijk in acht wordt genomen. En of de wettelijk voorgeschreven zorgvuldigheid adequaat is geborgd. Ook een externe prikkel in de vorm van robuust extern toezicht en handhaving is nodig om de grondslagen kracht bij te zetten. Daar zijn bovenal onafhankelijke audits op de werkvloer voor nodig. Audits die ook hun schaduw vooruitwerpen naar verwante praktijken. Audits die zo nodig in geval van het ontbreken van de vereiste zorgvuldigheid een vervolg krijgen in passende prikkels om nalatigheid te corrigeren.

Het College bescherming persoonsgegevens houdt momenteel toezicht op de naleving van de Wet bescherming persoonsgegevens naast de vervulling van taken als advisering over wetgeving, toetsing van gedragscodes en reglementen, voorlichting, bemiddeling, klachtbehandeling en internationale taken. Deze situatie is niet gewenst. De slagvaardigheid van het externe toezicht houden is er bij gebaat wanneer de externe toezichthouder organisatie geen bemoeienis had met advisering, voorlichting of facilitering.

[20] De *Kaderstellende visie op toezicht*, Tweede Kamer, vergaderjaar 2000-2001, 27 831, nr. 1, p. 18 definieert toezicht als: "*het verzamelen van de informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren.*" Van handhaving is sprake als de toezichthouder bestuurs- of strafrechtelijke dwang uitoefent. Op 'goed toezicht' zijn zes principes van toepassing: goed toezicht is selectief, slagvaardig, samenwerkend, onafhankelijk, transparant en professioneel.

Verantwoordelijkheid voor het houden van extern toezicht en de handhaving moet juist los staan van bemoeienis met zelfregulering door bijvoorbeeld de goedkeuring van gedragscodes, omdat verstrengeling van deze activiteiten per saldo de externe toezichthouder beperkt in zijn vrijheid. Daar komt bij dat het vanuit het perspectief van de organisaties waarop extern toezicht wordt uitgeoefend merkwaardig is, dat zij zich voor voorlichting en advisering moeten wenden tot dezelfde instantie die hen later een tik op de vingers kan geven met behulp van ten behoeve van advisering verstrekte informatie. Ook de schijn daarvan moet worden vermeden. Dat laat weer onverlet dat de toezichthouder gebruik kan maken van wat in het kader van zelfregulering ontwikkeld wordt aan instrumenten als codes en '*good*' en '*best practices*'. Robuust extern toezicht zal nimmer vrijblijvend kunnen zijn, wel 'gidsend' om de praktijk zekerheid te geven. De Nederlandse Mededingingsautoriteit doet dat bijvoorbeeld door het publiceren van richtsnoeren.

Wat nodig is, is een gemarkeerde verantwoordelijkheid voor onafhankelijk extern toezicht, handhaving, die zich concentreert op wat er feitelijk van de naleving van de regels terecht komt en met passende middelen tot handhaving de praktijk zo nodig bijstuurt.

Robuust toezicht

De Amerikaanse financiële dienstverlener LPL Financial Corporation betaalde in 2008 275.000 dollar aan de Amerikaanse toezichthouder de Securities and Exchange Commission (SEC) toen deze toezichthouder het bedrijf aansprak vanwege het niet voldoende beveiligen van klantgegevens en de privacyschending die dat opleverde. De gegevens konden gestolen worden en daardoor was er het gevaar van identiteitsdiefstal.

Wat betekent dit 'robuust extern toezicht en handhaving':

Als de ruimte voor zelfregulering goed wordt benut, als de 'professionals' ruimte krijgen om zorgvuldige afwegingen te maken en hun organisaties hen daarbij faciliteren en hun de benodigde rugdekking geven ontstaat ruimte de regeldruk te verminderen, mits tezelfdertijd een adequaat functionerend sluitstuk van extern toezicht en handhaving werkzaam is. Dat betekent ook dat op basis van een scherpe prioritering de feitelijke omgang met persoonsgegevens op de werkvloer aan toezicht wordt onderworpen: kijken hoe het verzamelen en delen van persoonsgegevens in de praktijk feitelijk verloopt en of dat volgens de regels gaat. Dat wil zeggen: niet volstaan met beoordelen of de papieren werkelijkheid van codes en reglementen strookt met de wettelijke verplichtingen. En niet alléén op basis van

signalen reageren, maar ook op basis van eigen prioritering pro-actief de praktijk ingaan om bij te dragen aan de wisselwerking tussen praktijk, regels en de belangen en waarden die in de regels zijn vervat. Deze benadering sluit naadloos aan bij de Kaderstellende visie op toezicht, die een belangrijk accent legt op een passende reactie van de toezichthouder op het feitelijke gedrag op de werkvloer. Het gaat ook om toezicht op de naleving door de publieke sector. Dat maakt het nodig het externe toezicht in relatieve onafhankelijkheid van de verantwoordelijke bewindspersonen uit te voeren. Het is noodzakelijk cyclisch een programma voor de ontwikkeling van het toezicht vast te stellen op basis van de grootste nalevingsrisico's, op basis van de te verwachten betekenis van toezicht voor de naleving en in samenhang met de ontwikkeling van zelfregulering.

Daar passen ook de goede sancties bij. Dat kunnen sancties zijn in de vorm van:

- een 'last' al dan niet onder dwangsom;
- bestuursdwang, waarbij de toezichthoudende autoriteit zelf voorziet in hetgeen deze nodig acht;
- '*naming* en *shaming*'; vooral in een setting waar 'vertrouwen' van de omgeving van de overtreder een belangrijke rol speelt kan deze sanctievorm effectief blijken;
- bestuurlijke boetes.

Volledigheidshalve: optreden van een externe toezichthoudende autoriteit laat vanzelfsprekend de bestaande privaatrechtelijke mogelijkheden onverlet. Ook is er geen aanleiding tot wijziging van de bestaande strafrechtelijke sanctionering.

De ruimte die de Wbp biedt voor zelfregulering heeft er nog niet toe geleid dat de regels op de werkvloer zijn aangekomen. Verantwoordelijkheden blijken gemakkelijk uit de weg te worden gegaan en vrijblijvendheid krijgt te ruim baan. Robuust extern toezicht met de passende middelen tot handhaving vormt daarom een onmisbaar sluitstuk bij het bevorderen van zorgvuldige omgang met persoonsgegevens op de werkvloer van de veiligheid.

Wie is verantwoordelijk voor 'robuust extern toezicht en handhaving':
De overheid is verantwoordelijk voor het instellen van een onafhankelijke toezichthouder met voldoende bevoegdheden en financiële middelen om toezicht en handhaving van privacyregels op het gebied van de veiligheid naar behoren te kunnen uitoefenen. De

toezichthouder moet in alle onafhankelijkheid kunnen opereren, ook naar onderdelen van de overheid. Wel kan hij er zelf voor kiezen samen te werken met andere organisaties en instellingen. Voorbeelden daarvan zijn het gezamenlijke oordeel van Cbp en Onafhankelijke Post en Telecommunicatie Autoriteit inzake "*tell a friend* systemen" op websites en het recente rapport over de informatiebeveiliging in ziekenhuizen dat het Cbp in samenwerking met de Inspectie voor de Gezondheidszorg heeft opgesteld.[21]

3.8 Uitleiding

Het richtinggevende kader brengt grondslagen en handreikingen tot leven die hun weg naar de praktijk van veiligheid en privacy moeten vinden. De Commissie constateert dat de grondslagen en handreikingen voortvloeien uit het al bestaande wettelijke kader. De Commissie adviseert met de voorgestelde grondslagen en handreikingen niet allerlei nieuwe instrumenten in het leven te roepen, maar te doen wat al gedaan had moeten zijn: op een eenvoudige manier de 'professionals' op het veiligheidsterrein helpen zorgvuldig met persoonsgegevens te werken door deze zorgvuldigheid in hun dagelijkse werk te verankeren en de passende prikkels om dat te waarborgen in het leven te roepen.

De werkvloer worstelt met de opslag, verwerking en uitwisseling van persoonsgegevens. Wat mag wel en wat niet? Het blijkt geen eenvoudige opgave hier adequaat mee om te gaan in de praktijk. Dat is begrijpelijk, want toepassen van de regelgeving in een concrete situatie is vaak lastig. De belangen die op het spel staan zijn echter groot, zowel het belang van veiligheid als dat van de bescherming van de persoonlijke levenssfeer. De werkvloer verdient daarom een betere facilitering:

- het goede gereedschap, d.w.z. goede ICT-voorzieningen, gemakkelijk toegankelijke handreikingen, '*good*' en *'best practices*' en dergelijke;
- goede training en geregeld met partners specifiek de goede omgang met persoonsgegevens als onderdeel van de dagelijkse routine doornemen;
- eenduidige en gemarkeerde verdeling van verantwoordelijkheden, ook bij samenwerkingsverbanden;
- de passende prikkels tot naleving, w.o. toezicht en handhaving;
- versterkte transparantie;

[21] Gezamenlijk oordeel van Cbp en Opta inzake "tell a friend systemen" op websites, december 2008 en rapportage van een onderzoek in 2007 door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg naar de informatiebeveiliging in 20 ziekenhuizen, Den Haag, november 2008; beide te raadplegen via www.cbpweb.nl.

- meer aandacht voor de integriteit van systemen;
- betere naleving en intern toezicht;
- robuust extern toezicht en handhaving door een sterke en onafhankelijke toezichthouder, die zich alleen is belast met ‘toezicht houden en handhaven’.

De Commissie legt in haar advies een belangrijk accent op de werkvloer, op de dagelijkse praktijk van de ‘professionals’ en hun organisaties. Verantwoordelijkheid voor zorgvuldig omgaan met persoonsgegevens ten behoeve van veiligheid berust voor een belangrijk deel bij de organisaties waar deze ‘professionals’ voor werken. Deze moeten de ‘professional’ faciliteren en rugdekking geven, ook door hun organisatie toe te rusten met integere systemen. Dat laat onverlet dat de overheid een belangrijke verantwoordelijkheid draagt voor het stelsel van veiligheid en persoonlijke levenssfeer. Die verantwoordelijkheid vervult de overheid op verschillende manieren. In de eerste plaats heeft de overheid de verantwoordelijkheid voor het stelsel van publiekrechtelijke regelgeving. Hoe nodig het ook is het accent bij het formuleren van handreikingen als onderdeel van het dagelijkse werk te verplaatsen naar de werkvloer en de organisaties waar de ‘professionals’ voor werken, er moet een wettelijk kader – alleen al vanwege de internationaalrechtelijke verplichtingen – van kracht zijn om de veiligheid van personen en persoonsgegevens te waarborgen.
In de tweede plaats zijn de grondslagen en handreikingen van de vorige paragraaf ook op de overheid van toepassing zodra deze aan het werk gaat op het raakvlak van veiligheid en persoonlijke levenssfeer. Dat de Commissie bij het tot stand brengen van dit advies geregeld stuitte op gefundeerde kritische observaties over de zorgvuldigheid van de overheid bij besluitvorming over omgaan met persoonsgegevens op het gebied van de veiligheid moet aanleiding geven tot handelen. De overheid is de grootste speler op dit terrein en de belangrijkste verwerker van persoonsgegevens. Voorbeeldgedrag zal het handelen van de private partners onmiskenbaar beïnvloeden.
In de derde plaats is er een verantwoordelijkheid voor het feitelijk functioneren van het stelsel van veiligheid en persoonlijke levenssfeer. Deze verantwoordelijkheid kan de overheid invulling geven:

- door zelf zorgvuldig te werk te gaan bij besluitvorming over en feitelijk omgaan met persoonsgegevens ten behoeve van veiligheid;
- door de verantwoordelijkheid voor het feitelijk invulling geven aan de grondslagen voor zorgvuldige persoonsgegevensverwerking op het gebied van

de veiligheid nadrukkelijk neer te leggen bij de organisaties van ‘professionals’;

- door de ‘professionals’ op een slimme manier te prikkelen er ook echt werk van te maken;
- door overheden en maatschappelijke partners te prikkelen hun ‘professionals’ goed te faciliteren;
- door toezicht uit te oefenen op de naleving van de regels en handhavend op te treden bij constatering van overtredingen.

HOOFDSTUK 4 TOEPASSING VAN KADER OP ACTUELE CASES

4. Het richtinggevende kader in de praktijk

De Commissie heeft op verzoek van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie aan twee onderwerpen bijzondere aandacht gegeven: kentekenherkenning met camera's en registratie op etniciteit en levensbeschouwing. Die twee onderwerpen zijn politiek en maatschappelijk actueel.

Het formuleren van een richtinggevend kader zoals in hoofdstuk 3 gedaan is heeft alleen zin en heeft alleen betekenis als beleidsmakers en uitvoerders van beleid dit kader in de praktijk ook toe kunnen passen. Het toetsingskader heeft een algemeen karakter. Dit is zowel een voordeel – het is breed toepasbaar - als een nadeel. Rechtshandhavers en hulpverleners zullen bemerken dat elke casus uniek is of op zichzelf staat. Sterker nog, de verschillende betrokkenen bij één en dezelfde casus hebben vaak ook verschillende percepties. Het is ook om die reden dat het gaat om 'grondslagen' en niet om 'wetten van Meden en Perzen'. Het is immers niet mogelijk om een 'absolute theorie' te geven waarlangs alle vraagstukken over de balans tussen veiligheid en persoonlijke levenssfeer 'eventjes' kunnen worden opgelost. Deze vraagstukken dienen elk voor zich en op hun eigen merites te worden gewogen, net zoals vraagstukken op andere beleidsterreinen. Maar het geschetste kader geeft wel aanknopingspunten om die weging te concretiseren en in te vullen.

4.1. Kentekenherkenning met camera's

Het verzoek van de ministers ziet op het gebruik van camera's die voorzien zijn van computerprogramma's en waarbij de automatisch herkende kentekens vergeleken worden met al in een de database vastgelegde kentekens.
Het verwerken van videobeelden van camera's valt onder de Wet bescherming persoonsgegevens of de Wet politiegegevens. Cameratoezicht moet voldoen aan de voorwaarden die zijn vastgelegd in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden: kenbaarheid, subsidiariteit, proportionaliteit, doelbinding, formeelwettelijke grondslag (zoals nu onder meer in de Politiewet en Gemeentewet geregeld). '*Automatic Number Plate Recognition*' (ANPR) is een programma waarmee camera's worden gebruikt om kentekens van voertuigen vast te leggen. De camera's die voorzien zijn van ANPR-programmatuur worden gekoppeld aan de database/verzameling kentekens. Het vastleggen van deze kentekens gebeurt met het doel

deze te vergelijken met een vooraf samengestelde verzameling kentekens die (nader) onderzoek behoeven. Gegevens worden vergeleken met informatie over gesignaleerde personen, gestolen voertuigen of openstaande boetes. De algemene doelstellingen zijn: de handhaving van de rechtsorde en de ondersteuning van de informatiepositie van de politie. De wettelijke basis hiervoor is dun, namelijk art.2 Politiewet. De artikelen 8 en 9 van de Wet politiegegevens regelen de bewaartermijnen. Soms wordt ANPR onder gezag van het Openbaar Ministerie ook ingezet voor opsporingsdoeleinden en vallen de verzamelde gegevens onder het regiem van de Wet strafvorderlijke en justitiële gegevens. Dit gebeurt dan onder het gezag van het Openbaar Ministerie.

Momenteel zijn 20 regiokorpsen van politie en het KLPD met ANPR aan het experimenteren. In de regionale driehoek wordt besloten tot de inzet van dit instrument, vanwege de drugsrunnersproblematiek in Limburg-Zuid, mobiel banditisme in het oosten des lands of het transport van illegale goederen via de Rotterdamse haven. Het regiokorps IJsselland bewaart de gegevens zeven dagen, het korps Drenthe veertien dagen (bijvoorbeeld ten tijde van massale verkeersstromen in het weekeinde van de TT-races te Assen). Het korps Rotterdam Rijnmond bewaart de gegevens vier maanden omdat ANPR ook wordt ingezet voor de opsporing, onder meer bij de bestrijding van drugssmokkel. Er zijn ook korpsen die langere termijnen hanteren.

Naast de politiekorpsen gebruiken ook de Belastingdienst (voor het innen van achterstallige belastingen, zowel rijks- als gemeentebelastingen), het ministerie van Verkeer en Waterstaat (transportcontroles), de Inspectie Verkeer en Waterstaat (controle taxivervoer), de Koninklijke Marechaussee (15 grensovergangen) en Rijkswaterstaat (wegwerkzaamheden) het programma ANPR. Dit gebeurt op een andere juridische basis.
De Nationaal Coördinator Terrorismebestrijding treft voorbereidingen voor toepassing van ANPR op hotspots (knooppunten in het openbaar vervoer zoals vliegvelden en grote treinstations).
ANPR wordt regionaal, incidenteel en zonder daadwerkelijke samenhang ingezet. Onderlinge afstemming vond tot voor kort nauwelijks plaats. Inmiddels zijn er verschillende samenwerkingsverbanden, maar kennis en ervaring worden nog onvoldoende gedeeld. Er kan sprake zijn van ‘*overpowering*’ en te weinig aandacht voor de bescherming van de persoonlijke levenssfeer.

Het richtinggevende kader toegepast op ANPR

Grondslag 1: Transparantie, tenzij;

Weinig burgers weten dat en met welk(e) doel(en) ANPR wordt gebruikt. Alleen van de politie weten wij het ‘een beetje’. Op snelwegen zien wij het waarschuwingsbord ‘radarcontrole’, maar nooit het bord ‘radarcontrole gekoppeld aan kentekenregistratie’. Elk korps formuleert – in het beste geval samen met het Openbaar Ministerie - de eigen doelen en in samenhang daarmee de bewaartermijnen. Er is geen inzicht in wat er met de gegevens (foto/datum/tijd/locatie gekoppeld aan kenteken) gebeurt die geen ‘*immediate hits*’ opleveren. Er is nu geen mogelijkheid tot inzage door burgers.

Grondslag 2: Selecteer voor je verzamelt

Het is nodig dat de doelen vooraf worden geformuleerd en dat daarbij wordt vastgesteld dat er geen minder ingrijpende manier is om deze doelen te bereiken. Vooraf moet ook duidelijk worden bepaald hoe lang en waarom deze gegevens zullen worden bewaard. Het antwoord dat deze elektronische inzet voor zowel de politie als de burgers ‘veel effectiever’ is, volstaat niet. Er moet een risicoanalyse aan de inzet van het instrument vooraf gaan.

Als ANPR alleen voor controledoeleinden wordt gebruikt, zouden verzamelde gegevens na verwerking van de ‘*immediate hits*’ vrijwel onmiddellijk moeten worden vernietigd. Bij de opsporing van strafbare feiten kan het geboden zijn de verzamelde gegevens een bepaalde termijn te bewaren waarbij een termijn van één jaar wat aan de lange kant lijkt. In ieder geval is een meer gedegen juridisch kader vereist dan nu voor de politiekorpsen voorhanden is.

Grondslag 3: Indien noodzakelijk voor de veiligheid, moet je delen

Het kader geeft aan dat uit een risicoanalyse moet blijken dat er een noodzaak om te delen moet zijn. Die risicoanalyse gebeurt nu nog niet overal. In het algemeen worden gegevens die met ANPR worden verzameld niet gedeeld, ook niet tussen de verschillende korpsen. Dit gebeurt alleen in specifieke situaties, zoals bij voetbalwedstrijden en bij mobiel banditisme. Personen die een stadionverbod hebben rijden vaak met eigen auto toch naar uitwedstrijden van hun club. Via ANPR gaan korpsen direct tot actie over als er een kenteken matcht met het bestand ‘stadionverboden’.

Grondslag 4: Zorg voor integriteit van systemen, gegevens en het handelen van gebruikers ervan

ANPR is een softwareprogramma dat is gekoppeld aan een camera. Vervolgens wordt dit programma gekoppeld aan een database van kentekens. Afgezien van herkenningsfouten door de camera's is in beginsel sprake van correcte invoer van kentekengegevens. De fraudegevoelige aspecten zien op de achterliggende databases waaraan ANPR is gekoppeld en minder op de programmatuur zelf. Bij opsporing zal er sprake zijn van een geclausuleerde toegang tot de gegevens, bijvoorbeeld alleen voor de recherche. Het systeem zou moeten voorzien in het plaatsen van (geautomatiseerde) schotten en het automatisch opschonen van het systeem.

Grondslag 5; Zorg voor voorlichting en facilitering
Voor facilitering van de rechtshandhaver – i.c. de politiemedewerkers –zou voor ANPR een meer uniforme, liefst landelijke standaard of een landelijk protocol moeten worden ontwikkeld voor de gezamenlijke politiekorpsen, de Koninklijke Marechaussee en de NCTb. In dit protocol kunnen de toepassing van een risicoanalyse, doeleinden, bewaartermijnen, uniformiteit van programmatuur, autorisatieniveaus, eisen aan de integriteit van systemen en de voorlichting aan de burgers inclusief mogelijkheid tot inzage worden opgenomen.

Grondslag 6: Zorg voor naleving en intern toezicht
De Wet politiegegevens verplicht politiekorpsen wel om een privacyfunctionaris aan te stellen. Dit zijn vaak adviseurs en doeners tegelijk. Zij houden echter geen intern toezicht. Elk politiekorps zou daarom ook een functionaris gegevensverwerking moeten aanstellen, die intern toezicht houdt, een meldingenregister bijhoudt en het privacy-jaarverslag opstelt.

Het richtinggevende kader geeft aan dat de toezichthouder de mogelijkheid zou moeten hebben streng op te treden wanneer de hierboven beschreven grondslagen niet in acht zijn genomen. Ook zou de toezichthouder moeten verlangen dat aan de eis van transparantie concreet gevolg wordt gegeven. Niet voldoen aan de wettelijke vereisten moet resulteren in het opleggen van (forse) boetes, tot de verplichting om systemen en convenanten aan te passen maar ook tot de publieke bekendmaking van inbreuken op de persoonlijke levenssfeer.

Deelconclusie Kentekenherkenning met camera's
De deelconclusie is dat de doelen (toezicht, controle, opsporing) scherper moeten worden geformuleerd en ook van elkaar moeten worden gescheiden. Wanneer er in de wet geen gerechtvaardigde argumenten zijn te vinden om ANPR te gebruiken voor algemene

opsporings- en vervolgingsdoeleinden, moeten de gegevens die in het kader van ANPR zijn verkregen daarvoor ook niet worden gebruikt. De transparantie en kenbaarheid van het gebruik moeten sterk worden verbeterd. Daarbij is ook van belang dat wordt bepaald gedurende welke termijn de gegevens voor de vastgestelde doelen moeten worden bewaard. De gebruikers van het systeem zijn gebaat bij een landelijke standaard of een landelijk protocol, waarin ook aandacht wordt gegeven tot de mogelijkheid van correctie van automatisch ingevoerde gegevens. Verder zouden privacywaarborgen in het systeem moeten worden ingebouwd, bijvoorbeeld door automatische verwijdering van de gegevens na een bepaalde termijn.

4.2 Registratie van etniciteit

Verzamelingen van persoonsgegevens leveren waardevolle informatie op over het gedrag van individuen binnen bepaalde groepen. Voor de lokale overheid is dit interessant met het oog op bijvoorbeeld het ontwikkelen en het voeren van een preventiebeleid ten behoeve van de handhaving van de openbare orde en het voorkomen van strafbare feiten. Deze behoefte is groeiende omdat de overheid al of niet bedoeld steviger inzet op het streven naar een 'risicoloze samenleving'. In de tweede plaats leveren de technologische toepassingen een ruime variatie aan mogelijkheden voor gegevensverwerking.

De Commissie spreekt zich niet uit over de wenselijkheid van registratie van etniciteit. Besluitvorming daarover is aan de politiek verantwoordelijken. Daargelaten of registreren van etniciteit daadwerkelijk bijdraagt aan het oplossen van problemen, schetst de Commissie de maatschappelijke en juridische context die bij deze registratie speelt.
Op een actueel voorbeeld, de aanpak van Antilliaanse probleemjongeren, worden de grondslagen van het richtinggevende kader getoetst.

Op grond van de Wbp is het *verwerken* van persoonsgegevens over iemands ras, gezondheid, etc. verboden, behalve in specifieke situaties (Wbp art. 16). De wet staat *verwerking* toe als dat gebeurt met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen, mits voldaan is aan de voorwaarde dat dit voor het bepaalde doel noodzakelijk is (Wbp art. 18 b). Het verbod van artikel 16 is ook niet van toepassing voor zover dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid met het oog op een goede behandeling of verzorging van betrokkene (Wbp art. 21, derde lid). De laatste uitzondering op het verbod van art. 16 staat in Wbp art. 23: wetenschappelijk onderzoek. Hierbij wordt onder andere de eis gesteld dat bij de uitvoering is voorzien in zodanig waarborgen dat de persoonlijke levenssfeer van betrokkenen niet onevenredig wordt geschaad.

De beleidspraktijk maakt al langer gebruik van registratie van allochtonen. Tot 2003 werd via de Wet Bevordering Evenredige Arbeidsdeelname Allochtonen respectievelijk de Wet Stimulering Arbeidsdeelname Minderheden de registratie aangewend voor een positief doel, nl. het vergroten van de toegankelijkheid van de arbeidsmarkt. Hetzelfde gold tot voor kort

voor de onderwijsfinanciering, waar kinderen van allochtone afkomst zwaarder meewogen in de financieringssystematiek. Hiervoor werden doorgaans de reguliere definities van het Centraal Bureau voor de Statistiek gebruikt.

De discussie over de registratie van etniciteit wordt niet alleen gevoerd bij criminaliteitsbestrijding en deradicalisering. Ook als het om de veiligheid en gezondheid van personen gaat, speelt de discussie volop. De staatssecretaris van Volksgezondheid, Welzijn en Sport schreef op 9 september 2008 aan de Tweede Kamer het volgende: "Zo (…) hebben vele ziekten een verschillende kans om voor te komen bij mensen van verschillende herkomst en komen sommige erfelijke eigenschappen in de ene groep vaker voor dan in een andere. En komt sikkelcelanemie vaker voor bij mensen afkomstig uit gebieden rond de Middellandse Zee. Voor individuele patiënten kan het zinvol zijn als hun behandelaar in bepaalde situaties op de hoogte is van hun herkomst, in het bijzonder als die gegevens een rol spelen bij de beoordeling van de gezondheidstoestand van die patiënt, zoals de onlangs in Rotterdam geopende polikliniek voor Hindoestanen met fragiel vaatstelsel."[1] Ook ware te denken aan het grote aantal schizofrene jongeren van Marokkaans-Nederlandse afkomt en het aantal pogingen tot zelfdodingen bij meisjes uit landen als Suriname en Turkije. Op dit moment bereiden twee adviesraden op het gebied van volksgezondheid een advies voor over registratie van etniciteit in de zorg.

Ten slotte woedt de discussie hierover ook in het buitenland. Zo is registratie van etniciteit opgenomen in het Franse politie informatiesysteem[2]. Na veel verzet zijn de criteria betreffende de seksuele voorkeur en gezondheidsproblemen wel uit het bestand geschrapt, maar de criteria aangaande etniciteit (nog) niet. Ook daar is een werkgroep 'Veiligheid en privacy' aan het werk gezet.

Richtinggevend kader leidend

Er is een verschil tussen de registratie voor beleidsinformatie en de registratie voor individuele gevallen. Registratie voor beleidsinformatie geeft inzicht in de problemen van bepaalde groepen en de lacunes in de aanpak. Dit gebeurt regelmatig. Door een koppeling van de gemeentelijke basisadministratie (GBA) en het Herkenningssysteem Politie is inzichtelijk hoe

[1] TK 2007-2008, II, 27 428, nr. 114, *Brief van de staatssecretaris van Volksgezondheid, Welzijn en Sport aan de Tweede Kamer*, 9 september 2008.
[2] Voorheen: Edvige, Exploration documentaire et valorisation de l'information générale.

de etnische afkomst (tot en met de tweede generatie) van verdachten is. Ook is in 2006 het Sociaal Statistisch Bestand van het CBS gekoppeld aan het Herkenningssysteem Politie. Deze gegevens zijn breed toegankelijk maar uiteraard niet tot individuele personen herleidbaar en volstrekt anoniem. Deze cijfers komen jaarlijks beschikbaar. Het Wetenschappelijk Onderzoeks- en Documentatiecentrum van het ministerie van Justitie heeft zowel in 2005 als in 2007 gerapporteerd over de herkomst van verdachten van criminaliteit[3].

Bij registratie op individueel niveau zijn gegevens wel herleidbaar tot persoonsniveau. Het doel is hier specifiek de aanpak voor een specifieke probleemjongere aan te pakken en daarvoor maatwerk te leveren. Een strikte toepassing van het richtinggevende kader is noodzakelijk. Het moet dan daadwerkelijk en overtuigend gaan om een op basis van een risicoanalyse en –beoordeling geselecteerde gegevens, die – omdat de veiligheid dit vereist – gedeeld worden met uitsluitend de noodzakelijke partners (gemeente, politie). Proportionaliteit en subsidiariteit zijn daarbij leidend als kader waarbinnen de risicoanalyse wordt gemaakt. Bespreking van individuele gevallen moet ook plaatsvinden op lokaal niveau, hetzij in de gezagsdriehoek, hetzij in Veiligheidshuizen of bij andere gemeentelijke informatie- en adviespunten.

Een voorbeeld, de aanpak van Antilliaanse risicojongeren[4]
Antilliaanse Nederlanders zijn sterk vertegenwoordigd in de cijfers over schooluitval, schulden, werkloosheid en criminaliteit. Naar schatting zijn ongeveer 13.000 Antilliaans-Nederlandse jongeren niet geregistreerd in het GBA.[5].Van alle Antilliaans-Nederlandse verdachten in de leeftijdscategorie 18–60 jaar in 1999 recidiveerde 72% in de periode 1999–2004.[6]

Belangrijk is dat veel vaker dan andere groepen Antilliaans-Nederlandse risicojongeren geen vaste woon- of verblijfplaats hebben. Ook vertonen zij een frequent verhuisgedrag. Gemeenten maken zich zorgen over een harde kern van Antilliaanse Nederlanders die met de huidige aanpak niet wordt bereikt. Gemeenten geven aan een hulpmiddel nodig te hebben om de jongeren beter in beeld te krijgen voor een gerichte aanpak en betere hulpverlening. De

[3] WODC, *Verdacht van criminaliteit, allochtoon en autochtoon nader bekeken*, 2005.
[4] Casus is gebaseerd op brief van de minister van Wonen, Wijken en Integratie aan de Tweede Kamer van 19 december 2008
[5] Kennisnet Integratiebeleid Etnische Minderheden, 2006.
[6] TK 2006-2007, II, 30 810, nt.1, *Integratiekaart 2006*; Sociaal en Cultureel Planbureau, *Jaarrapport Integratie 2007*, TK 2006-2007, II, 25 726, nr. 22, WODC, *Verdacht van criminaliteit; allochtoon en autochtoon nader bekeken*, 2007.

doelen van de gerichte aanpak waarvoor gegevensverzameling nodig is, zijn: achterstanden wegwerken, de risicojongeren een gepast hulptraject aanbieden en het terugdringen van criminaliteit. In het voorstel van de minister voor Wonen, Wijken en Integratie van 19 december 2008 worden de volgende instrumenten beschreven:

- gemeenten krijgen onderling meldingen over Antilliaanse probleemjongeren;
- de meldingen over Antilliaanse probleemjongeren worden opgenomen in de algemene Verwijsindex Risicojongeren;
- het niet ingeschreven staan in het GBA wordt ondervangen door het toekennen van een VerwijsindexServiceNummer (VSN);
- de meldcriteria voor Antilliaanse probleemjongeren zijn duidelijk omschreven.;
- de Antillianen-coördinator (de gemeenteambtenaar die verantwoordelijk is voor de aanpak van Antilliaanse probleemjongeren) wordt in de toekomst ‘meldingsbevoegd’.

Lang niet álle jongeren van Antilliaanse afkomst worden zonder meer opgenomen in de Verwijsindex Risicojongeren. Het gaat alleen om de groep met meervoudige problemen. Een jongere behoort tot de doelgroep wanneer er sprake is van een of meer van onderstaande criteria over de laatste twaalf maanden. Wanneer een jongere de laatste twaalf maanden niet meer valt onder één of meer van deze criteria dan wordt de verwijzing automatisch verwijderd. De criteria zijn:

- alleen registratie van jongeren wanneer hij of zij niet ouder is dan 24 jaar;
- deelname aan schuldhulpverleningstraject;
- niet geregistreerd in de Gemeentelijke Basisadministratie;
- in aanraking met hulpverlening;
- langdurig schoolverzuim of voortijdig schoolverlaten;
- grote afstand tot arbeidsmarkt;
- uitkeringsfraude;
- huurschuld van meer dan zes maanden;
- betrokkene voldoet aan 1-2-3- criteria van de politie: 1x geweldsdelict en/of 2x overig delict en/of 3x overlast.

De verwijsindex bevat uitsluitend verwijzingen en géén inhoudelijke informatie over de jongeren. Bovenstaande criteria worden ingepast in de algemene meldcriteria van de Verwijsindex Risicojongeren:

- blootstaan aan geestelijk of lichamelijk geweld, enige andere vernederende behandeling, of verwaarlozing;
- meer of andere dan bij zijn leeftijd normaliter voorkomende psychische problemen, waaronder verslaving aan alcohol, drugs of kansspelen;
- meer of andere dan bij zijn leeftijd normaliter voorkomende opgroei- of opvoedingsproblemen;
- minderjarig en moeder of zwanger;
- verzuim om andere reden dan ziekte of gebrek veelvuldig van school of andere onderwijsinstelling, dan wel (de dreiging) van voortijdig schoolverlaten;
- niet gemotiveerd om door legale arbeid in zijn levensonderhoud te voorzien;
- meer of andere dan bij zijn leeftijd normaliter voorkomende financiële problemen;
- geen vaste woon- of verblijfplaats;
- gevaar voor anderen door lichamelijk of geestelijk geweld of ander intimiderend gedrag;
- laat zich in met activiteiten die strafbaar zijn gesteld;
- ouders of andere verzorgers schieten tekort in de verzorging of opvoeding.

Het systeem beperkt zich tot een verwijzing naar instanties die betrokken zijn bij de jongeren. Als op basis van de verwijsindex blijkt dat een jongere bij meerdere instanties bekend is, dan kan er onderling contact worden opgenomen. De informatie-uitwisseling vindt vervolgens rechtstreeks plaats tussen de betrokken instanties.

Het richtinggevende kader toegepast op de Antilliaanse probleemjongeren

Grondslag 1: Transparantie, tenzij

Dat er een Verwijsindex Risicojongeren tot stand zou kunnen komen, zou voor een ieder kenbaar moeten zijn. De uitvoerende partijen en hun medewerkers hebben de index zelf ontwikkeld. Of de geregistreerde Antilliaanse jongere ervan op de hoogte is, is de vraag. Bij meldingen in de Verwijsindex Risicojongeren dient degene over wie een melding is binnengekomen, ook te worden geïnformeerd. De Verwijsindex bevat zelf geen feitelijke informatie, maar is alleen een piepsysteem (de ene instantie kan zien of een andere instantie ook een melding heeft gemaakt over een risicojongere).
Het kenbaarheidsvereiste kan bij specifiek beleid gericht op risicojongeren contraproductief zijn. De risicojongere of zijn ouders die te horen krijgen dat er over hen meldingen zijn

binnengekomen, zouden minder snel geneigd zijn om hulpverleners of politieagenten in vertrouwen te nemen.

Grondslag 2: Selecteer voor je verzamelt

De criteria ten aanzien van de Antilliaanse risicojongeren zijn door de politie en gemeente opgesteld. Op basis van een risicoanalyse is tot een selectie van criteria gekomen. Zo is uitgesloten dat de vele Antilliaanse jongeren, die in Nederland gewoon studeren en werken, in deze index terechtkomen. Ook de beperking in de tijd – de registratie gaat over de feiten van de afgelopen twaalf maanden – en de automatische verwijdering passen goed in deze grondslag. Wel worden eerdere signaleringsgegevens in de backoffice bewaard.
De handreiking 'scherm persoonsgebondenheid zoveel mogelijk af' in deze grondslag is niet sluitend; een jongere met een VSN-nummer verwijst bijna altijd naar een Antilliaanse jongere, omdat het probleem van niet-ingeschrevenen bij andere bevolkingsgroepen nauwelijks aan de orde is. Ook de toekomstige meldingsbevoegdheid van de Antillianencoördinator is herleidbaar tot – inderdaad – een Antilliaanse jongere. Op getrapte wijze wordt met deze instrumenten registratie op etniciteit herleidbaar.

Grondslag 3: Indien noodzakelijk voor de veiligheid, moet je delen

Persoonsgegevens moet je delen als uit een risicoanalyse blijkt dat delen noodzakelijk is voor de veiligheid. Op basis van een gemaakte risicoanalyse zijn de criteria voor de groep Antilliaanse probleemjongeren omlijnd en is de Verwijsindex tot stand gekomen.
Het verstrekken van gegevens in een concreet geval vergt een individuele afweging, een risicobeoordeling. Als er sprake is van meerdere meldingen over één Antilliaanse probleemjongere – bijvoorbeeld een acute bedreiging – dan maakt de professional uiteindelijk op basis van een risicobeoordeling de afweging dat informatie gedeeld móet worden. Gemeenten en politie zijn verantwoordelijk voor doorgeleiden van informatie naar de bij de Antilliaanse jongere betrokken instanties.

Grondslag 4: Zorg voor integriteit van systemen, gegevens en het handelen van gebruikers ervan

Bij de Verwijsindex Risicojongeren is een correctiemechanisme voor (de ouders van) jongeren nog niet goed geregeld. Ook moet duidelijk zijn welke gegevens voor welke doel worden bewaard en wanneer deze gegevens zullen worden verwijderd. Hier ziet de integriteit ook op de gebruikers van de systemen. Zij moet waarborgen dat de gegevens niet meer

worden gebruikt en gedeeld dan nodig. Er dient strikt met autorisatieniveaus te worden gewerkt.

Grondslag 5: Zorg voor voorlichting en facilitering
Zoals in hoofdstuk 2 gesteld, moeten in de nieuwe samenwerkingsverbanden op preventief (veiligheids)beleid al afwegingen over meldingen en informatie-uitwisselingen worden gemaakt voordat er sprake is van mogelijk ernstige feiten. Dat vergt investeringen in opleidingen, voorlichting via '*best practices*' en vooral duidelijke werkafspraken over autorisatieniveaus en inzage- en correctiemechanismen voor de burger.

Grondslag 6; Zorg voor naleving en (intern) toezicht
In gemeenten die kampen met Antilliaanse probleemjongeren zou de verantwoordelijke ambtenaar, de zogeheten Antillianen-coördinator, ondersteund moeten worden door een privacyfunctionaris.
Voor het interne toezicht (meldingenregister, jaarverslag) is de functionaris gegevensverwerking aangewezen.

Hier geldt het uitgangspunt dat waar vooraf meer vrijheid wordt geboden om, indien noodzakelijk, gegevens te moeten delen, er achteraf robuust toezicht plaatsvindt. Ook zou de toezichthouder stevig moeten kunnen handhaven. *Naming and shaming*, (hoge) boetes en de mogelijkheid tot een verplichte wijziging van gedragscodes en dergelijke kunnen daarbij aan de orde zijn.

Deelconclusie aanpak Antilliaanse risicojongeren
In het meest recente kabinetsvoorstel is gekozen voor een aanpak van Antilliaanse risicojongeren zonder direct de etniciteit van betrokkenen te registreren. Dit voorbeeld laat zien dat ook zonder directe registratie van etniciteit tot een gerichte aanpak van problemen kan worden gekomen. In het voorstel zijn de onderdelen van de risicoanalyse (noodzaak, subsidiariteit, proportionaliteit) in acht genomen. Omdat het voorstel mede door de 21 gemeenten die met deze specifieke problematiek kampen is ontwikkeld, staat de aanpak dicht 'bij de werkvloer'. Net zoals bij de ontwikkeling van andere indexen en registraties is landelijke regie nodig, die er vooral op moet toezien dat de index niet voor andere doeleinden wordt gebruikt.

4.3. Registeren van levensovertuiging

In het oude stelsel van het Besluit bevolkingsboekhouding werd op de persoonskaart van een ingeschrevene diens geloof of levensovertuiging opgenomen. Dit gegeven kon op verzoek van betrokkene zelf worden verwijderd. Daarnaast werd de verstrekking van het gegeven aan instanties in de loop der tijd beperkt tot de kerkgenootschappen. Vanaf 1984 wordt dit gegeven niet meer opgenomen in de Gemeentelijke Basisadministratie (GBA). De bescherming van de persoonlijke levenssfeer verzette zich tegen de opneming van dit gegeven. Ook hadden instanties met een publiekrechtelijke taak geen behoefte aan dit gegeven. Voor kerkgenootschappen is de voorziening getroffen dat op basis van vrijwilligheid van de ingeschrevenen zelf een indicatie wordt geplaatst.

Art.17, tweede lid van de Wbp verbiedt registratie van godsdienst en levensovertuiging. Uitzonderingen zijn mogelijk. Zo geeft art.5 van de Wet politiegegevens aan dat registratie van "dit soort gegevens slechts plaats vindt in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is".

Een aantal burgemeesters is voorstander van registratie van levensovertuiging, om het beleid tegen radicalisering beter vorm te kunnen geven. Radicalisering is een containerbegrip waarin verschillende typen van gedrag bij elkaar worden gebracht. Zo focust de minister van Binnenlandse Zaken en Koninkrijksrelaties in het *Actieplan Polarisatie en Radicalisering* [7] op drie groepen; radicaliserende moslimjongeren, jongeren met extreemrechtse denkbeelden en dierenrechtactivisten.

Radicalisering is een gelaagd verschijnsel waarvan de oorzaken talrijk kunnen zijn. Een bepaalde religieuze opvatting kan daarbij een rol spelen, maar dat hoeft niet. Dierenrechtactvisme en extreem-rechtse denkbeelden zijn meestal niet gebaseerd op een geloof. Bij het meld- en adviespunt radicalisering in een gemeente komen meldingen binnen over concrete personen. Vaak is een melding over mogelijke radicalisering een heel verhaal over een persoon. Daarin zitten feiten maar ook beelden die kunnen gaan over levensovertuiging, religie of politieke ideologie. Op basis van een risicoanalyse kan advies worden gegeven of aan een interventie worden gewerkt.

[7] TK 2006-2007, II, 29 754, nr. 103, *Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer*, 27 augustus 2007.

Een levensovertuiging is, anders dan bij biometrische kenmerken, geen objectief gegeven. De medewerkers in de gemeenten kunnen slechts afgaan op “wat iemand zegt dat hij gelooft of vindt”. En iemands gedrag kan aanwijzingen geven of iemand een bepaalde levensovertuiging aanhangt. Ontkenning ervan door betrokkene is echter niet goed te weerleggen. De betrouwbaarheid van de registratie van iemands overtuiging is niet eenvoudig toetsbaar. Bovendien is het een momentopname. Het verhaal dat bij een melding binnenkomt, is feitelijk “een observatie”. In de strijd tegen radicalisering zou per geval scherp moeten worden beoordeeld of een dergelijke observatie wordt ondersteund door andere vergelijkbare verhalen of observaties. Daarvoor dient het casusoverleg bij het advies- en meldpunt op lokaal niveau. Er is naar het oordeel van de Commissie ruimte om in die gevallen via een zorgvuldige informatiestroom tussen gemeenten en (regionale en nationale) inlichtingendiensten informatie uit te wisselen. Daarom is geen aparte registratie op levensovertuiging nodig.

BIJLAGE 1: INSTELLINGSBESLUIT

De Minister van Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties;

Handelende in overeenstemming met het gevoelen van de ministerraad;

Gelet op artikel 6, eerste lid, van de Kaderwet adviescolleges;

Besluit

Artikel 1
Er is een Adviescommissie 'Veiligheid en persoonlijke levenssfeer', hierna te noemen: de commissie.

Artikel 2
De commissie heeft tot taak te adviseren over regulering van, voorlichting over, werkwijzen bij en indien nodig protocollisering van de omgang met persoonsgegevens, zodat deze de veiligheid van personen bevorderen.

De commissie onderzoekt:

- hoe mogelijke belemmeringen, die rechtshandhavers en hulpverleners ervaren bij hun werk in veiligheidsdomein en hulpverlening, weggenomen kunnen worden;
- hoe zowel de doelstellingen op het gebied van de persoonlijke levenssfeer als die op het gebied van veiligheid zo goed mogelijk in samenhang met elkaar verwerkelijkt kunnen worden;
- hoe technologische ontwikkelingen benut kunnen worden op de raakvlakken van bescherming van persoonlijke levenssfeer en veiligheid;
- de mogelijkheid van een overkoepelende visie op regulering en facilitering van de omgang met persoonsgegevens voor de publieke en private sfeer;
- hoe de bevindingen en adviezen van de commissie zich verhouden tot de internationaal-rechtelijke context.

N.B. lopende de werkzaamheden is de Commissie verzocht om in haar advies aandacht te geven aan twee actuele onderwerpen: kentekenherkenning met camera's en de registratie van etniciteit en levensovertuiging.

Artikel 3
1. Voorzitter, tevens lid, van de commissie is:
mevrouw mr. A.H. Brouwer-Korf.
2. De overige leden van de commissie zijn:
a. mevrouw prof. mr. C.P.M. Cleiren
b. de heer mr. L.K. Geluk
c. de heer mr. S. Harchaoui
d. de heer dr. E.P. De Jong
e. de heer mr. A.J.A.M. Nieuwenhuizen
f. mevrouw prof. mr. J.E.J. Prins
g. mevrouw J.G. Stam
h. mevrouw mr. E.H. Swaab

Artikel 4
Het secretariaat van de commissie wordt vervuld door ambtenaren van de ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties.

Artikel 5
1. De commissie brengt haar advies uit voor 1 november 2008 aan de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties.
2. Na het uitbrengen van haar advies is de commissie opgeheven.

Artikel 6
De archiefbescheiden van de commissie worden na haar opheffing of, zo de omstandigheden daartoe eerder aanleiding geven, zoveel eerder, overgebracht naar het archief van het ministerie van Justitie.

Artikel 7
De voorzitter van de commissie ontvangt overeenkomstig het Vergoedingenbesluit per vergadering € 310.
De leden van de commissie ontvangen overeenkomstig het Vergoedingenbesluit per vergadering € 235.

Artikel 8
Deze regeling treedt in werking met ingang van de tweede dag na dagtekening van de Staatscourant waarin zij wordt geplaatst en vervalt met ingang van 1 januari 2009.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

DE MINISTER VAN JUSTITIE,

E.M.H. Hirsch Ballin

DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES,

Mevrouw dr. G. ter Horst

TOELICHTING

1. De opdracht

De Adviescommissie ‘Veiligheid en persoonlijke levenssfeer’ wordt gevraagd te adviseren over de regulering van, voorlichting over, werkwijzen bij en indien nodig protocollisering van de omgang met persoonsgegevens, zodat deze de veiligheid van personen bevorderen.

Een belangrijke aanleiding voor de opdracht is gelegen in het Beleidsprogramma ‘*Samen werken, samen leven’*, waarin onder pijler V (*Veiligheid, stabiliteit en respect*) is opgenomen dat bij de aanpak van agressie, geweld en criminaliteit “het kabinet privacybelemmeringen voor betrokken beroepsgroepen aanpakt”.
Maar ook overigens hebben de bewindslieden behoefte aan een advies over hoe versterking van de veiligheid ten goede kan komen aan de persoonlijke levenssfeer en vice versa. De verwachting is dat nieuwe technologische mogelijkheden daarbij goede diensten kunnen bewijzen. Zo heeft ook - mede namens de ministers van Justitie en Defensie - de minister van Binnenlandse Zaken en Koninkrijksrelaties in reactie op het rapport *‘Data voor daadkracht’*, in een brief aan de Tweede Kamer van 30 augustus 2007 de Tweede Kamer bericht dat het kabinet een nieuwe visie op privacy en veiligheid zal ontwikkelen: “Onder meer het spanningsveld en de balans tussen veiligheid en privacy zullen onderwerp van onderzoek zijn, evenals de rol van technologie en internationale aspecten”.

2. Mogelijke belemmeringen bij rechtshandhavers en hulpverleners in veiligheidsdomein

De bescherming van de persoonlijke levenssfeer loopt dikwijls vanzelfsprekend gelijk op met de bescherming van de veiligheid. Immers, het waarborgen van ‘veiligheid’ heeft als resultaat dat de burger zich vrij kan bewegen en zich beschermd weet tegen externe bedreigingen en onrechtmatige of disproportionele inbreuken op lijf, eerbaarheid en goed. En maatregelen die de veiligheid bevorderen leiden dikwijls tevens tot verbeterde bescherming van de persoonlijke levenssfeer.

Dat neemt niet weg dat in beeldvorming, publiek en politiek debat de begrippen ‘veiligheid’ en ‘bescherming van de persoonlijke levenssfeer’ nogal eens tegenover elkaar komen te staan. Rechtshandhavers en hulpverleners in het veiligheidsdomein voelen zich soms beperkt door in ieder geval hun perceptie van de normen ter bescherming van de persoonlijke levenssfeer in

het bijzonder die van persoonsgegevens. Dat maakt het van belang na te gaan:

- of hun perceptie van de normen met betrekking tot persoonsgegevens juist is;
- welke belemmeringen het kabinet kan wegnemen om ervoor te zorgen dat hulpverleners in het veiligheidsdomein en mensen die werken aan preventie en rechtshandhaving gewoon hun werk kunnen doen en de bescherming van personen in relatie tot persoonsgegevens verder tot ontplooiing kunnen brengen;
- hoe het kabinet het stelsel van bescherming van persoonsgegevens zodanig kan inrichten, dat het optimaal aan de veiligheid van personen bijdraagt, mede in het licht van de te verwachten technologische ontwikkelingen.

3. Anticiperen op technologische ontwikkelingen

Gegevens zijn niet langer uitsluitend via een enkele database toegankelijk. Steeds gemakkelijker zijn gegevens bijeengebracht uit een groot aantal verschillende bronnen. Uit diverse bestanden worden virtuele databanken opgebouwd, die niet als entiteit herkenbaar en aan regulering onderworpen zijn. In het vrije verkeer van diensten en personen in een bovendien globaliserende context is sprake van een grote toename in het gebruik van web-technologie. Dit gaat vergezeld van een groei van (in ‘cookies’) opgeslagen informatie over personen en hun surfgedrag: hun voorkeuren, interesses en aankopen. Principes en voorwaarden die tot voor kort bruikbaar waren om de bescherming van persoongegevens te garanderen, schieten door deze virtualisering van gegevensopslag en gegevensverwerking in toenemende mate tekort. Dat roept verschillende vragen op:

- wat valt te verwachten van gecentraliseerde of juist gedecentraliseerde gegevensverwerking?
- stelt de miniaturisering van gegevensverwerking (ict-, nano- en chiptechnologieën) bijzondere eisen aan het stelsel van bescherming van persoonsgegevens?
- welke mogelijkheden bieden technologische ontwikkelingen voor burgers om preciezer en sneller op de hoogte te geraken van welke instantie over welke gegevens beschikt, welke andere instantie om die gegevens heeft gevraagd; en natuurlijk ook om die gegevens te kunnen controleren en corrigeren?
- wat zijn de gevolgen van het feit dat normering en handhaving (als gevolg van en met behulp van de technologie) samen komen te vallen voor ontwerpfase en normontwikkeling?

- is het vooral nodig om de bescherming van persoonsgegevens toe te spitsen op systeemontwerp en systeembouw? moeten de bescherming en beveiliging van persoonsgegevens bij het systeemontwerp worden genormeerd en moet de benodigde expertise in het ontwerpteam zijn vertegenwoordigd?
- kunnen elektronische gegevens eigenlijk wel écht worden gewist?
- welke gevolgen hebben technologische ontwikkelingen voor de persoonlijke levenssfeer in bredere zin van de burgers.

4. Anticiperen op veranderingen in internationale omgeving

Gewijzigde machtsverhoudingen binnen de Europese Unie zullen tegelijk zowel kansen scheppen als beperkingen opleggen aan de manier waarop wij in Nederland de bescherming van personen in relatie tot persoonsgegevens reguleren. De Europese regulering van zowel strafvordering – waaronder internationale samenwerking (Verdrag van Prüm) – als van verwerking van persoonsgegevens zullen met die drift in een stroomversnelling komen.

Welke tendensen tot harmonisatie in de sfeer van de strafvordering zijn te ontwaren en wat zijn daarvan dan de gevolgen voor verwerking van persoonsgegevens bij strafvordering in zowel internationaal als nationaal perspectief? Gaan de pijlers die respectievelijk toezien op strafvordering en bescherming persoonsgegevens elkaar versterken? Is harmonisatie van strafvorderlijke gegevensverwerking in de respectieve lidstaten tot welk niveau noodzakelijk en ook te verwachten? Welke koers willen we in nationaal en internationaal verband varen?

Vanzelfsprekend speelt in de internationale context gegevensverwerking die raakt aan de persoonlijke levenssfeer ook op andere terreinen dan alleen de strafvordering. Aanbestedende diensten zijn soms verplicht integriteitsgegevens te verzamelen over ondernemingen. Daarnaast is er de context van internationaal werkende bedrijven, waarbij de vraag speelt op welke wijze vorm gegeven wordt aan de gelding van nationale en EU-regelgeving

Het komt er vooral op aan de internationale context van bescherming van de veiligheid van personen en de veiligheid van persoonsgegevens op een hanteerbare manier te vertalen naar praktische handreikingen voor de koersbepaling.

5. Mogelijkheid van richtinggevend kader voor publieke en private sfeer

Werden de klassieke grondrechten ooit vooral in het leven geroepen als drempel tegen een potentieel almachtige en rond persoonsgegevens alwetende overheid, inmiddels kunnen

risico's bij de omgang met persoonsgegevens bepaald niet minder van private partijen afkomstig zijn. Gegevensopslag bij vervoerders (OV-chipkaart) of bij banken of verzekeringsmaatschappijen vragen om passende regulering van de verwerking en zeker ook de beveiliging van persoonsgegevens. En wellicht juist levert de uitwisseling van gegevens tussen private en publieke sfeer nog het grootste risico op.

Daarom is het aangewezen een kader te ontwikkelen voor de verwerking van persoonsgegevens, dat tegen de achtergrond van technologische ontwikkelingen en de internationale context richting geeft aan:

- de wijze waarop overheidsdiensten en private partijen – ook onderling – gegevens verzamelen, beheren, toegankelijk maken, gebruiken en uitwisselen. Daarbij moet ook aandacht worden geschonken aan de regulering van bewaartermijnen en de mogelijk verplichte bewaring van gegevens voor doelen die strekken tot preventie en rechtshandhaving zoals de bewaarplicht van telefoon- en internetproviders en verkeersgegevens bij cameratoezicht en banken;
- de wijze waarop een systeem voor de verwerking van persoonsgegevens in een specifieke situatie moet worden ontworpen: wie (van wie en door wie) mag wat (welke gegevens, welke technologie) verwerken, en waarom (subsidiariteit, proportionaliteit);
- het ontwerp van de beveiliging van systemen en van uitwisseling van gegevens
- en dat tevens een waardering geeft aan het beginsel van doelbinding van verwerking van persoonsgegevens en andere bestaande of te ontwerpen beginselen in hun verhouding tot de Europese privacyrichtlijn en het Databeschermingsverdrag van 1981.

DE MINISTER VAN JUSTITIE,

E.M.H. Hirsch Ballin

DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES,

Mevrouw dr. G. ter Horst

BIJLAGE 2: DE AUTEURS VAN HET RAPPORT

Mevrouw mr. A.H. Brouwer-Korf, voorzitter van de Commissie
Mevrouw Brouwer-Korf was tot 1 januari 2008 burgemeester van Utrecht. Daarvoor was zij burgemeester van Amersfoort (1994-1999) en Zutphen (1989-1994). Thans is zij onder meer lid van de Onderzoeksraad voor Veiligheid.

Mevrouw prof. mr. C.P.M. Cleiren
Mevrouw Cleiren is hoogleraar straf- en strafprocesrecht aan de Universiteit te Leiden. Zij is daar tevens voorzitter van het departement strafrecht en criminologie. Daarvoor was zij directeur-generaal Wetgeving, Rechtspleging en Rechtshandhaving bij het ministerie van Justitie.

De heer mr. L.K. Geluk
De heer Geluk is wethouder Jeugd, Gezin en Onderwijs in de gemeente Rotterdam. Voor zijn wethoudersloopbaan was de heer Geluk gemeenteraadslid te Rotterdam en deelgemeenteraadslid te Delfshaven. Hij werkte voor diverse advies- en consultancy-bureaus. De heer Geluk is sinds 1 januari 2009 ook lid van de Onderwijsraad.

De heer mr. S. Harchaoui
De heer Harchaoui is voorzitter van het Instituut voor Multiculturele Ontwikkeling, FORUM. Hij is tevens voorzitter van de Raad voor Maatschappelijke Ontwikkeling (RMO), een adviesraad van de regering. Ook had hij zitting in de TaskForce Jeugdwerkloosheid (2003-2007). De heer Harchaoui studeerde strafrecht en privaatrecht en was tot 2002 plaatsvervangend Officier van Justitie.

De heer dr. E.P. de Jong
De heer De Jong was van 2000 tot 2003 lid van de Raad van Bestuur van Achmea Holding NV. Voordien was hij voorzitter van de Raad van Bestuur van de Gak Groep NV (1996-2000) en president-directeur van het GAK (1987-1995). Vanaf 2003 is hij onder meer voorzitter van de Raad van Advies van de Sociale Verzekeringsbank

De heer mr. A.J.A.M. Nieuwenhuizen
De heer Nieuwenhuizen is sinds 2005 hoofdofficier van justitie bij het Landelijk Parket van het Openbaar Ministerie (internationale georganiseerde criminaliteit). Hiervoor bekleedde de heer Nieuwenhuizen diverse functies bij het Openbaar Ministerie, waaronder die plv. hoofdofficier bij het Landelijk Parket en officier eerste klasse.

Mevrouw prof. mr. J.E.J. Prins
Mevrouw Prins is raadslid bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Daarnaast is zij (sinds 1994) hoogleraar recht en informatisering aan de Universiteit van Tilburg. Zij was aldaar van 1994 tot 2006 voorzitter van TILT, het Tilburg Institute for Law, Technology and Society, dat zich richt op recht en regulering van nieuwe technologieën. Mevrouw Prins studeerde rechten en Slavische taal- en letterkunde aan de Rijksuniversiteit te Leiden.

Mevrouw J.G. Stam
Mevrouw Stam was van 2004 tot 2007 voorzitter van het College van Bestuur van de Politieacademie en Hoofdcommissaris van Politie. Vanaf 1998 was zij al

plaatsvervangend voorzitter. Daarvoor was zij voorzitter van de faculteit Gamma aan de Hanzehogeschool te Groningen. Thans is zij voorzitter van het programma ‘Politietop Divers, naar een duurzaam perspectief’.

Mevrouw mr. E.H. Swaab
Mevrouw Swaab is advocaat en sinds 2003 senior advisor bij Boekel De Nerée advocaten & notarissen. Zij is vanaf 1977 werkzaam bij dit kantoor (sinds 1985 als partner) en bekleedde daar diverse functies waaronder die van voorzitter van het bestuur en managing partner. Ook is zij voorzitter van de Raad voor Cultuur, het adviesorgaan van de regering op het gebied van kunst cultuur en media, en van het Nationaal Comité 4 en 5 mei.

BIJLAGE 3: DE GESPREKSPARTNERS VAN DE COMMISSIE

de heer E.H.L. Aarts, Philips Research en hoogleraar *design for ambient intelligence* TU Eindhoven

de heer P.J. Aalbosberg, korpschef IJsselland

de heer J.M.A. Berkvens, hoogleraar informatica en recht Radboud Universiteit Nijmegen en directeur Rabobank

de heer R.G.C. Bik, korpschef KLPD

de heer R. de Boer, publicist, programmamaker en researcher

de heer M. Bolhuis, European Policy Manager Benelux, Google

de heer S. Broekhuizen, Politieacademie Nederland

mevrouw M.R. Bruning, hoogleraar jeugdrecht, RU Leiden

de heer P. Deelman, korpschef Twente

mevrouw M.C.H. Donker, hoofd GGD Rotterdam-Rijnmond

de heer C.J. Heijsman, korpschef Utrecht

de heer F.C. Hoogewoning, adviseur korps Amsterdam-Amstelland

de heer J. Holvast, bureau Holvast & Partners

de heer M.J. van den Hoven, hoogleraar ICT en Ethiek, TU Delft

de heer G. Huijser van Rheenen, korpschef Zaanstreek-Waterland

de heer P.J. Hustinx, Europees Toezichthouder voor gegevensbescherming

de heer B. Jacobs, hoogleraar ICT Radboud Universiteit Nijmegen en TU Eindhoven

de heer J. Kohnstamm, voorzitter College bescherming persoonsgegevens

de heer R.F. Koorn, IT Advisory KPMG EDP Auditors NV

de heer A. Meijboom, korpschef Rotterdam-Rijnmond

mevrouw D.M.J.J. Monissen, directeur-generaal curatieve zorg ministerie van VWS

de heer G.M. Munnichs, Rathenau Instituut

de heer H. Moraal, procureur-generaal

mevrouw E. Prins, MKB-Nederland

mevrouw M. Rieback, faculteit informatica VU Amsterdam

de heer G.D. Rijken, lector Haagse Hogeschool ‘s-Gravenhage

de heer C.J.M. Schuyt, lid van de Raad van State

de heer I. Snellen, emeritus hoogleraar bestuurskunde Erasmus Universiteit

Rotterdam

mevrouw K. Spaink, publicist

mevrouw M. Stikker, directeur De Waag Society

de heer J.J.H. Suyver, voorzitter evaluatiecommissie antiterrorismemaatregelen

de heer J. van der Tak, burgemeester gemeente Westland

de heer J. Terstegge, privacyofficer Philips en commissie privacy VNO-NCW

de heer A.H. Vedder, hoofddocent TILT Tilburg

mevrouw R. Voss, hoofdinspecteur van de Inspectie van het Onderwijs;

mevrouw J.F. de Vries, hoofdinspecteur van de Inspectie jeugdzorg;

mevrouw H.H. de Vries, partner advocatenbureau Kennedy Van der Laan

de heer G. Wabeke, manager KPN

de heer P. Wierenga, CEO Philips Research

mevrouw Y. Wijnands, programmaministerie voor Jeugd en Gezin

BIJLAGE 4: SUMMARY

DO IT SIMPLY – SIMPLY DO IT,
to protect security and privacy

PROLOGUE

This opinion relates to security and privacy. Security and privacy – the terms *'personal life'*, and *'private life'* are used as synonyms – are increasingly interdependent, and in various situations, one is prerequisite for the other.
Sometimes, the relationship between these two is strained. The central message of this opinion is that the challenge of seeking a balance between security and protection of privacy must be addressed simply. We cannot run away from this challenge. And what we mean by simply is: not trying frenetically to do justice to both interests as far as possible when we have a situation, but try to be relaxed. The opinion therefore presents a framework to serve as guidance.

UNDER THE SPOTLIGHT

A normal area of policy

One of the key conclusions of this opinion is that the legal system has given virtually no guidance to those working on the ground about how to deal carefully with personal data for security purposes. Organisations where professionals are working on the security of persons have often left their professionals ill-equipped to put into practice the legal system for handling personal data. By 'professionals', the Committee means all those who carry out activities for the purpose of security. Some of them do this nearly all the time, such as the police, while others only do this as a subsidiary part of their job, such as staff working in mental health care or schools who sometimes observe security threats. Careful handling of privacy rules is not ingrained in the daily work of the organisations where these professionals are employed. The discussion about careful handling of personal data remains dominated by an almost exclusively legalistic approach. Starting out from this diagnosis, the Committee recommends treating the area where security and privacy meet as a normal policy area. That means a policy field in which considerations from different viewpoints are taken into account,

and sufficient attention is devoted to professional, technological and economic considerations. The key questions are:

- How to guarantee careful handling of personal data in their day-to-day work by professionals employed in fields where requirements are imposed in the interests of security?
- What facilities can organisations put at the disposal of their professionals to give them sufficient backing?
- Which mechanisms can be used to ensure that all parties – professionals, managers, administrators and politicians – live up to their responsibilities in seeking and achieving a balance between privacy and security?
- How can we incorporate privacy rules as effectively and as soon as possible into technical systems (*privacy by design*) and how can we encourage this "incorporation"?
- What can we do to encourage compliance?

The organisations concerned can start work immediately on facilitating the work of their professionals.

In order to bring about this transformation into a normal area of policy, the Committee is developing a reference framework for guidance. This framework is intended to contribute to rationality and consistency in decision-making, where tensions can arise between security and privacy ('prior evaluation'). The reference framework can serve as a source of inspiration in order to facilitate the daily work of professionals who work on security and privacy in a practical way. The framework is also a tool to alert those who have to implement decisions about handling personal data about vulnerabilities. Finally, the reference framework can serve as a tool for validating policy and legislation relating to privacy and security.

Principles for careful handling of personal data

A key starting point in the reference framework is: "keep it simple, facilitate and ensure that security and privacy are mutually reinforcing as far as possible."

The reference framework consists of six principles combined with relevant assistance:

1. 'Transparency, except ...';
2. 'Select before you collect';
3. ´If necessary for security, you must share´;
4. Ensure integrity of data, systems and action by users;

5. Ensure information and facilitation;
6. Ensure compliance and internal supervision.

With the principles and assistance proposed, the Commission recommends doing nothing more or less than what should have been done already: helping professionals in a simple way to build the necessary care in handling personal data into their daily work, and provide the necessary incentives to guarantee that.

Robust external supervision and enforcement

In order to lend weight to these principles and assistance, it is necessary that an independent external supervisor should be appointed. The supervisor must have a free hand, and have no involvement in advice, facilitation or information. Based on the major compliance risks and in conjunction with the development of self-regulation, the supervisor should draw up a programme for his work in a regular cycle. Whenever necessary, the supervisor should take enforcement action using instruments such as penalties, administrative pressure, naming and shaming and administrative fines.

Robust supervision means: subjecting the actual handling of personal information in the workplace to supervision based on tightly-focused prioritisation. Looking at how the collection and sharing of personal data happens in reality, and whether that is done in accordance with the rules. That means: not settling for assessing whether the paper-based reality of codes and regulations comply with legal obligations. It also entails: not just reacting to signals, but also delving pro-actively into what actually happens based on his own prioritisation, in order to contribute to the interaction between practice, rules and the interests and values enshrined in those rules.

In the current situation, the Board on protection of personal data carries out its supervisory tasks in addition to other tasks such as advising on legislation, validation of codes of conduct and regulations, information, mediation, complaints handling and international tasks. This situation is undesirable. The ability of external supervisors to do their job effectively and credibly benefits from having a free hand, and not having to carry out tasks like giving advice, information or facilitation.

THE BACKGROUND

Societal developments and the day-to-day work within which law enforcers and social workers have to make judgements about security and privacy. These judgements have become more complex. That is due to the demand for a risk-free society, new technological possibilities, the intertwining of private and public aims and funding, as well as international pressure in connection with fighting terrorism and organised crime. Citizens are finding it increasingly difficult to exercise oversight of what is done with personal data.

If anything has changed fundamentally in the field of information in the security field over the last ten years, it is the growth in the number of databases, the amount of information stored in them and the possibilities for searching those databases and sharing them with other organisations. Now that government policy is focusing on precautionary and preventive measures, new cooperative relationships are coming into existence between local authorities, police and the judicial authorities and parties who previously had involvement with security policy (network society).

Besides the advice about supervision and about being more specific, the Commission does not come to a recommendation to make wholesale changes to the legislation. The priority is to embed key concepts for careful handling of personal data into day-to-day work on or for the purpose of security, such as 'goal-linking', 'transparency and predictability' and 'subsidiarity and proportionality'. Therefore, it is necessary to facilitate the making of judgements in concrete cases, in a way that matches the interests at stake, and which is appropriate for the responsibilities and the work of the professionals making those judgements. For this reason too, it is best to devote more attention to responsibility for and compliance with the duty of care in handling personal data when working on security. This can concern all kinds of situations. It may concern a teacher who notices that one of his pupils frequently has bruises. Or an airline which wants to be able to serve a Halal meal without those passengers having to worry about being considered as potential terrorists. Or a mayor who releases or withholds the address of a convicted paedophile. Or maintaining a number plate registration system or not. Or about the desirability of introducing national electronic patient records.

PRESENTATION

The reference framework consists of 6 principles that are explained below.

1. ***'Transparency, unless ...''***

   Wherever handling personal data has become more complex and citizens are more and more dependant on the use made of their data, transparency is crucial. The principle

'transparency, unless ...' implies that, in principle, citizens must know who does what with their personal data. Even if this concerns the use of data within chains of organisations. This principle reinforces the endeavour to achieve a 'society of trust'. Provide information actively about the right to inspect, correct or, if necessary, object to data, contributes to the accuracy of the data. The Committee considers it important that (cooperating) organisations take the importance of transparency seriously and work hard to produce instruments that deliver that transparency. So they should work, among other things, immediately to remove unnecessary barriers that prevent citizens exercising their right to inspect and correct their data. The person who decides to process personal data and the person who actually does the processing are both responsible for the creation of 'transparency'. The Committee suggests that organisations consider appointing an official charged with implementing this principle.

2. ***'Select before you collect' and keep it simple***

With the principle "*select before you collect and keep it simple'*, the Committee intends to limit working with personal data to the essential minimum, and thus implement the open wording of Article 8, subsections e. and f. of the Privacy Act. Furthermore, the Committee advises the Cabinet in the light of this principle always to consider when introducing statutory regulations in the field of security and privacy whether a scope definition should be an option, and whether it is desirable.

3. ***'If necessary for security, you must share´,***

The Committee wants to give an emphatic signal to those working in this field: **if** risk assessment reveals that the security of individuals is actually threatened, and the sharing of information may eliminate that risk, personal data must be shared. The Committee advises the Cabinet to promote an arrangement where professionals working on security can turn to an external trusted person for their occupational group: a person in authority, who operates as a contact and sounding board with whom they can discuss doubts about their risk assessment or the necessity of sharing personal data. In the same way as the President of the Bar Association performs this function for lawyers.

The fact that processing of items of personal data is not allowed where a duty of confidentiality applies under a professional code of conduct or by law must not mean that in a concrete situation – for example, a psychiatrist who becomes aware of life-threatening circumstances on the part of or affecting those surrounding his

client, but withholds this knowledge. The Committee suggests making this principle more explicit in Article 9 of the Privacy Act.

4. ***Ensure integrity of data, systems and action by users***

   With this principle, it is essential, among other things, to overcome privacy risks when writing the specifications for the development of systems. The architecture of the technology determines what the system can do, as well as what the future options should be. Therefore, it is necessary to keep control of this. Privacy considerations can play a role in the development of technology without any problem. Smarter environments impose ever higher requirements on creating the necessary privacy guarantees. Appropriate expertise will have to be available in (putting out to tender of) development of ICT services.

5. ***Ensure information and facilitation***

   With this principle, standard codes and protocols for those working at grass roots level are essential. Development of good and best practices and simulations can contribute to embedding the interests of privacy in the day-to-day work of professionals, who are working on or in relation to security interests. Responsibility for the development of codes and good and best practices lies with the organisations handling personal data>. The authorities have an important role to play here.

6. ***Ensure compliance and internal supervision***

   This principle provides a permanent incentive within the organisation to bring considerations of privacy and security, including risk analyses and risk assessment up to an appropriate level and keep them there. It is necessary, in the view of the Committee, to appoint an official within each institution or within each company, with the authority necessary to enforce compliance. Depending on, among other things, the size of the organisation, this may be, but often will not, an official working only on this task. The Committee feels that it is worthwhile in larger organisations to appoint a '*Data Protection Officer*' with the necessary authority, as defined in the Privacy Act, to put into practice the policy on judgements and risk analyses than have to be made when security and privacy come into contact. This official can also lend weight to compliance with the policy agreed within the organization.

THE EPILOGUE

At the request of the principals, the opinion discusses two topical issues. The opinion makes two marginal comments using the reference framework:

- number-plate recognition cameras;
- registration of ethnicity/religion in crime-fighting and deradicalisation policy.

THE CLOAKROOM

The opinion also contains a number of recommendations spread throughout the text:

- Government campaigns like 'We are working on your security' should be supplemented by adding 'and your privacy';
- Investigate how development and establishment of privacy protection systems and standardisation and certification can contribute to building a bridge between what happens in practice and regulation in the field of security and privacy;
- Within government, ensure that there is sufficient expertise so that when systems are developed (or this is put out to tender), the interests of security are adequately taken into account;
- Ensure that in cases where government asks citizens for data, these citizens know that it is government that is asking for this information, even when the data reaches the government through private organisations; for example, this is important for air travel data: airlines collect passenger data to satisfy obligations imposed on them by government. It must be clear to citizens whether an obligation has been imposed by government, and it is government's job to make that clear.

BIJLAGE 5: AFKORTINGENLIJST

ANPR	Automatic Numberplate Recognition
Cbp	College bescherming persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
EKD	Elektronisch Kind Dossier
EPD	Elektronisch Patiënten Dossier
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden
ISO	International Organisation for Standardization
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
FG	Functionaris voor de Gegevensbescherming
FIOD-ECD	Fiscale inlichtingen- en opsporingsdienst – Economische controledienst
KLPD	Korps landelijke politiediensten
NCTb	Nationaal Coördinator Terrorismebestrijding
NEN	Nederlands centrum voor normalisatie
NIVRA	Koninklijk Nederlands Instituut van Registeraccountants
NOREA	Nederlandse Orde van Register EDP-Auditors
Pb EG	Publicatieblad van de Europese Gemeenschappen
PNR	Passenger Name Record Record in het bestand van een computerreserveringssysteem (CRS) dat informatie bevat over een reis geboekt voor een passagier of voor een groep passagiers die samen reizen
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
RFID	radio frequency identification
SISA	Stedelijk Instrument sluitende Aanpak
TILT	Tilburg Institute of Law, Technology, and Society
Stb.	Staatsblad
UWV	Uitvoeringsinstituut WerknemersVerzekeringen
VSN-nummer	Verwijsindex Servicenummer
Wbp	Wet bescherming persoonsgegevens

BIJLAGE 6: AANBEVELINGEN

1. De Commissie adviseert de ministers van Justitie en BZK het richtinggevende kader voor informatieverwerking bij veiligheid zoals gepresenteerd in hoofdstuk 3 van dit advies over te nemen en – om de implementatie ervan te bevorderen – het kader op te nemen in de Aanwijzingen voor de regelgeving. Overnemen van het richtinggevende kader zal eraan bijdragen dat bescherming van veiligheid en persoonlijke levenssfeer opgevat kan worden als een ‘normaal’ beleidsterrein waar naast juridische overwegingen ook professionele, economische en technologische invalshoeken betekenis hebben.
2. De Commissie adviseert de ministers van Justitie en BZK zorg te dragen voor robuust extern toezicht op de naleving en handhaving van de regels voor het omgaan met persoonsgegevens door een sterke en onafhankelijke toezichthouder, die alleen is belast met ‘toezicht houden en handhaven’.
3. De Commissie adviseert de overheid geregeld te heroverwegen of het verzamelen van gegevens aan een horizon gebonden moet worden.
4. De Commissie adviseert alle bij veiligheid betrokken organisaties direct van start te gaan met het heel concreet wegnemen van de huidige drempels voor burgers voor hun recht op inzage en correctie van hun gegevens.
5. De Commissie adviseert alle organisaties met functionarissen die werkzaamheden verrichten ten behoeve van veiligheid hun ‘professionals’ te faciliteren bij een zorgvuldige omgang met persoonsgegevens en hen de benodigde rugdekking te verschaffen.
6. De Commissie adviseert in iedere instelling of binnen ieder bedrijf een functionaris aan te wijzen die met voldoende gezag tot naleving van de zorgvuldigheidsnormen voor omgaan met persoonsgegevens kan aanzetten. Afhankelijk van onder meer de omvang van de organisatie zal dat soms wel, maar vaak ook niet een speciale functionaris zijn. De Commissie acht het in grotere organisaties de moeite waard een gezaghebbende *‘Functionaris voor de gegevensbescherming’* als bedoeld in de Wet bescherming persoonsgegevens aan te stellen om concreet handen en voeten te geven aan de afwegingen en risicoanalyses die gemaakt moeten worden wanneer veiligheid en privacy elkaar raken.
7. De Commissie adviseert overheidsorganisaties transparant te zijn over verplichtingen die zij soms private bedrijven oplegt om persoonsgegevens te verzamelen ten behoeve

van publieke doelen. Daarbij aan te geven met welk doel de persoonsgegevens worden verzameld, wat er met de gegevens gebeurt, hoe lang de gegevens bewaard worden en hoe de burger de gegevens kan controleren of (doen) verbeteren.

8. De Commissie adviseert opdrachtgevers en opdrachtnemers werk te maken van *'privacy by design'* en daartoe al in de allereerste plannen voor opdrachten en ontwerpen het privacybelang te verankeren bij het ontwerpen van systemen voor verwerking van persoonsgegevens.
9. De Commissie adviseert er voor te zorgen dat binnen de overheid de passende deskundigheid bij ICT-diensten beschikbaar is om privacybelangen meer geconcentreerde aandacht te geven.
10. De Commissie adviseert na te gaan of het privacybelang verankerd kan worden in 'zorgsystemen', mogelijk als onderdeel van andere zorgsystemen op het gebied van milieu, arbeidsomstandigheden. kwaliteit e.d. En hoe normalisatie en certificering van deze systemen er toe kan bijdragen een brug te slaan tussen praktijk en regelgeving op het gebied van veiligheid en persoonlijke levenssfeer. Wellicht kan certificering van een privacyzorgsysteem het 'privacybelang' tot een *'unique selling point'* maken voor de private sector.
11. De Commissie beveelt ten aanzien van kentekenherkenning met camera's aan om de beoogde doelen van dit instrument scherp te formuleren en van elkaar te scheiden en de transparantie en kenbaarheid van het gebruik van kentekenherkenning te verbeteren. Een landelijke standaard is daarbij dienstig.
12. De Commissie spreekt zich niet uit over de wenselijkheid van registratie van etniciteit. Wel adviseert de Commissie de politiek verantwoordelijken het richtinggevende kader te hanteren bij hun beslissing. De Commissie adviseert daarbij een onderscheid te maken tussen registratie voor beleidsinformatie en registratie voor individuele gevallen. De Commissie acht registratie van levensbeschouwing niet zinvol, mede omdat levensovertuiging geen objectief gegeven is.
13. De Commissie adviseert het er toe te leiden dat met recht overheidscampagnes zoals '*Wij werken aan uw veiligheid'* aangevuld kunnen worden met de toevoeging *'en aan uw privacy'* .