



Privacy en veiligheid

*Op zoek naar
een liberale balans*

**Wergroep Privacy en Veiligheid
VVD Den Haag**

april 2005



Inhoud

1	Inleiding	3
	<i>Aanleiding</i>	3
	<i>Doel</i>	3
	<i>Leeswijzer</i>	4
2	De maatschappelijke dynamiek rond privacy en veiligheid.....	6
	2.1 <i>Steeds meer gegevens digitaal opgeslagen</i>	6
	2.2 <i>Meer bevoegdheden tot inzage</i>	6
	2.3 <i>Uitwisseling van gegevens</i>	8
	2.4 <i>Slimmere overheid</i>	9
	2.5 <i>Weinig interesse burger voor privacy</i>	10
	2.6 <i>Samenvattend</i>	10
3	Principiële context	11
	3.1 <i>Privacy als essentieel onderdeel van de liberale democratie</i>	11
	3.2 <i>Privacy als grondrecht</i>	12
	3.3 <i>Wet- en regelgeving</i>	14
4	Toekomstbeelden.....	16
	4.1 <i>Kansen</i>	16
	4.2 <i>Bedreigingen</i>	18
5	Een liberale balans tussen privacy en veiligheid	20
	5.1 <i>De liberale beginselen</i>	20
	5.2 <i>Definitie begrippen</i>	20
	5.3 <i>De liberale beginselen toegepast op privacy en veiligheid</i>	21
	5.4 <i>Een liberaal toetsingskader</i>	25
	5.5 <i>Voorbeeld: één landelijke databank van criminelen</i>	25
6	Rol van de overheid.....	28
7	Het vinden van een balans in concrete situaties	31
8	Conclusie	33
	Bijlage 1 De liberale beginselen nader toegelicht	35



1 Inleiding

Aanleiding

Er lijkt relatief geruisloos een maatschappelijke dynamiek gaande te zijn, waarbij de balans tussen veiligheid en privacy steeds meer lijkt op te schuiven naar het belang van veiligheid. De toegenomen informatisering en snelle ontwikkelingen van de informatietechnologie bieden veel nieuwe mogelijkheden. Zo maakt informatietechnologie het mogelijk voor organisaties om onderling gegevens uit te wisselen, waardoor zij hun taken en doelstellingen beter kunnen realiseren. Meer specifiek is een trend waarneembaar, waarin enerzijds het gebruik van technologie wordt aangemoedigd om criminaliteit te bestrijden en anderzijds technologie wordt toegepast om criminele daden te begaan. Tegelijkertijd is de nasleep van 11 september 2001 nog altijd merkbaar, en is het gevoel van onveiligheid toegenomen.

Eén van de uitgangspunten van het liberale gedachtegoed is 'vrijheid'. De VVD is als geen andere partij een warm voorvechter van de bescherming van grondrechten. De grondrechten vormen immers één van de pijlers van onze moderne beschaving en rechtstaat. De bescherming en handhaving van de veiligheid is echter een ander belang, waarvoor de VVD zich traditiegetrouw hard maakt. Het evenwicht tussen deze twee waarden – privacy en veiligheid – is echter in het geding en dreigt ten koste van de bescherming van de persoonlijke levenssfeer naar veiligheid op te schuiven. Het is belangrijk dat de VVD een doordacht standpunt inneemt over de wijze waarop het evenwicht het beste kan worden bewaard.

Doel

In deze notitie wordt de wijze waarop privacybescherming kan worden gewaarborgd, terwijl tegelijkertijd veiligheid kan worden gerealiseerd, onderzocht. Het doel daarbij is te komen tot een doordacht standpunt over het waarborgen van veiligheid als één van de kerntaken van de overheid aan de ene kant en privacybescherming als één van de pijlers van de democratische rechtstaat aan de andere kant. Een standpunt waarmee de



VVD de eerstvolgende (Kamer)verkiezingen kan ingaan, en dat zou moeten worden opgenomen in het partijprogramma van de VVD.

Een ander doel is het vergroten van bewustzijn bij politici op landelijk, provinciaal en gemeentelijk niveau en het verspreiden van kennis en informatie om er voor te zorgen dat de discussies rond dit thema verder gaan dan het schetsen van karikaturen. Nog weer een ander doel is het aanreiken van instrumenten aan politici en beleidsmakers, zodat zij beter in staat zijn om een zorgvuldige afweging te maken bij beleidskeuzes waarin zowel privacy- als veiligheidsthema's aan de orde zijn. Uitgangspunt is dat privacybescherming en veiligheid hand in hand kunnen gaan en tegelijkertijd kunnen worden gerealiseerd, zonder dat het één ten koste gaat van het andere. Richtsnoer bij het creëren van een balans zijn de liberale beginselen.

Leeswijzer

Hierna wordt in hoofdstuk 2 de maatschappelijke dynamiek geschetst rond privacy en veiligheid. In hoofdstuk 3 wordt de meer principiële context beschreven. Ingegaan wordt op het privacybegrip als grondrecht, dat tevens een wezenlijk element vormt van de uitgangspunten van de liberale democratie. Tevens wordt in dit hoofdstuk het juridische kader kort aangestipt. Vervolgens wordt in hoofdstuk 4 een toekomstbeeld geschetst, waarbij zowel de kansen als de bedreigingen in kaart worden gebracht. In hoofdstuk 5 wordt dan de liberale balans tussen privacy en veiligheid aan de hand van de liberale beginselen gevormd en beschreven. Hoofdstuk 6 gaat nog kort in op de rol van de overheid waarbij suggesties worden gegeven voor een liberale rol van de overheid. Hoewel de liberale balans tussen privacy en veiligheid een principiële karakter draagt, is het belangrijk dat deze liberale balans in de dagelijkse praktijk waarin wetsvoorstellen, regelingen en beleid gemaakt en gecontroleerd worden, ook daadwerkelijk geconcretiseerd kan worden. Vandaar dat in hoofdstuk 7 een kort hoofdstuk is gewijd aan het vinden van een balans in concrete situaties. Hoofdstuk 8 bevat ten slotte een zogenaamde verklaring. Deze verklaring moet worden opgevat als een conclusie van de werkgroep en is tevens bedoeld voor diegenen die niet de gehele notitie willen lezen, maar toch een indruk willen krijgen hoe die liberale balans tussen privacy en veiligheid er uit kan zien. Die lezers die een



meer concrete indruk willen krijgen, worden verwezen naar hoofdstuk 5.4 en hoofdstuk 7.

Deze notitie is geschreven door de werkgroep privacy en veiligheid van de VVD Den Haag, in de periode van februari tot november 2004. De werkgroep is in februari 2004 van start gegaan. De resultaten van de werkzaamheden van deze werkgroep, die verwoord zijn in deze notitie, zijn voorgelegd aan de leden van de VVD. Zo is er onder meer een discussieavond in november van 2004 georganiseerd, waarin op de belangrijkste resultaten is ingegaan en waarin gediscussieerd is aan de hand van verschillende stellingen.

Aan de werkgroep namen deel Anne-Wil Duthler (voorzitter), Erik van der Heijden, Marian Luursema, Anand Sahti, Rudolph Tammes en Bart Vosmer.



2 De maatschappelijke dynamiek rond privacy en veiligheid

2.1 Steeds meer gegevens digitaal opgeslagen...

In de afgelopen vijftien jaar hebben we als burgers de gemakken van de informatietechnologie omarmd. Pinbetalingen, internet, e-mail, mobiele telefonie en digitale camera's zijn vrijwel niet meer weg te denken uit het dagelijks leven. Onze portemonnee zit vol met bonus- en klantenkaarten. Het gebruikmaken van deze nieuwe technologieën laat echter ook allerlei sporen na. Digitale gegevens zijn gemakkelijk op te slaan. Vele jaren na dato kunnen ergens in een digitaal bestand de gegevens staan van het telefoongesprek dat u op 3 november 2002 met uw schoonmoeder voerde en hoe lang dat gesprek duurde, of welke sites u op het internet heeft bezocht op 5 maart 2003 en welke aankopen u bij Albert Heijn deed op 16 december 2004. Kortom, digitale technologieën hebben er in de afgelopen jaren in sneltreinvaart voor gezorgd dat het soort en aantal gegevens dat over burgers is opgeslagen exponentieel is gegroeid.

2.2 Meer bevoegdheden tot inzage

Tegelijkertijd is er in de afgelopen jaren een grotere behoefte aan veiligheid en is terrorismebestrijding hoog op de politieke agenda gekomen. Dit heeft in de afgelopen tijd een veelheid aan beleidsvoornemens tot gevolg gehad op grond waarvan politie, justitie en inlichtingendiensten meer bevoegdheden krijgen tot het inzien van gegevensbestanden van burgers. Sinds 1 januari 2005 moet iedere Nederlander van 14 jaar en ouder zich legitimeren in de openbare ruimte, als de politie, opsporingsambtenaren of toezichthouders erom vragen. Volgens plannen van de minister van VWS zal binnenkort iedereen die in een ziekenhuis, polikliniek of eerstehulp post wil worden behandeld, zich moeten legitimeren - ook jongeren onder de 14.¹ Er worden voorbereidingen getroffen voor de invoering van een biometrisch paspoort

¹ Patiënt moet zich voortaan legitimeren NRC Handelsblad 14 augustus 2004.



met vingerafdruk en gelaatsscan.² Amerikaanse veiligheidsdiensten hebben sinds maart 2004 al rechtstreeks toegang tot databanken met passagiersgegevens van Europese maatschappijen die op de VS vliegen.³ En het kabinet bereidt in het kader van terreurbestrijding plannen voor om alle telefoontjes, internetinformatie en e-mail en sms-gegevens te bewaren, zodat die gegevens toegankelijk zijn voor justitie en politie. Cameratoezicht wordt inmiddels op allerlei plaatsen ingevoerd. Verder krijgt Nederland een 'mega-afluisterbasis' in Zoutkamp, waar de AIVD en MIVD berichtenverkeer gaan controleren.⁴

Er is ook een veelheid aan specifieke maatregelen in voorbereiding, met het oog op het bestrijden van terrorisme, het tegengaan van misdaad en het veiliger maken van onze samenleving. Er is inmiddels een wetsartikel in werking getreden dat voorschrijft dat personen die zijn veroordeeld voor een delict waarop maximaal vier jaar of meer gevangenisstraf staat, hun DNA moeten afstaan ten behoeve van een opsporingsdatabank. Justitie wil vaker foto's van verdachten verspreiden.⁵ Opsporingsambtenaren hebben op grond van de nieuwe Wet vorderen gegevens financiële sector sinds 1 juni 2004 meer bevoegdheden gekregen om gegevens op te vragen bij financiële instellingen. Verder heeft minister Donner onlangs voorgesteld om de Wet politieregisters aan te passen, zodat bij de politie de reeds beschikbare persoonsgegevens worden gekoppeld en centraal beschikbaar gemaakt.⁶ De Europese Commissie bepleit een geautomatiseerd register voor veroordeelde terroristen of personen die worden verdacht van het hebben van banden met terroristische groeperingen.⁷

Deze sterke uitbreiding van bevoegdheden voor politie en justitie hangt vaak samen met calamiteiten en incidenten waarin het is misgegaan, die dikwijls

² Scan en vingerafdruk op toekomstig paspoort, Volkskrant, 27 oktober 2004.

³ EP hekelt uitwisseling info met VS, *Financieele Dagblad*, 19 maart 2004.

⁴ Mega-afluisterbasis in strijd tegen terrorisme, *De Telegraaf*, 8 april 2004.

⁵ Justitie: meer foto's van verdachten verspreiden, NRC Handelsblad 21 augustus 2004.

⁶ Politie mag meer met persoonsgegevens, *ANP*.

⁷ Commissie bepleit terreurregister in EU, *Financieele Dagblad*, 19 maart 2004.



bijna automatisch leiden tot een roep om meer en strengere maatregelen. Een voorbeeld is dat politie en justitie naar aanleiding van de tbs-er op proefverlof die een Chinees meisje ontvoerde nu bevoegdheden krijgen om via gegevens over mobiel telefoonverkeer, financiële gegevens, inbeslagneming van poststukken en voorwerpen, doorzoeken van computers etc. achter de verblijfplaats van een ontsnapte tbs-er te komen. Verder bleek in 2004 dat een van seriemoorden verdachte persoon ondanks een veroordeling in Frankrijk voor pedofilie een baan als schoolopzichter in België had gekregen. Dit heeft inmiddels geleid tot een pleidooi voor een Europese databank met gegevens van veroordeelde pedoseksuelen.

Bestrijding van terrorisme en misdaad staat – terecht – hoog op de politieke agenda. Het belang van privacy krijgt bij al deze nieuwe maatregelen echter relatief weinig aandacht en lijkt het bij al deze maatregelen af te leggen tegen het belang van de veiligheid. Het lijkt erop dat deze ontwikkeling een eigen dynamiek heeft gekregen.

2.3 Uitwisseling van gegevens

Doordat veel overheidsinstanties hun gegevens in geautomatiseerde bestanden hebben staan, is het technisch eenvoudiger geworden om gegevens uit te wisselen tussen verschillende overheidsdiensten. Gegevensuitwisseling tussen overheidsdiensten is in de eerste plaats een manier om de uitoefening van toezicht door de overheid efficiënter te maken. Zo kunnen op grond van de in 2003 in werking getreden Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (kortweg Wet BIBOB) allerlei overheidsgegevensbestanden worden gecombineerd en kan daarmee een aanvraag voor een vergunning of subsidie van een dubieuze aanvrager worden afgewezen. Verder is onlangs besloten dat allerlei opsporings- en handhavingdiensten toegang krijgen tot UWV-gegevens om illegale arbeid en fraude beter te kunnen bestrijden. Door het koppelen van politiebestanden aan een apparaat voor verkeerscontroles (de zogenaamde Catch Ken) kan de Amsterdamse politie stelselmatig criminelen staande houden van wie het autokenteken bekend is. Eén van de Amsterdamse beroepscriminelen is zo vaak staande gehouden dat hij de stad de rug heeft toegekeerd.⁸ Ook de

⁸ Crimineel weggepest met Catch Ken, *NRC Handelsblad*, 12 juli 2004.



Rotterdamse 'patsersaanpak' valt in die categorie, waarbij het bezit van een kostbare auto of luxe huis voor de politie aanleiding is om de financiële handel en wandel van de eigenaar compleet door te lichten.⁹

Een woningcorporatie in Nijmegen is begonnen met het checken of potentiële huurders wel eens zijn opgepakt voor geweld, drugs of wapenbezit om verloedering van wijken tegen te gaan.¹⁰

2.4 Slimmere overheid

De behoefte om de overheid anders en slimmer te organiseren en overheidslasten en administratieve lasten voor burgers en bedrijfsleven te reduceren, leidt óók tot een ontwikkeling waar steeds meer gegevens van burgers worden gekoppeld. Zo krijgen Nederlanders een uniek persoonsnummer, het zogenaamde burgerservicenummer. Daarmee wordt de dienstverlening door de overheid eenvoudiger. Ook wordt het eenvoudiger om persoonsgegevens uit te wisselen en hoeven burgers nog maar eenmaal hun gegevens aan de overheid te verstrekken. Het is de bedoeling dat het nummer, dat is gebaseerd op het sofi-nummer, op 1 januari 2006 wordt ingevoerd.¹¹ Een samenwerkingsverband van de NS, Connexion en de gemeentelijk vervoerbedrijven van Amsterdam, Rotterdam en Den Haag streeft ernaar om de strippenkaart en het treinkaartje te vervangen door een OV-Chipkaart. Via deze kaart kan het reisgedrag van iedere passagier worden opgeslagen en geanalyseerd. Een anonieme versie van deze kaart wordt extra duur.

Ook waar het gaat om maatschappelijke en sociale problematiek is winst te behalen met koppeling van gegevensbestanden. De speciale commissaris voor jeugd- en jongerenbeleid Van Eyck pleit ervoor om informatie van politie, artsen en scholen over probleemjongeren te koppelen aan het sofi-nummer. Hulpverleners moeten inzage in die gegevens krijgen, zodat ze sneller kunnen ingrijpen als kinderen in de problemen komen. De gebrekkige beschikbaarheid

⁹ Patsers doelwit politie, *De Telegraaf*, 11 februari 2004.

¹⁰ Screening huurders Nijmegen succes, Teletekst, 25 januari 2005.

¹¹ Servicenummer voor burgers, *NRC Handelsblad*, 15 mei 2004.



van informatie staat hulp nu in de weg.¹² Jongeren moeten van nul tot 23 jaar continu in de gaten worden gehouden door consultatiebureaus, scholen en regionale meld- en coördinatiecentra voor schooluitvallers.¹³

2.5 Weinig interesse burger voor privacy

In vergelijking met de jaren zeventig en tachtig is de burger anders gaan denken over de bescherming van zijn privacybelang. De algemene redenering lijkt: "Wie niets te verbergen heeft, heeft ook niets te vrezen". De burger lijkt bereid te zijn een stukje van zijn privacy op te offeren als de veiligheid daarmee kan worden vergroot, als meer criminaliteit kan worden opgespoord en meer criminelen kunnen worden vervolgd. Ook lijkt de burger bereid te zijn zijn privacy op te geven als hij daar financiële of andere voordelen tegenover ziet staan.

2.6 Samenvattend

Er is een veelheid aan redenen om maatregelen te nemen om méér gegevens over burgers te verzamelen of de reeds bestaande gegevens te koppelen. De noodzaak voor de overheid om informatie te verzamelen over burgers en bedrijven wordt steeds vaker als vanzelfsprekend aangenomen. Deze tendens heeft de laatste tijd – in het licht van de toegenomen dreiging van terrorisme – steeds meer accent gekregen.

Het belang van privacy krijgt bij al deze maatregelen relatief weinig aandacht. De balans schuift langzamerhand steeds meer naar veiligheid op. Er worden steeds meer gegevens over burgers verzameld en gegevensbestanden worden steeds meer met elkaar gekoppeld. Hierbij lijkt sprake te zijn van een ontwikkeling die zich tamelijk geruisloos steeds verder voortzet. De pleitbezorgers van méér veiligheid zijn talrijker en invloedrijker dan de voorvechters van privacy. Bovendien is er een zekere onomkeerbaarheid van deze dynamiek. Ontkoppeling van gegevensbestanden, versnippering van registraties en beperking van politieële bevoegdheden is in de afgelopen jaren niet voorgekomen en lijkt ook niet waarschijnlijk.

¹² Voorstel: Probleemkind helpen door bundelen informatie, *Algemeen Dagblad*, 24 maart 2004.

¹³ Jongeren van nul tot 23 volgen, ANP november 2004



3 Principiële context

3.1 Privacy als essentieel onderdeel van de liberale democratie

In het vorige hoofdstuk zijn allerlei voorbeelden gegeven, waaruit kan worden afgeleid dat privacybescherming plaats lijkt te maken voor het belang van veiligheid. De vraag die gesteld moet worden is of privacybescherming inderdaad een essentieel onderdeel is van een liberale democratie of liberale rechtstaat, ervan uitgaande dat de inrichting van onze samenleving als liberale democratie nog steeds de meest wenselijke is.¹⁴ De liberale democratie of liberale rechtsstaat kan wel worden omschreven als de leer van de vrijheid van het individu en de soevereiniteit van het volk.¹⁵ Liberalisme en democratie hangen nauw met elkaar samen, maar zijn aparte begrippen. Politiek liberalisme kan worden gedefinieerd als een rechtsorde waarin het individu bepaalde grondrechten bezit die niet kunnen worden aangetast door de overheid. Fukuyama bijvoorbeeld definieert politiek liberalisme of de rechtstaatidee als de "rule of law" die bepaalde individuele rechten en vrijheden erkent als vrijgesteld van regeringscontrole. Kenmerkend voor het liberalisme is dat het recht op vrijheid van de mens beschermd wordt. Democratie is het universele recht om deel te hebben aan de politieke macht, het recht van alle burgers om te stemmen en te participeren in de politiek. Democratisch is een regime wanneer het gelegitimeerd wordt door de goedkeuring van de geregeerden. Cliteur geeft aan dat de rechtstaatidee altijd gehanteerd is als een 'counter-majoritarian' correctie op democratie. De rechtstaat is een wettelijk gereguleerde beperking van democratische beslissingsmacht.¹⁶

¹⁴ Hierover kunnen de meningen uiteraard verschillen. Zie bijvoorbeeld Francis Fukuyama, *Het einde van de geschiedenis van de laatste mens*, Contact 1999 en Paul Cliteur, *Tegen de decadentie. De democratische rechtstaat in verval*, Arbeiderspers 2004.

¹⁵ Zie F. Fukuyama, p. 68.

¹⁶ P. Cliteur, p. 140.



3.2 Privacy als grondrecht

Grondrechten behoren tot het "hogere recht", dat wil zeggen het recht waaraan een hogere status wordt verleend dan het recht van alledag en dat een speciale bescherming verdient.¹⁷ Grondrechten zijn vastgelegd in de Nederlandse grondwet. Vinden we het hogere recht in verdragen, dan spreken we doorgaans van mensenrechten. Het recht op privacybescherming is een voorbeeld van een grondrecht en een mensenrecht. Grondrechten kunnen op verschillende manieren worden gedefinieerd. In Nederland worden grondrechten wel onderscheiden naar klassieke grondrechten en sociale grondrechten. Voor het doel van deze notitie laten we de sociale grondrechten verder buiten beschouwing. De klassieke grondrechten zouden we verder naar Lord Bryce kunnen indelen naar burgerrechten (vrijstelling van controle op persoon en bezit van de burger), religieuze rechten (vrijstelling van controle op geloofsovertuiging en godsdienstoefening) en politieke rechten (vrijstelling van controle op zaken die niet zo duidelijk het welzijn van de gehele gemeenschap betreffen dat controle noodzakelijk is).¹⁸

Het is opvallend dat Bryce grondrechten vooral omschrijft als "vrijstelling van controle".

Het begrip "privacy" wordt zeer uiteenlopend omschreven.¹⁹ Blok omschrijft privacy als ontoegankelijkheid van de persoonlijke levenssfeer.²⁰ Het is volgens hem geen absoluut recht. Onder omstandigheden kan een ingreep in of inbreuk op de persoonlijke levenssfeer gerechtvaardigd zijn. Hij brengt privacy in verband met verschillende classificaties, te weten de classificaties:

- privacy als subjectief recht,

¹⁷ Zie P. Cliteur, p. 99.

¹⁸ Zie de verwijzing op F. Fukuyama, p. 68

¹⁹ Een groot deel van deze subparagraaf is ontleend aan A.W. Duthler, *Digitale identiteit en pseudonieme digitale certificaten*, Sdu Uitgevers: 2004.

²⁰ P.H. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlands en Amerikaanse recht*, Den Haag: Boom Juridische Uitgevers 2002, p. 278.



- privacy als recht *in rem*,²¹
- privacy als persoonlijkheidsrecht en
- privacy als negatief recht.

Privacy als subjectief recht impliceert dat privacy een belang van een individueel rechtssubject is en dat het individu zelf mag beslissen over de bescherming van dat belang. Privacy als recht *in rem* houdt in dat privacy het genot van een bepaald goed beschermt en de betekenis van privacy niet contextafhankelijk is. Privacy als persoonlijkheidsrecht brengt met zich mee dat het door dit recht beschermde goed een onvervreemdbaar onderdeel is van de persoon en dat de waarde van dit goed van immateriële aard is. Privacy als negatief recht tenslotte, maakt duidelijk dat privacy een afweerrecht is en dat iedereen geacht wordt privacy te genieten, zolang men met rust wordt gelaten. Warren en Brandeis hebben het recht op privacy gelijkgesteld als *the right to be left alone*, dat door Cooley als een algemeen persoonlijkheidsrecht is gekwalificeerd.²² Warren en Brandeis zien het privacyrecht als een recht *in rem*. Het moet tegenover iedereen kunnen worden ingeroepen, en niet alleen tegen personen met wie een contractuele of quasi-contractuele verhouding bestaat. Het klassieke privacybegrip van Warren en Brandeis zag voornamelijk op binnendringing of openbaarmaking van het privéleven. Het klassieke privacybegrip was echter minder goed bruikbaar voor de ontwikkeling van een evenwichtig beoordelingskader voor de omgang met persoonsgegevens.²³ In de Verenigde Staten zijn daarom bijvoorbeeld de beginselen van behoorlijk gegevensbeheer ontwikkeld, die moeten garanderen dat de verwerking van persoonsgegevens zorgvuldig

²¹ Een recht *in rem* bekrachtigt een betrekking tussen een persoon en een goed, in plaats van een betrekking tussen personen onderling zoals de rechten *in personam* doen. Tegenover een recht *in rem* staan algemeen geldige plichten in plaats van plichten van een specifiek persoon zoals bij de rechten *in personam*. Zie Blok, p. 22.

²² S.D. Warren & L.D. Brandeis, 'The right to Privacy. The Implicit Made Explicit', *Harvard Law Review* 1890, p. 193-220. T.M. Cooley, *A Treatise on the Law of Torts, or, The Wrongs which Arise independent of Contract*, Chicago: Callagan 1879.

²³ Blok, p. 248.



verloopt en recht doet aan alle belangen van partijen.²⁴ Ook de Wet bescherming persoonsgegevens gaat van vergelijkbare beginselen uit, en beoogt een zorgvuldige verwerking van persoonsgegevens.²⁵

3.3 Wet- en regelgeving

Privacybescherming is een grondrecht dat met behulp van verschillende wetten en regels wordt beschermd. Er is een verandering waarneembaar van privacy als absoluut recht dat tegen iedereen kan worden ingebracht, zoals het recht om met rust te worden gelaten ("the right to be left alone") naar privacy als een relatief recht zoals het recht om te weten wat er met je gegevens gebeurt en wie de beschikking heeft over je gegevens ("controlling your personal data"). Deze verandering vinden we terug in vooral veel van de lagere wet- en regelgeving, die vooral betrekking heeft op privacybescherming als relatief recht.

Het juridische kader voor de bescherming van privacy of de persoonlijke levenssfeer bestaat uit verschillende richtlijnen, wetten en regelingen. Allereerst is er het Europees Verdrag voor de Rechten van de Mens (EVRM), het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR), de Europese privacyrichtlijn,²⁶ de ontwerp Europese richtlijn privacy en elektronische communicatie,²⁷ de Grondwet en de Wet bescherming persoonsgegevens. Daarnaast zijn er nog allerlei sectorspecifieke wet- en regelgeving, zoals de Wet Gemeentelijke Basisadministratie, de Wet Geneeskundige Behandelingsovereenkomst voor de zorgsector, en de SuWi-wet voor de sociale zekerheidssector. Voor zover de sectorspecifieke wet- en regelgeving relevante bepalingen bevatten voor dit onderzoek, worden zij in hoofdstuk 4 of 5 behandeld.

²⁴ Blok, p. 252.

²⁵ Zie artikel 6 Wbp: persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

²⁶ Europese richtlijn 95/46/EG, *PbEG*, 1995 L281-31.

²⁷ Europese richtlijn 2002/58/EG.



Belangrijke uitgangspunten van de geldende privacywet- en regelgeving zijn naast zorgvuldigheid en transparantie, proportionaliteit en subsidiariteit. Proportionaliteit houdt in dat een inbreuk op de belangen van een bij een verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Subsidiariteit houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden bereikt. Men dient dus af te zien van de verwerking van persoonsgegevens indien hetzelfde doel ook langs andere weg en met minder ingrijpende middelen kan worden gerealiseerd, bijvoorbeeld door het verzamelen van anonieme gegevens. Wordt desondanks tot gegevensverwerking overgegaan, dan is van belang dat degene die gegevens wil verwerken in redelijkheid alle bestaande mogelijkheden benut om de inbreuk op de persoonlijke levenssfeer van betrokkenen te beperken.²⁸

²⁸ T.F.M. Hooghiemstra, *Teksten en toelichting op de Wet bescherming persoonsgegevens*, Lelystad: Koninklijke Vermande 2001, p. 17.



4 Toekomstbeelden

In de vorige hoofdstukken hebben we gezien dat er een maatschappelijke dynamiek op gang is gekomen, waarbij steeds meer gegevens over burgers worden verzameld en deze gegevensbestanden steeds vaker worden gekoppeld. Redenen hiervoor liggen in misdaad- en terreurbestrijding, reductie van administratieve lasten, een efficiëntere organisatie van de overheid en betere uitoefening van toezicht.

In de toekomst zullen technologische mogelijkheden tot het verzamelen van gegevens alleen maar toenemen. Voortschrijdende technologie (internet, mobiele telefonie, DNA, satelliet, digitale camera, biometrie, radio frequency identification), leidt tot het beschikbaar komen van meer en nieuwe gegevens, die door de overheid kunnen worden verzameld. DNA-techniek maakt het mogelijk om ook bepaalde uiterlijke kenmerken vast te stellen. Automatisering maakt het gemakkelijker om gegevens die vroeger slechts met zeer veel moeite te verzamelen waren, met één druk op de knop uit de printer te laten rollen. Dataminingtechnieken worden steeds geavanceerder.

De kans bestaat dat van deze technologische mogelijkheden daadwerkelijk gebruik zal worden gemaakt in de strijd tegen terrorisme, om veiligheidsbelangen te behartigen, de overheid efficiënter te maken en administratieve lasten te verminderen. Dat zou betekenen dat er in de toekomst nóg meer gegevens over burgers worden verzameld en gebruikt. Een scenario is zelfs denkbaar waarin steeds meer uitwisseling van gegevensbestanden tussen overheidsorganisaties plaatsvindt en uiteindelijk één mega-gegevensbestand over alle Nederlandse burgers en organisaties ontstaat.

In dit hoofdstuk doen wij een poging om een toekomstbeeld te schetsen, waarbij wij de kansen en bedreigingen aangeven.

4.1 Kansen

Nederland kent een grote hoeveelheid inspectiediensten en toezichhoudende instanties. Niettemin heeft in het openbaar bestuur in de afgelopen jaren een



ontwikkeling plaatsgevonden waarbij sectorale inspecties werden samengevoegd tot grotere – departementsbrede - inspectiediensten.

In de uitvoering van het toezicht is er een trend waarneembaar waarbij toezicht steeds meer “risk-based” wordt vormgegeven. Burgers en bedrijven worden daarbij niet meer als één homogene massa beschouwd, maar ingedeeld naar risicoprofiel. Om de beperkte inspectie- en toezichtscapaciteit zo efficiënt mogelijk in te zetten, worden prioriteiten bij de uitoefening van het toezicht voornamelijk geconcentreerd op de toezichtssubjecten met het hoogste risicoprofiel. Zo heeft de Arbeidsinspectie een systematiek voor risico-analyse ontwikkeld, teneinde te kunnen ‘vissen waar vis zit’. De aanpak van de veelplegers is een ander voorbeeld. Dit sluit ook beter aan bij het rechtvaardigheidsgevoel van de burger.

Wanneer toezichthoudende instanties nog meer met elkaar gaan samenwerken en informatie- en gegevensbestanden gaan uitwisselen of zelfs gaan fuseren, zal dit toezicht nog efficiënter kunnen worden georganiseerd. ‘Brave burgers’ zullen dan relatief met rust worden gelaten, maar wanneer een ondernemer heeft geknoeid met zijn belastingaangifte zal hij ook al snel een bezoekje krijgen van de Arbeidsinspectie, de Keuringsdienst van Waren, ambtenaren van Bouw- en woningtoezicht, de Brandweerinspectie etc. Uiteindelijk kan dit het nalevingsgedrag op alle fronten verhogen.

Meer koppeling van gegevensbestanden, er vanuit gaande dat de betrouwbaarheid, kwaliteit en integriteit van de gegevens gegarandeerd kan worden, biedt allerlei voordelen. Er wordt een hoger niveau van naleving bereikt, doordat de pakkans groter is, er treedt maatschappelijk kostenbesparing op doordat er minder fraude en diefstal plaatsvindt, de overheid kan efficiënter werken waardoor uitvoeringslasten omlaag kunnen. Burgers worden eerlijker behandeld door de overheid. Bovendien kan de overheid pro-actiever optreden en burgers beter informeren. Door efficiënt gebruik van gegevens kan zij burgers informeren dat zij recht hebben op huursubsidie en dergelijke. Dit draagt bij aan gelijkheid in de samenleving. Bovendien kan de overheid de gegevens ook inzetten in het kader van beleidsinformatie en daarmee beter en effectiever beleid maken.



4.2 Bedreigingen

Overbodig om te noemen is dat de keerzijde van de hierboven geschetste ontwikkelingen is dat deze ten koste kunnen gaan van de privacybelangen van burgers. Bij bijvoorbeeld koppeling van gegevensbestanden geldt niet dat één en één twee is. Al heel snel ontstaat na koppeling van gegevensbestanden een vrij compleet beeld van mensen. Is dat niet een te grote inbreuk op onze vrijheid? Willen we wel dat de overheid zich bevoogdend gaat opstellen? Vinden we het wel leuk dat naamloze ambtenaren inzicht hebben in ons hele hebben en houden? Willen we eigenlijk wel dat burgers worden gedwongen zich als heilige robots te gedragen? Is het niet verstikkend als we nooit meer anoniem kunnen zijn? Hoe lang moet een misstap iemand worden nagedragen? Levert dit alles nog wel een leuke samenleving op om in te leven?

Vergissingen kunnen nooit geheel worden uitgesloten. De in te zetten technologie kan gevoelig zijn voor hackers, hetgeen misbruik, identiteitsfraude of chantage kan opleveren. Informatie kan uitlekken. Er kan stigmatisering van bepaalde bevolkingsgroepen ontstaan. En hoe krachtiger een instrument, hoe groter de schade die ermee kan worden aangericht wanneer er iets fout gaat. Door de automatisering ontstaat een steeds groter risico dat grote gegevensbestanden uitlekken of 'op straat belanden'. In verkeerde handen kan verschrikkelijk misbruik worden gemaakt van een bestand dat alle gegevens over alle burgers bevat. Ook kunnen bevoegdheden of gegevensbestanden worden misbruikt. Denk aan het relatief onschuldige voorbeeld van politieagenten die een eigen onderzoekje naar hun burens plegen, of naar het nieuwe vriendje van hun dochter.

Bovendien moet bij het schetsen van een doembeeld niet worden vergeten dat zich in het horizontale domein – dat wil zeggen het domein burgers – burgers, burgers – bedrijven en bedrijven – bedrijven - ook allerlei consequenties voor privacy kunnen optreden. Ouders controleren via een verborgen camera hun babysitter. Zogenaamde videobloggers houden een dagboek bij van hun leven door het vanuit hun eigen perspectief te filmen. In die films figureren echter ook anderen, die geen toestemming hebben gegeven om te worden gefilmd. Ondernemers zetten zwarte lijsten met wanbetalers op het internet. Verder zien we dat van personen die om één of andere reden plotseling bekend worden de informatie die over hen op het



internet staat op veel meer belangstelling kan rekenen dan toen zij nog anonieme burgers waren. Foto's of filmpjes van privésituaties uit gestolen camera's worden op het internet gezet, waartegen de rechtmatige eigenaar feitelijk niets kan beginnen. In de toekomst zullen mensen via private DNA-laboratoria en een gebruikt koffiekopje vaderschapstesten kunnen uitvoeren. Wellicht zullen werkgevers zelfs kunnen gaan testen of een sollicitant misschien een erfelijke ziekte heeft. De nieuwe Google-diensten zijn niet alleen commercieel interessant. Voor inlichtingendiensten, die sinds de aanslagen van 11 september 2001 ruimere bevoegdheden hebben om gegevens te vergaren, is Google straks een goudmijn. Aan de hand van het cookie²⁹, het ip-adres³⁰ en de inhoud van Gmail³¹ kunnen zeer gedetailleerde persoonlijke profielen opgesteld worden. Natuurlijk zegt Google in reactie op kritische vragen de privacy van gebruikers te respecteren. Volgens de Amerikaanse wetgeving heeft Google echter veel ruimte om gegevens van klanten te koppelen en door te verkopen aan andere bedrijven. Een privacystatement mag ook elk moment worden veranderd.

²⁹ Een cookie is een stukje tekst dat automatisch door de beheerder van een website naar een bezoeker wordt gestuurd. Met deze tekst wordt de bezoeker herkend waardoor de site informatie van deze bezoeker kan ophalen.

Deze informatie kan o.a. gebruikt worden om de bezoeker te helpen bij de navigatie op de site.

³⁰ IP staat voor internet protocol.

³¹ Gmail is een e-mail service van Google. Dit is een gratis e-mail service met o.a. als voorwaarde dat de klant akkoord gaat met persoonsgebonden advertenties op basis van het zoekgedrag en interesses van de klant.



5 Een liberale balans tussen privacy en veiligheid

5.1 De liberale beginselen

In de beginselverklaring van de Volkspartij voor Vrijheid en Democratie staan de beginselen vrijheid, verantwoordelijkheid, verdraagzaamheid, sociale gerechtigheid en de gelijkwaardigheid van alle mensen centraal. Artikel 1 van de Beginselverklaring van de VVD, vastgesteld in 1980, luidt:

"De grondslag van de VVD: De Volkspartij voor Vrijheid en Democratie staat als liberale partij open voor een ieder die de overtuiging heeft, dat vrijheid, verantwoordelijkheid, verdraagzaamheid, sociale gerechtigheid en de gelijkwaardigheid van alle mensen de fundamentele behoren te zijn van elke samenleving. De beginselen die uit deze overtuiging voortvloeien, aanvaardt zij als grondslag voor haar politiek."

In de bijlage bij deze notitie worden de beginselen nader toegelicht. Voordat deze beginselen worden toegepast op de begrippen privacy en veiligheid, wordt in de volgende paragraaf eerst een definitie gegeven van deze begrippen.

5.2 Definitie begrippen

Privacy en vooral veiligheid zijn brede begrippen. Een eenduidige (werk)definitie van deze begrippen is dus noodzakelijk.

Het recht op privacybescherming kan worden beschouwd als een uitwerking van het vrijheidsbeginsel. Het betreft dan de eerbiediging van de persoonlijke levenssfeer, zowel ten aanzien van het lichaam, van gegevens, van omgeving en dergelijke. Voor een nadere uitwerking van het privacybegrip wordt verwezen naar hoofdstuk 3.

Veiligheid is een begrip dat alleen in een maatschappelijke context kan worden geplaatst; daar waar interactie tussen individuen en omgeving plaatsvindt. Maximale veiligheid betekent dat men zich op een zo onbezorgd en onbelemmerd mogelijke manier vrij kan bewegen binnen de samenleving. Een minimalisatie van bedreigingen en gevaren als gevolg van daden van



anderen wordt zo veel mogelijk binnen de maatschappij gewaarborgd. Veiligheid kent zowel een subjectieve (emotionele) als een objectieve dimensie. Ten behoeve van maatschappelijke bruikbaarheid moet ernaar worden gestreefd het begrip zo objectiveerbaar mogelijk te behandelen.

Om iedereen een maximale veiligheid te kunnen garanderen zijn collectieve spelregels noodzakelijk. De persoonlijke veiligheid van een individu is immers direct afhankelijk van de interactie met zijn omgeving. Om collectief een maximale veiligheid te kunnen garanderen kan het nodig zijn dat men individueel een gedeelte van zijn vrijheden op moeten geven. Deze paradox zorgt voor een continu spanningsveld tussen veiligheid en privacy. Om maximale vrijheid te kunnen genieten moet men dus bereid zijn een deel van de persoonlijke vrijheid op te geven. Het is de vraag echter of het noodzakelijk en ook mogelijk is om maximale veiligheid te garanderen en welke consequenties dit heeft voor de persoonlijke vrijheid.

Zoals we hiervoor hebben gezien, heeft het privacybegrip alles te maken met vrijheid: een vrije levenssfeer, vrij van controle. Het veiligheidsbegrip lijkt alles te maken te hebben met ingrijpen in de vrije levenssfeer en het controleren van de persoonlijke levenssfeer. Bewust wordt het woord "lijkt" gebruikt, want het is maar de vraag of voor het creëren van een zo groot mogelijke veiligheid het ingrijpen en controleren echt noodzakelijk is.

De mogelijke consequentie van het volledig inperken van een grondrecht als privacybescherming kan een totaal gecontroleerde staat zijn. Als een grondrecht naar de definitie van Lord Bryce inhoudt dat het gaat om een recht "vrij van controle" betekent dit dat het inperken van een grondrecht het uitbreiden van controle met zich meebrengt.

5.3 De liberale beginselen toegepast op privacy en veiligheid

Tot welke inperkingen in de vrijheid leiden de liberale beginselen? Laten we aan de hand van de in 5.1 geschetste liberale beginselen nagaan tot hoever het ingrijpen in en controle van de vrije persoonlijke levenssfeer wenselijk lijkt.

Vrijheid

Uitgangspunt is dat mensen vrij zijn geboren en in beginsel alles moeten kunnen doen waarmee ze anderen geen schade toebrengen. Inperkingen in



die vrijheid moeten zeer goed kunnen worden onderbouwd. Het beginsel van vrijheid leidt er toe dat alle maatregelen op het terrein van veiligheid ook moeten worden beschouwd vanuit het perspectief van de consequenties voor de vrijheid van de burger.

Het handhaven van de rechtsstaat en van een democratisch staatsbestel vormt een onmisbare voorwaarde voor de vrijheidsbeleving van burgers.³² Het handhaven en het beschermen van het privacyrecht vormt daarmee ook een onmisbare voorwaarde voor de vrijheidsbeleving van burgers. Maar ook het treffen van veiligheidsmaatregelen kan onmisbaar zijn om de vrijheid of vrijheidsbeleving van burgers te garanderen. Het treffen van veiligheidsmaatregelen brengt echter vaak een uitbreiding van controle en daarmee een inperking van de vrijheid met zich mee. Daarom moeten te treffen veiligheidsmaatregelen altijd worden afgewogen tegen de mate waarin inbreuk op de vrijheid wordt gemaakt. Voorop staat immers dat de VVD staat voor vrijheid en democratie en niet voor veiligheid en democratie.

Een uitvloeisel van dit vrijheidsbeginsel dat vaak als uitgangspunt van het liberalisme en meer in het bijzonder van de VVD is gehanteerd is het zo weinig mogelijk ingrijpen door de overheid in het maatschappelijk speelveld. Op dit punt gaan wij in hoofdstuk 6 dat gaat over de rol van de overheid en in de aanbevelingen nog nader in.

Verantwoordelijkheid

Verantwoordelijkheid houdt in dat een ieder vrij is zijn of haar keuzes te maken, maar daarvan ook de consequenties behoort te dragen. Omdat niet iedereen in staat is met deze verantwoordelijkheid om te gaan en omdat de individuele percepties over verantwoordelijkheid uiteenlopen, dienen collectieve spelregels overeengekomen te worden. In deze geldt aldus het belang van de grootste gemene deler ('grootste geluk voor het grootste aantal mensen').³³ Dit rechtvaardigt dat in bepaalde gevallen van overheidswege kan worden toegetreden tot de individuele levenssfeer om te controleren en/of te sanctioneren. Omdat het niet mogelijk is en wellicht ook

³² Zie beginsel 9 van de Beginselverklaring van de VVD.

³³ Naar J. Bentham.



niet wenselijk is gericht alle 'potentiële overtreders' uit te filteren of te benaderen, is het soms onontkoombaar dat ook collectieve privacyschendende maatregelen genomen worden. Hierbij kan gedacht worden aan preventief fouilleren van alle reizigers alvorens een vliegtuig wordt betreden.

Verdraagzaamheid

In een denkbeeldige maatschappij waarin ieder individu over een oneindige verdraagzaamheid zou beschikken, zou eenieder vrijwillig bereid zijn de eigen vrijheid te beperken omwille van anderen. Daarmee wordt de noodzaak bij anderen weggenomen om 'jouw vrijheid' aan te tasten. Dit is echter een utopie. We leven nu eenmaal in een maatschappij waarin verdraagzaamheid beperkt is.

Een beperkte verdraagzaamheid of onverdraagzaamheid kan echter leiden tot de aantasting van de vrijheid en veiligheid van anderen. Als de mate van onverdraagzaamheid toeneemt wordt de bereidwilligheid van de een om de vrijheid van de ander te respecteren minder. Dit kan leiden tot een wederzijds versterkend effect.

Zoals in de Beginselverklaring valt te lezen en eerder is geciteerd, is verdraagzaamheid onverbrekkelijk verbonden met het begrip vrijheid. De ware vrije mens laat ook anderen vrij in geloofsbelijdenis, levensbeschouwing, meningsuiting en gedrag; hij erkent de mogelijkheid van overheidsingrijpen indien de grenzen van het maatschappelijk toelaatbare worden overschreden. Mensen kunnen slechts in gemeenschapsverband leven. De uit dit gemeenschapsverband voortvloeiende gebondenheid is geen beperking van de vrijheid, maar een onmisbare voorwaarde om de vrijheid van iedereen te verzekeren. Zo kan het treffen van veiligheidsmaatregelen noodzakelijk zijn om de vrijheid van iedereen te verzekeren. Bij het bepalen van deze maatregelen zal echter steeds het waarborgen van een zo groot mogelijke geestelijke, staatkundige en maatschappelijke vrijheid voor allen voorop moeten staan.

Sociale Gerechtigheid

Sociale gerechtigheid dient door de overheid te worden bevorderd door het scheppen van gelijke kansen voor iedereen en het verstrekken van bijstand aan hen, die deze nodig hebben. In de maatschappij bestaan nu eenmaal



ongelijke voorwaarden en ongelijke mogelijkheden voor individuele burgers. Deze ongelijkheid moet zoveel mogelijk worden opgeheven. Gelijke ontwikkeling- en ontplooiingskansen voor iedereen is vanouds een liberaal verlangen. Het zijn liberalen geweest die begonnen zijn met de bouw van de sociale wetgeving. Om sociale gerechtigheid te realiseren kan het soms nodig zijn om maatregelen te treffen die een inbreuk op de persoonlijke levenssfeer met zich meebrengen. Voor een effectieve uitvoering van en ter voorkoming van misbruik van de Bijstandswet of Wet werk en bijstand kan dit bijvoorbeeld noodzakelijk zijn. Om voor een ieder een rechtvaardig gebruik van collectieve middelen in te schatten is bepaalde basisinformatie over personen benodigd. Ook bij het treffen van maatregelen ter waarborging van veiligheid zou rekening kunnen worden gehouden met de maatschappelijke positie van individuen. Eenieder heeft evenveel recht op veiligheid maar niet iedereen kan dit even goed voor zichzelf bewerkstelligen. Een oude dame zal zich in een tram sneller onveilig voelen dan een jongeman, omdat zij minder makkelijk voor haar eigen belang kan opkomen.

Gelijkwaardigheid

Mensen zijn niet gelijk, wel gelijkwaardig. Een ieder dient de mogelijkheid te hebben zich naar eigen kunnen en wil te ontplooien. Daarom is het ook zo belangrijk dat privacyinbreuken zo beperkt mogelijk zijn en zo beperkt mogelijk van invloed zijn op de wijze waarop een ieder tegemoet wordt getreden in het maatschappelijke verkeer. Dit kan bereikt worden door gegevens niet langer te bewaren dan voor het doel noodzakelijk is, en slechts een beperkte gegevensset te bewaren. Ieder mens heeft recht op vrijheid in geestelijk, staatkundig en materieel opzicht ongeacht zijn geestelijke overtuiging, huidskleur, nationaliteit, seksuele geaardheid, geslacht of maatschappelijke positie.

Ondanks het feit dat mensen niet gelijk zijn en bijvoorbeeld verschillen als het gaat om maatschappelijke kansen, dient gewaarborgd te worden dat mensen gelijkwaardig worden behandeld. Eventuele privacybeperkende maatregelen dienen dan ook zo gelijkmatig mogelijk te worden toegepast. Voorkomen dient te worden dat een bepaalde individu een zwaardere inbreuk op zijn privacy moet ondergaan omdat hij afkomstig is uit een bepaalde sociale klasse of stratificatie. Tevens geldt dat alle individuen in een samenleving in gelijke mate recht hebben op veiligheid.



5.4 Een liberaal toetsingskader

Uit bovenstaande toetsing blijkt dat het voor een goed begrip noodzakelijk is de termen privacy en veiligheid in de liberale context van alle vijf beginselen te plaatsen.

Voor een goede analyse van maatschappelijke thema's vanuit een liberaal perspectief is het van belang te komen tot een toetsingskader. Dit valt uiteen in een aantal elementen die te allen tijde moeten worden meegenomen:

1. Toets aan alle vijf de uitgangspunten zoals hierboven geschetst en niet alleen aan de beginselen vrijheid en verantwoordelijkheid;
2. Streef naar zoveel mogelijk uitsluiten van emotionele subjectieve elementen en het zoveel mogelijk objectief (meetbaar) maken van de onderwerpen. Dit geldt zowel op het gebied van veiligheid (in plaats van het afgaan op percepties van onveiligheid kan bijvoorbeeld inzichtelijk gemaakt worden hoeveel inbraken er in een buurt plaatsvinden) als op het gebied van privacy die vaak op basis van emotionele argumenten overdreven wordt (het opslaan van een DNA-profiel hoeft minder impact te hebben dan veel mensen denken; technische oplossingen kunnen de emotionele argumenten van tafel schuiven door ervoor te zorgen dat genetische informatie niet afleidbaar is)
3. In alle gevallen zal bepaald moeten worden of het middel (de privacyschendende maatregel) in verhouding staat tot het doel (proportionaliteit);
4. In alle gevallen zal vastgesteld moeten worden of er een 'lichter' middel mogelijk is. Bijvoorbeeld cameratoezicht in plaats van fouilleren;
5. In alle gevallen zal bepaald moeten worden wat de meest specifieke aanpak is. Privacyschendende maatregelen moeten zich beperken tot zo min mogelijk individuen.

5.5 Voorbeeld: één landelijke databank van criminelen

Het liberale toetsingskader wordt hieronder aan de hand van een voorbeeld toegepast. Het toetsingskader dient als een soort checklist en heeft tot doel bij vraagstukken waarbij veiligheid en privacy een rol spelen eenvoudiger te kunnen bepalen hoe de liberale balans zou kunnen uitvallen.



Het voorbeeld betreft een maatregel om de gegevens van criminelen in één landelijke databank op te slaan, ten behoeve van opsporingsdoeleinden.

1. Toets aan de liberale beginselen

Hoewel in principe de vrijheid van een aantal personen wordt geschonden door het opnemen van hun gegevens in één centrale databank, kan vanuit het beginsel verantwoordelijkheid worden gelegitimeerd dat dit ten aanzien van bepaalde personen geschiedt. Vanuit het beginsel van de sociale gerechtigheid kan wel worden beredeneerd dat gegevens slechts voor een beperkte duur in een centrale databank worden opgeslagen. Aan het beginsel van gelijkwaardigheid wordt voldaan wanneer duidelijk wordt aangegeven dat deze maatregel geldt voor een specifiek gedefinieerde (algemene) groep vanwege specifieke redenen en zich niet louter richt op bepaalde individuen.

2. Meetbaarheid

Vanuit een liberaal perspectief zal moeten worden voorgesteld dat er duidelijke eisen worden gesteld aan de criteria op basis waarvan persoonsgegevens van bepaalde individuen worden opgenomen in één centrale database. Er zal dus bijvoorbeeld moeten worden gespecificeerd dat alleen mensen worden opgenomen in de database die een bepaald soort delicten hebben begaan of een bepaalde hoeveelheid tijd achter tralies hebben doorgebracht. Het kan niet zo zijn dat alle gegevens van alle personen in Nederland met een strafblad worden opgenomen.

Tevens zullen bij het voorstel voor een dergelijke maatregel meetbare (objectiveerbare) doelen moeten worden gesteld, zoals bijvoorbeeld een dalingspercentage van een bepaald soort criminaliteit in een bepaalde periode.

3. Doel/middel-relatie

Er zal duidelijk moeten worden aangegeven welk doel gaat worden gerealiseerd met het toepassen van het middel. In dit geval zal duidelijk moeten worden aangegeven dat met het opnemen van gegevens van bepaalde personen in één centrale database een x-percentag criminaliteit op een bepaald gebied kan worden voorkomen. Als het middel niet in verhouding staat tot het doel, is het middel vanuit liberaal perspectief niet acceptabel.



4. 'Lichter' middel mogelijk?

Er zal duidelijk moeten worden aangetoond of voor het bereiken van het doel geen lichtere maatregel mogelijk. De vraag zal moeten worden gesteld of het doel van het terugbrengen van een bepaald soort criminaliteit niet op een wijze kan worden gerealiseerd die bijvoorbeeld minder inbreuk maakt op de privacy van de personen waarop de maatregel betrekking heeft. In dit geval kan worden bekeken of minder gegevens van betrokken personen worden opgeslagen, bijvoorbeeld wel gegevens met betrekking tot een strafblad maar geen gegevens van de sociale dienst of medische gegevens.

5. Specificiteit

De groep waarop de maatregel betrekking heeft zal duidelijk moeten worden gespecificeerd. Er zal te allen tijde gekeken moeten worden of de maatregel zich niet kan beperken tot een meer afgebakende groep, zonder dat het doel in gevaar komt. Men zal dus in het geval van de centrale database niet alleen moeten kijken naar personen die een bepaald soort delicten hebben begaan maar bijvoorbeeld ook naar hoe vaak personen een dergelijk delict hebben begaan. Daaruit kan voortvloeien dat de groep personen waarop de maatregel betrekking heeft kan worden beperkt tot mensen die een bepaald delict vaker dan bijvoorbeeld twee keer gepleegd hebben.

Ten slotte zullen ook eisen gesteld moeten worden op het gebied van de doorlooptijd van een maatregel. Er zullen dus evaluatiemomenten ingebouwd moeten worden in het traject van uitvoering waarbij op basis van vastgestelde criteria wordt bepaald of een maatregel succesvol is en verder kan worden uitgevoerd of onvoldoende succes heeft en teruggedraaid dan wel herzien zal moeten worden.

Uit dit voorbeeld blijkt dat de voorgestelde maatregel op zich vanuit een liberaal perspectief kan worden onderschreven, mits kan worden gegarandeerd dat aan bepaalde randvoorwaarden of waarborgen wordt voldaan. Er zullen dus vanuit een liberaal toetsingskader eisen worden gesteld aan de doelen, de wijze van uitvoering en de kaders van een bepaalde maatregel.



6 Rol van de overheid

Het steeds verder koppelen van bestanden, het steeds langer bewaren van gegevens van burgers, het steeds verder uitbreiden van bevoegdheden van politie en justitie leidt tot het steeds verder ingrijpen van de staat in het particuliere leven van burgers. Dit past niet bij de visie van de VVD dat inmenging van de staat zo beperkt mogelijk moet zijn. Liberalen komen op voor het individu, zo staat te lezen in het Liberaal Manifest van 1981.

Daar waar het individu de staat ontmoet, is de staat almachtig.³⁴ De mogelijke consequentie van het volledig inperken van een grondrecht als privacybescherming kan een totaal gecontroleerde staat zijn. Er van uitgaande dat een grondrecht naar de definitie van Lord Bryce inhoudt dat het gaat om een recht "vrij van controle" betekent dit dat het inperken van een grondrecht het uitbreiden van controle met zich meebrengt. Het treffen van veiligheidsmaatregelen betekent ook vaak een uitbreiding van controle. De overheid dient er dan ook voor te waken dat de balans tussen de inbreuk op het grondrecht dat privacybescherming is, en het uitbreiden van controle ter versterking van de veiligheid, in evenwicht blijft.

Er is veelal geen 'natuurlijk portefeuillehouder', bewindspersoon of ministerie om de balans te bewaken tussen privacy en veiligheid. Uiteraard is er het College Bescherming Persoonsgegevens (CBP), dat er op toeziet dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd. Maar er is geen overkoepelend afwegingskader, waarlangs nieuwe voorstellen die een beperking van privacy met zich meebrengen in samenhang met elkaar worden gewogen. Een dergelijke visie is in het licht van de huidige maatschappelijke en toekomstige technologische ontwikkelingen zeer wenselijk.

Suggesties voor een liberale rol voor de overheid

Om de liberale balans tussen privacy en veiligheid beter te kunnen bewaken, worden hieronder suggesties gedaan voor de rol van de overheid.

³⁴ Zie pagina 3 van het Liberaal Manifest van 1981.



- Voor een goede balans tussen privacy en veiligheid is integraal beleid nodig. Daarom moet er één bewindspersoon worden aangewezen die verantwoordelijk wordt voor het bewaken van deze balans. Deze bewindspersoon heeft tot taak het totaaloverzicht en de samenhang tussen de maatregelen die in het kader van het overheidsbeleid voor veiligheid worden getroffen te bewaken en er voor te zorgen dat de inbreuk op de privacy zo beperkt mogelijk is.
- Hoewel burgers hun eigen verantwoordelijkheid hebben, moet de overheid burgers actief beschermen, ook waar het gaat om horizontale inbreuken op hun privacy. Met het laatste wordt bedoeld de inbreuken die door andere burgers of door bedrijven kan worden gemaakt.
- De overheid moet daarom investeren in voorlichting en educatie, om ervoor te zorgen dat mensen goed gaan nadenken over consequenties van verlies van privacy en ethische vraagstukken die daarmee samenhangen.
- De overheid moet pro-actief reageren op mogelijke uitwassen op het terrein van privacy in de informatiemaatschappij en daarom de handhaving van delicten als chantage, bespieding en misbruik van gegevens intensiveren. Strafhoogtes voor dit soort delicten moeten omhoog en er moet actief worden opgespoord en vervolgd.
- De Algemene Rekenkamer zou bij haar jaarlijkse controle niet alleen de naleving van de privacywetgeving moeten onderzoeken, maar ook een onderzoek moeten uitvoeren naar de balans tussen privacy en veiligheid.
- De overheid moet meer doen aan het onderzoeken van de effectiviteit van maatregelen, waarbij veiligheid zo objectief mogelijk meetbaar wordt gemaakt.
- De overheid moet pro-actiever nadenken over privacy en veiligheid. Technologische ontwikkelingen gaan vaak sneller dan wetgeving. Nu worden maatregelen veelal reactief genomen. De overheid moet zich al tevoren bezinnen op de technologische ontwikkelingen en de vraagstukken die daardoor mogelijk ontstaan, en daarop vooruitlopend een standpunt formuleren.

Bij voorstellen voor uitbreiding van bevoegdheden en instrumenten voor het verzamelen en verder verwerken van persoonsgegevens (waaronder het



koppelen), dient de verantwoordelijke bestuurder op niet vrijblijvende wijze aan te geven hoe gewaarborgd wordt dat de gegevens rechtmatig worden gebruikt.



7 Het vinden van een balans in concrete situaties

De afwegingen en conclusies die in deze notitie zijn verwoord, hebben ondanks de diverse praktische voorbeelden, een theoretisch en abstract karakter. Het is van belang dat deze afwegingen en conclusies ook vertaald kunnen worden naar concrete situaties. Het zijn immers de beslissingen in concrete situaties die tot het vinden van een uiteindelijke balans tussen veiligheid en privacy in onze huidige maatschappij moeten leiden.

De volgende vragen zouden kunnen worden gesteld bij het vinden van een balans in concrete situaties waarin maatregelen worden getroffen ter voorkoming, bestrijding en opsporing van criminaliteit en terrorisme

Word(en)t met deze maatregel(en) een inbreuk gemaakt op de persoonlijke levenssfeer of ook wel de privacy van een natuurlijke persoon?

1. Zo ja, is het vanuit het beginsel van verantwoordelijkheid gelegitimeerd dat dit ten aanzien van bepaalde personen geschiedt?³⁵
2. Leveren de maatregelen een aantoonbaar en meetbaar effectieve bijdrage aan het doel, in algemene termen, het verhogen van de veiligheid?
3. Zo ja, wordt de groep van personen op wier privacy inbreuk wordt gemaakt, zodanig gekozen dat aan het beginsel van gelijkwaardigheid wordt voldaan?³⁶
4. Zo ja, is het noodzakelijk voor het doel waarvoor de maatregel wordt getroffen, om een inbreuk op de persoonlijke levenssfeer te maken?

³⁵ Met andere woorden, is er een gerechtvaardigd doel voor het treffen van de maatregel? Het beginsel van verantwoordelijkheid kan met zich meebrengen dat maatregelen worden getroffen om collectieve belangen te behartigen. Deze collectieve belangen moeten de privacy inbreuk kunnen rechtvaardigen. Als het gaat om belangen van veiligheid, zal dat meestal het geval zijn.

³⁶ Wordt er door de selectie van personen waarop de maatregel wordt toegepast, geen ongerechtvaardigde of onnodige discriminatie gemaakt?



5. Zijn ook maatregelen voorstelbaar die een minder ingrijpende inbreuk op de persoonlijke levenssfeer maken?
6. Zijn er ook maatregelen voorstelbaar die inbreuk op de privacy van een kleinere groep van bepaalde personen maken?
7. Indien een inbreuk wordt gemaakt op de privacy, worden er maatregelen getroffen die de privacy inbreuk beperken?
8. Denk hierbij aan de volgende vragen:
 - a. Welke maatregelen worden getroffen om er voor te zorgen dat alleen die personen persoonsgegevens van anderen kunnen bekijken die ze echt nodig hebben voor hun taakuitoefening?
 - b. Welke maatregelen worden getroffen om er voor te zorgen dat de persoonsgegevens voldoende zijn beveiligd en dat de kwaliteit van de gegevens kan worden gegarandeerd?
 - c. Met kwaliteit bedoelen we juistheid en volledigheid van gegevens.
 - d. Zijn alle persoonsgegevens die worden gebruikt noodzakelijk voor het doel waarvoor ze worden gebruikt of kan met minder gegevens worden volstaan?
 - e. Worden persoonsgegevens niet langer bewaard dan noodzakelijk is voor het doel van de privacy inbreuk?
 - f. Hoe wordt gegarandeerd dat deze personen zorgvuldig met de persoonsgegevens omgaan?
 - g. Worden garanties ingebouwd om het effect van de privacyschendende maatregel na verloop van tijd te evalueren, en de maatregelen zonodig te herzien of te herroepen?



8 Conclusie

Hieronder worden de belangrijkste conclusies van deze notitie in tien punten samengevat.

1. Er is een trend waarneembaar, waarin steeds meer maatregelen worden getroffen ter voorkoming, bestrijding en opsporing van criminaliteit en terrorisme.
2. Deze maatregelen kunnen vaak een vergaande inbreuk op de persoonlijke levenssfeer van natuurlijke personen met zich meebrengen.
3. De VVD Den Haag onderschrijft het belang van het zo goed mogelijk beschermen van de veiligheid van burgers, bedrijven, instituties en gebouwen in Nederland.
4. Het recht op bescherming van de persoonlijke levenssfeer, of ook wel privacybescherming, is een grondrecht en betreft een essentieel onderdeel van de liberale democratie of liberale rechtsstaat. Het hangt tevens nauw samen met en is een uitwerking van één van de liberale beginselen van de VVD, namelijk het beginsel van vrijheid.
5. Het beginsel van vrijheid leidt er toe dat alle maatregelen die ter bescherming van de veiligheid worden getroffen, moeten worden beoordeeld vanuit het perspectief van de consequenties voor de vrijheid van de burger.
6. Het handhaven van de rechtstaat en van een democratisch staatsbestel – en daarmee het beschermen van het privacyrecht - vormt een onmisbare voorwaarde voor de vrijheidsbeleving van burgers.³⁷ Maar ook het treffen van veiligheidsmaatregelen kan onmisbaar zijn om de vrijheid of vrijheidsbeleving van burgers te garanderen. Het treffen van veiligheidsmaatregelen brengt echter vaak een uitbreiding van controle en daarmee een inperking van de vrijheid met zich mee. Daarom moeten te treffen veiligheidsmaatregelen altijd worden afgewogen tegen de mate

³⁷ Zie beginsel 9 van de Beginselverklaring van de VVD.



waarin inbreuk op de vrijheid wordt gemaakt. Voorop staat immers dat de VVD staat voor vrijheid en democratie en niet voor veiligheid en democratie.

7. Het waarborgen van veiligheid en het beschermen van privacy hoeven niet op gespannen voet met elkaar te staan. Veiligheid en privacybescherming kunnen tegelijkertijd worden gewaarborgd, mits een aantal uitgangspunten in acht worden genomen, zoals:
 - Veiligheidsmaatregelen moeten worden beoordeeld op de consequenties voor de vrijheid van de burger, en meer in het bijzonder voor het privacyrecht van de burger.³⁸
 - Veiligheidsmaatregelen die mogelijk van invloed zijn op de individuele vrijheid, moeten worden beoordeeld op effectiviteit van maatregelen, proportionaliteit en controleerbaarheid.
8. Het treffen van veiligheidsmaatregelen moet niet leiden tot een totaal gecontroleerde rechtstaat. Dat risico bestaat indien de veiligheidsmaatregelen niet in gezamenlijkheid en in samenhang worden gezien. De VVD Den Haag beveelt daarom aan om één bewindspersoon verantwoordelijk te maken voor het bewaken van de balans tussen veiligheid en privacy.
9. De overheid heeft tot taak de burger te wijzen op zijn privacyrecht en de instrumenten die hij heeft om dat privacyrecht uit te oefenen.
10. Alleen dan kan een liberale balans tussen veiligheid en privacy worden gecreëerd en kunnen de uitgangspunten van de liberale rechtsstaat in volle omvang worden gehandhaafd.

³⁸ Hiertoe heeft de VVD Den Haag in het vorige hoofdstuk een handreiking gedaan.



Bijlage 1 De liberale beginselen nader toegelicht

Hieronder worden de liberale beginselen van artikel 1 van de Beginselverklaring van de VVD nader toegelicht.

Vrijheid: Een zo groot mogelijke vrijheid van de mens, zowel in geestelijk, staatkundig als in materieel opzicht, is naar de mening van de VVD een onmisbare voorwaarde voor zijn ontplooiing. Deze vrijheid komt ieder mens toe zonder enige vorm van discriminatie. Bij het gebruiken van die vrijheid moet de mens zich verantwoordelijk weten voor zijn medemensen, die even zeer recht hebben op een zo groot mogelijke vrijheid. De vrijheid van één mag de vrijheid van de ander dus niet belemmeren. Daar ligt de grens. Tevens moet hij rekening houden met de belangen van toekomstige generaties.

Verantwoordelijkheid: Vrijheid is geen onbeperkte vrijheid. Volgens liberalen kan vrijheid slechts worden beleefd in het besef van verantwoordelijkheid. Individuele verantwoordelijkheid is een onderdeel van de menselijke waardigheid. Een mens behoort de gevolgen van zijn daden zelf te dragen. Het streven naar sociale gerechtigheid mag derhalve niet leiden tot verdwijning van het besef van die verantwoordelijkheid. Dit laat onverlet dat zij die zichzelf niet kunnen redden geholpen moeten worden.

Verdraagzaamheid: Verdraagzaamheid is onverbrekkelijk verbonden met het begrip vrijheid. De ware vrije mens laat ook anderen vrij in geloofsbelijdenis, levensbeschouwing, meningsuiting en gedrag; hij erkent de mogelijkheid van overheidsingrijpen indien de grenzen van het maatschappelijk toelaatbare worden overschreden. In groter verband geldt deze verdraagzaamheid ook ten opzichte van democratische minderheden en tussen geestelijke en sociale groepen onderling. Als consequentie hiervan verwerpt de VVD de klassenstrijd en de terreur van minderheden of meerderheden. Mensen kunnen slechts in gemeenschapsverband leven. De uit dit gemeenschapsverband voortvloeiende gebondenheid is geen beperking van de vrijheid, maar een onmisbare voorwaarde om de vrijheid van iedereen te verzekeren. Het is de taak van de overheid om mate en vorm van deze gebondenheid te bepalen. Hierbij zal



echter steeds het waarborgen van een zo groot mogelijke geestelijke, staatkundige en maatschappelijke vrijheid voor allen voorop moeten staan.

Sociale Gerechtigheid: Sociale gerechtigheid dient door de overheid te worden bevorderd door het scheppen van gelijke kansen voor iedereen en het verstrekken van bijstand aan hen, die deze nodig hebben. In de maatschappij bestaan nu eenmaal ongelijke voorwaarden en ongelijke mogelijkheden voor individuele burgers. Deze ongelijkheid moet zoveel mogelijk worden opgeheven. Gelijke ontwikkeling- en ontplooiingskansen voor iedereen is vanouds een liberaal verlangen. Het zijn liberalen geweest die begonnen zijn met de bouw van de sociale wetgeving.

Gelijkwaardigheid: Mensen zijn niet gelijk, wel gelijkwaardig. Een ieder dient de mogelijkheid te hebben zich naar eigen kunnen en wil te ontplooiën. Ieder mens heeft recht op vrijheid in geestelijk, staatkundig en materieel opzicht ongeacht zijn geestelijke overtuiging, huidskleur, nationaliteit, seksuele geaardheid, geslacht of maatschappelijke positie. Discriminatie is dan ook uit den boze.