Vrijheid en veiligheid in de digitale samenleving

Een agenda voor de toekomst

1. Inleiding

De voortschrijdende digitalisering van onze samenleving heeft gevolgen voor onze economie, voor onze veiligheid, voor de manier waarop we met elkaar omgaan en voor onze privacy. Zij biedt veel kansen, maar brengt ook kwetsbaarheden mee. Dit klonk niet alleen door in een motie van mevrouw Barth die op 29 oktober jl. tijdens de algemene politieke beschouwingen in de Eerste Kamer met brede steun is aangenomen.[1] Het was ook een belangrijk thema tijdens de behandeling van de begroting van Veiligheid en Justitie op 20 en 21 november jl.

De inzet van dit kabinet is gericht op een veilig digitaal domein, waarin kansen van digitalisering worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en de internetvrijheid zo optimaal mogelijk worden beschermd. Met het oog daarop heeft het kabinet eind oktober al de Nationale Cybersecurity Strategie 2 aan de Tweede Kamer aangeboden.[2] In lijn daarmee alsook ter uitvoering van de motie Barth gaan wij in deze notitie in op de invloed van allerlei technologische ontwikkelingen op onze veiligheid en vrijheid, in het bijzonder onze privacy. Het gaat hierbij vooral om ontwikkelingen op het terrein van de informatie- en communicatietechnologie (ICT).

Deze notitie beoogt een aanzet te zijn voor een verdergaand maatschappelijk debat over dit thema, waarin de overheid zich zal moeten herbezinnen op haar rol bij het beschermen en respecteren van de persoonlijke levenssfeer, ook in het digitale domein. Dit debat gaat echter niet alleen over het hoofd bieden aan bedreigingen, maar het debat biedt ook juist veel kansen om veiligheid, vrijheid en maatschappelijke groei op een hoogst mogelijk niveau samen te laten gaan.

In § 2 van deze notitie staan wij stil bij een aantal ontwikkelingen en bij de vraagstukken die deze oproepen. Zij leiden tot twee hoofdvragen, die wij in § 3 en § 4 van deze notitie willen beantwoorden:

1. Welke rol moet de overheid in het licht van de technologische ontwikkelingen spelen bij de bescherming van persoonsgegevens tegen schendingen door anderen? Hoe benut zij daarbij de kansen die deze ontwikkelingen haar bieden?
2. Hoe moet de overheid in het licht van de technologische ontwikkelingen bij de uitoefening van haar taken op het terrein van de veiligheid zèlf omgaan met persoonsgegevens? Hoe benut zij daarbij de kansen die deze ontwikkelingen haar bieden, om zowel haar informatiepositie te optimaliseren als recht te doen aan bescherming van de privacy en van persoonsgegevens?

De beantwoording van deze hoofdvragen mondt uit in een aantal actiepunten, die in § 5 zijn weergegeven in een overzicht.

Het thema van deze notitie is zo complex en dynamisch dat sommige vraagstukken nog verder doordacht moet worden. Dat impliceert dat de ontwikkelingen en vraagstukken die hierna aan de orde komen, niet nu al van een al omvattende definitieve reactie kunnen worden voorzien. De notitie vormt in die zin ook een agenda voor de toekomst. Vraagstukken die als onderdeel van deze agenda nog verdere doordenking vergen, benoemen wij aan het slot van § 2.

Deze notitie staat niet op zichzelf. Zij bouwt voort op het kabinetsstandpunt over het advies van de Commissie Veiligheid en persoonlijke levenssfeer, "Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer" (Commissie Brouwer-Korf)[3], op de Notitie privacybeleid die het toenmalige kabinet in 2011 heeft uitgebracht[4], op de motie-Franken uit datzelfde jaar[5] en op afspraken over privacybescherming in het regeerakkoord van het huidige kabinet[6]. Verder vertoont deze notitie raakvlakken met de kabinetsvisie op e-privacy die dit voorjaar is uitgebracht.[7]

---

[1] Kamerstukken I 2013-2014, 33750, E.
[2] Kamerstukken II 2013-2014, 26643, nr. 291.
[3] Kamerstukken II 2009-2010, 31051, nr. 5.
[4] Kamerstukken II 2010-2011, 32761, nr. 1.
[5] Kamerstukken I 2010-2011, 31051, D.
[6] Kamerstukken II 2012-2013, 33410, nr. 15, blz. 27.
[7] Kamerstukken II 2012-2013, 32761, nr. 49.

Weliswaar zijn de domeinen waarop deze notitie en de kabinetsvisie op e-privacy betrekking hebben verschillend (publieke veiligheid versus particuliere sector), maar staan beide stukken wel in het teken van relevante ontwikkelingen op technologisch vlak. Daarbij zijn in de kabinetsvisie op e-privacy de randvoorwaarden vastgelegd die in de relatie tussen burger en particulier bedrijfsleven gelden. Informatieverwerking door de overheid in relatie tot o.a. het recht op privacy komt op ook andere terreinen dan de veiligheid aan de orde in het Nationaal actieplan mensenrechten dat het kabinet onlangs heeft uitgebracht. Tot slot heeft de notitie uiteraard samenhang met de eerdergenoemde Nationale Cybersecurity Strategie 2.

Met deze notitie geven wij, in aanvulling op de Nationale Cybersecurity Strategie 2, uitvoering aan eerdergenoemde motie-Barth en aan de toezegging die is gedaan in de antwoorden op de kamervragen van de leden van de Tweede Kamer Schouw en Verhoeven over de Big Brother Award[8].

Deze notitie gaat niet in op het werk van de inlichtingen- en veiligheidsdiensten, omdat het kabinet separaat zijn standpunt zal uitbrengen naar aanleiding van het rapport van de Commissie Dessens, die de Wet op de inlichtingen- en veiligheidsdiensten heeft geëvalueerd[9], en nog in afwachting is van het rapport van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten naar dataverzameling door deze diensten.[10]

2. Ontwikkelingen rond technologie, veiligheid en privacy[11]

De cruciale rol die ICT en computers spelen in de samenleving, zorgt voor bijzondere kwetsbaarheden. ICT vormt de kern van onze huidige netwerksamenleving en is dan ook verantwoordelijk voor de interdependenties tussen de talloze systemen, computers, software, telecom-infrastructuur en apparaten, die door burgers en organisaties in publieke en private sector worden gebruikt. Er is geen deel meer van de samenleving dat zich aan het netwerk onttrekt zonder daarvan grote nadelen te ondervinden. Storingen binnen het netwerk kunnen dientengevolge grote gevolgen hebben.

Verstoringen, al dan niet door personen en organisaties met kwade bedoelingen, vormen een andere categorie dreigingen waarvoor ons soort netwerksamenleving zeer kwetsbaar is geworden. ICT kan, zoals alle technologie, ook voor strafbare zaken en andere verwerpelijke doeleinden worden gebruikt. Georganiseerde (cyber)misdaad, belastingontduiking en witwassen, terroristische netwerken, spionageactiviteiten van vreemde mogendheden, identiteitsfraude, onlusten, zoals in Berlijn, Stockholm, Parijs, London, en een massale ordeverstoring als in Haren hebben impact, omdat betrokkenen cyberspace en nieuwe media gebruiken en de bijzondere eigenschappen ervan vaardig benutten.

De kritiek vanuit de samenleving op politiek en overheid bij het managen en adresseren van dergelijke problemen is steeds vaker gericht op het ontbreken van vroege signalen, kennis, overzicht en inzicht. Waarom wisten we dit niet, waarom konden we dit niet zien aankomen, heeft geen wetenschapper dit voorspeld? De kritiek veronderstelt ten onrechte dat wij reeds over de kennis kunnen beschikken om problemen van deze orde het hoofd te bieden. Daarbij wordt ook uit het oog verloren dat de overheid niet in staat is alle risico's te beheersen.[12]

Deze nieuwe kwetsbaarheid van netwerksamenlevingen vraagt om een nieuwe wetenschap van de socio-technische systemen, waarvoor nu hier en daar de eerste bouwstenen worden aangedragen. Deze nieuwe wetenschap wordt gevoed met ongebruikelijk grote volumes data over mensen en

---

[8] Aanhangsel Handelingen II, 2013-2014, 211.

[9] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.html.

[10] Kamerstukken II 2012-2013, 30977, nr. 57.

[11] Voor deze paragraaf is dankbaar gebruik gemaakt van de inbreng van prof. dr. M.J. van den Hoven (TU Delft), gebaseerd op o.a.: Jeroen van den Hoven e.a., "FutureICT- The Road towards Ethical ICT", 2012 (http://arxiv.org/pdf/1210.8181v1.pdf) en Jeroen van den Hoven, "Innovatie als moreel concept" in: Mark Geels en Tim van Opijnen (red), Nederland in ideeën, 2013, blz. 318-320 . Voor een beeld van het relevante juridische kader wordt verwezen naar bijlage 1, voor een beeld van de relevante technologische ontwikkelingen naar bijlage 2.

[12] Zie ook kabinetsstandpunt op het WRR-rapport iOverheid, kamerstukken II 2011-2012, 26643, nr. 211, blz. 4.

hun gedrag. De sociale wetenschappen staan voor de uitdaging daarvan een optimaal gebruik te maken.

ICT vormt dus een belangrijk onderdeel van het probleem, maar biedt ook een onderdeel van de oplossing. Datzelfde samenstel van systemen waarin mensen, apparaten, software, organisatie en instituties verbonden zijn, legt zonder enige moeite vast wat er van seconde tot seconde gebeurt. *Social network sites, search engines, cloud computing, sensor networks*, *CCTV camera's*, *mobile computing*, *You Tube downloads and up-loads*, twitterberichten, betalingsverkeer, verkeersbewegingen en mobiele telefoongesprekken leveren steeds grotere data volumes. De hoeveelheid data in de wereld die per maand wordt gegenereerd, beslaat een stapel CD-Rom's tot aan de maan en terug. Dit is de eeuw van *Big Data*. Veel van deze informatie heeft op de een of andere manier betrekking op personen en hun gedrag. Overheidsdiensten beschikken over steeds meer en gevarieerdere soorten data van deze aard om de veiligheid te dienen. Verdere verbeteringen in het optreden van deze diensten kunnen alleen tot stand worden gebracht als we persoonsgegevens kunnen gebruiken zonder de belangen die onder de noemer "privacy" worden gevat, te schaden.

Het recht op bescherming van persoonsgegevens is vastgelegd in diverse internationale verdragen, in de Grondwet en in onder meer de Wet bescherming persoonsgegevens.[13] De bescherming daarvan is een immer terugkerend thema, omdat er aan de datacollectie nooit meer een eind zal komen en het in de toekomst ondersteund zal worden door steeds geavanceerdere ICT. Quantum-fysici verwachten op dit moment dat we over 15 jaar over quantum-computers kunnen beschikken. Deze quantum-computers zullen een onvoorstelbare rekenkracht hebben en met gemak de data die we tegen die tijd hebben verzameld in een oogwenk kunnen doorzoeken en verwerken op zoek naar patronen, samenhangen en wetmatigheden. Dat is het moment waarop de dataverzameling die nu in volle gang is, zich echt zal uitbetalen.

Overheidsdiensten die zich bezighouden met toezicht, opsporing en rechtshandhaving hebben goede redenen om de nieuwe mogelijkheden van ICT te benutten in het algemeen belang. Sommige van die diensten hebben mede tot taak de toegang van burgers tot publieke goederen te bewaken, terwijl burgers soms calculerend gedrag vertonen en zich als "free riders" opstellen. Zwartrijders gebruiken het openbaar vervoer, maar betalen hun kaartje niet. Als er teveel "free riders" komen, dan kunnen we deze diensten ten algemene nutte op den duur niet meer leveren. Access management wordt daarmee van groot belang. Identificatie en koppeling van bestanden maakt het "free riders" onmogelijk of zeer onaantrekkelijk om te proberen voordeel te genieten van een publiek goed.[14] Ten tweede, de overheid moet ook zorgen voor het opsporen en vervolgen van strafbare feiten, het handhaven van de openbare orde en het bevorderen van cybersecurity. Met behulp van de nieuwe mogelijkheden van ICT kunnen overheidsdiensten een optimale informatiepositie opbouwen om hun taken op die terreinen goed te kunnen uitvoeren. De groeiende technische mogelijkheden om grote hoeveelheden data te verzamelen en te verwerken, brengt ook de vraag met zich hoe de waarborgen voor de beveiliging en het gebruik van deze data gelijke tred kunnen houden.

Uit de dataprotectiewetgeving vloeien verschillende beginselen voort die voor de bescherming van persoonsgegevens van belang zijn, zoals doelbinding, kenbaarheid, voorzienbaarheid, proportionaliteit en subsidiariteit. Aan de hand daarvan kan in een concreet geval worden uitgemaakt in welke mate en op welke wijze bepaalde persoonsgegevens beschermd moeten worden. Het kan dienstig zijn bij de beoordeling daarvan ook nog andere principes te betrekken. Daarbij kan onder meer worden gedacht aan het belang van het voorkomen van (reputatie)schade, de economische waarde van persoonsgegevens en de contextuele integriteit, d.w.z het vermijden van het risico dat een gegeven in een andere context wordt gezet en daarmee een andere betekenis krijgt.[15]

Voor gegevensbescherming is ook innovatie van belang. Innovatie in de 21e eeuw gaat over meer dan functionele eisen als "harder, sneller, meer". "Veiliger, transparanter, duurzamer,

[13] Zie hierna in bijlage 1, juridisch kader.

[14] In Italië werd het bestand van de personen die een uitkering wegens blindheid genoten, ooit gekoppeld met het bestand van mensen die net hun rijbewijs hadden gehaald. De doorsnede van de twee verzamelingen was niet leeg en er werd een veelvoud bespaard aan uitkeringen van wat werd uitgegeven aan het schrijven van de software die de koppeling van de twee bestanden mogelijk maakte.

[15] Zie in dit verband ook: Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid, 2011, blz. 214-217.

rechtvaardiger" worden steeds belangrijker. In de toekomst hebben we nieuwe technologie nodig die ons in staat stelt aan meer van onze maatschappelijke verplichtingen aan burgers, milieu en toekomstige generaties te voldoen. Op die manier wordt innovatie een instrument voor maatschappelijke vooruitgang.

We hebben vaak te maken met meerdere verantwoordelijkheden, verplichtingen of waarden, die met elkaar verenigd moeten worden. Dat geldt ook voor vrijheid en veiligheid in een digitale samenleving. Dit vergt dat voortdurend gezocht moet worden naar wegen om èn de veiligheid van onze burgers èn hun persoonsgegevens te beschermen.[16] Innovatie kan hierbij helpen. Nu er een samenloop is van "big data" en "post 9/11 security denken", wordt duidelijk wat de impact daarvan is en ontstaat er ook buiten Europa vraag naar het in Europa ontwikkelde concept van "Privacy by design" en in Europa ontwikkelde "privacy respecting technologies" en "privacy enhancing technologies". Europa was een goede voedingsbodem voor de ontwikkeling van deze technologie, omdat beide verplichtingen serieus werden genomen, namelijk de slimme inzet van nieuwe ICT-functionaliteit in belang van de veiligheid van de burgers alsook de erkenning van het belang van respect voor de persoonlijke levenssfeer van diezelfde burgers. Verantwoorde innovaties veranderen de wereld op zodanige wijze dat we aan meer verplichtingen kunnen voldoen - economische groei en duurzaamheid, privacy en veiligheid – dan voorheen. Innovatie is in deze zin niet alleen een economische motor of een "nice to have", maar ook een morele verplichting, niet alleen van het bedrijfsleven, maar ook van de overheid. Als we vandaag de mogelijkheid hebben om door innovatie de wereld zo te veranderen dat we morgen een dilemma kunnen vermijden of aan meer verplichtingen kunnen voldoen dan vandaag, dan hebben we vandaag de morele plicht om te innoveren. Het concept van Maatschappelijk Verantwoord Innoveren (MVI), zoals dat door een aantal universiteiten is ontwikkeld, kan daaraan een nuttige bijdrage leveren.[17]

Voorgaande beschouwingen laten zich kernachtig samenvatten in het beeld dat de voortschrijdende digitalisering van de samenleving haar grote kansen op maatschappelijke groei biedt, maar haar tevens voor de grote uitdaging plaatst deze groei zo vorm te geven dat zij gepaard gaat met een adequate bescherming van de enorme hoeveelheid aan digitale gegevens. Voor de overheid mondt deze uitdaging in een tweetal hoofdvragen, waarop wij hierna in § 3 en § 4 zullen ingaan:

1. Welke rol moet de overheid in het licht van de technologische ontwikkelingen spelen bij de bescherming van gegevens tegen schendingen door anderen? Hoe benut zij daarbij de kansen die deze ontwikkelingen haar bieden?
2. Hoe moet de overheid in het licht van de technologische ontwikkelingen bij de uitoefening van haar taken op het terrein van de veiligheid zèlf omgaan met persoonsgegevens? Hoe benut zij daarbij de kansen die deze ontwikkelingen haar bieden, om zowel haar informatiepositie te optimaliseren als recht te doen aan bescherming van de persoonlijke levenssfeer?

In § 1 is al aangegeven dat de ontwikkelingen en vraagstukken die hier aan de orde zijn gekomen, op sommige punten nog verder doordacht zullen moeten worden. Het gaat daarbij vooralsnog om de volgende vragen:

1. Moeten we in deze tijd van "big data" voor de bescherming van persoonsgegevens op het terrein van de veiligheid niet een sterker onderscheid maken tussen toegang tot en gebruik van gegevens? Traditioneel ligt de nadruk bij gegevensbescherming op het eerste punt. Echter, in tijden van "big data" is het in veel situaties haast niet te doen om de toegang tot gegevens te beschermen en zal men sterker zijn toevlucht moeten nemen tot het reguleren van het gebruik van gegevens.
2. Hoe kan bij het gebruik van "big data" ervoor worden gezorgd dat het proces van "profiling" ten behoeve van de veiligheid voldoende transparant is? Het vermogen om uit een grote hoeveelheid aan digitale gegevens snel en precies relevante verschillen in kaart te brengen, vormt een belangrijk kenmerk van cyberspace. Daarbij verdient aandacht hoe transparant het

[16] Zie ook het kabinetsstandpunt naar aanleiding van het advies van de Commissie Veiligheid en persoonlijke levenssfeer (Commissie Brouwer-Korf), kamerstukken II 2009-2010, 31051, nr. 5, blz. 11-12.

[17] Maatschappelijk Verantwoord Innoveren betreft de opgave het publieke debat en resultaten van wetenschappelijk onderzoek te benutten om er overwegingen aan te ontlenen die gebruikt kunnen worden als randvoorwaarden voor de ontwikkeling van slimme ICT-oplossingen, die zowel onze veiligheid als ook onze privacy respecteren. Zie nader: http://www.nwo.nl/onderzoek-en-resultaten/programmas/maatschappelijk+verantwoord+innoveren.

proces van "profiling" is waarin personen worden gecategoriseerd en op grond daarvan bepaalde beslissingen worden genomen.[18]

3. Wat betekent de komst van quantum-computers voor het proces van gegevensverwerking ten behoeve van de veiligheid? Op welke wijze kunnen we zowel de mogelijkheden die deze computers bieden, goed benutten als een adequaat niveau van gegevensbescherming handhaven?

Bij de verdere gedachtenvorming over vragen als deze zullen wij, overeenkomstig de motie van het lid van de Tweede Kamer Segers[19], ook partijen van buiten betrekken. Daarbij valt onder meer te denken aan de Wetenschappelijke Raad voor het Regeringsbeleid. Wij zullen deze verdere gedachtenvorming, waar nodig, ook afstemmen op de inhoud van de brief die het kabinet voornemens is dit voorjaar aan de Tweede Kamer te sturen over "big data" en "profiling" in de relatie tussen de burger en het particuliere bedrijfsleven. Zodra de gedachtenvorming over één van deze vragen tot een afronding is gekomen en tot een kabinetsstandpunt heeft geleid, zullen wij de kamers daarover informeren.

3. De rol van de overheid bij gegevensbescherming

3.1 Cybersecurity

Het digitale domein is allengs een integraal onderdeel geworden van het dagelijks leven in Nederland. ICT is een belangrijke factor gebleken voor productiviteitsgroei en innovatiekracht. Binnen Europa is Nederland leidend in de wijze waarop wordt ingespeeld op technologische trends en het effectief gebruik van ICT middelen en -vaardigheden. Nederland is een internationaal internetknooppunt, heeft de meest competitieve internetmarkt ter wereld en een van de hoogste online gebruikersdichtheden.

Dankzij een innovatieve houding en de juiste condities behoort de Nederlandse digitale-infrastructuursector tot de top van de wereld. Door ondernemerschap, innovatief vermogen en actieve participatie in de internet-community, heeft Nederland een leidende rol in de wereldwijde digitale-infrastructuursector weten te bereiken. De markt voor internetdiensten is bovendien open en neutraal. Hierdoor is Nederland een aantrekkelijke (vestigings)locatie voor bedrijven in de digitale-infrastructuursector.[20]

De Minister van Veiligheid en Justitie heeft tot taak bij te dragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein en daarmee aan een veilige, open en stabiele informatiesamenleving ("cybersecurity"). Cybersecurity gaat zowel om veiligheid van ICT als om de veiligheid van daarin opgeslagen informatie. Uitval van ICT-gebaseerde diensten en processen kan grote maatschappelijke gevolgen hebben. Het beschermen van persoonsgegevens en andere gevoelige informatie is essentieel voor het vertrouwen dat partijen hebben in het digitale domein en daarmee voor de economische en maatschappelijke voordelen die digitalisering biedt.

We genereren steeds meer en nieuwe soorten data, die data zijn steeds beter doorzoekbaar en analyseerbaar. Dit schept zowel kansen als kwetsbaarheden. Nieuwe digitale technieken raken bovendien steeds meer verweven met onze fysieke en psychische privésfeer. Verdergaande vormen van gezichtsherkenning maar ook het aansturen van apparaten met hersengolven zijn daar voorbeelden van. Recent zijn wetenschappers erin geslaagd om een breinsignaal over het internet te sturen dat de hand van een collega aanstuurde die enkele kilometers verderop zat.[21]

De data die we genereren en over het internet sturen, vertellen dus steeds meer over wie we zijn en wat we doen. Dat heeft grote gevolgen voor hoe we aankijken tegen fundamentele rechten en waarden. Er zijn nieuwe afspraken nodig over wat we daadwerkelijk willen en moeten beschermen en welke rolverdeling we daarbij wenselijk vinden tussen overheid, bedrijfsleven en burger, zowel nationaal als internationaal.

---

[18] Zie ook: M. Hildebrandt, De rechtsstaat in cyberspace?, 2011, blz. 21.

[19] Kamerstukken II 2013-2014, 33750-VI, nr. 70.

[20] Deloitte, Digital Infrastructure in the Netherlands, The Third Mainport, 2013.

[21] http://news.nationalgeographic.com/news/2013/08/130829-mind-brain-control-robot-brainwave-eeg-3d-printing-music.

Recente onthullingen over heimelijke activiteiten van staten gericht op verwerven van informatie en de toenemende commerciële waarde van persoonlijke data, onderstrepen het belang van bewustzijn van informatiebeveiliging bij alle stakeholders, evenals de noodzaak tot het verhogen van de algehele weerbaarheid van onze vitale infrastructuur tegen alle vormen van digitale bedreigingen. De ontwikkelingen op dit terrein zullen zeer snel blijven gaan en onze respons zal flexibel genoeg moeten zijn om op actuele ontwikkelingen in te spelen.

Staten vormen vooral een dreiging in de vorm van diefstal van vertrouwelijke of concurrentie-gevoelige informatie ("cyberspionage"). Criminelen richten zich met name op digitale fraude en diefstal van informatie. Door de toegenomen complexiteit, afhankelijkheid en kwetsbaarheid van ICT-gebaseerde producten en diensten is de digitale weerbaarheid tegen deze en andere cyber-dreigingen nog onvoldoende.

Deze ontwikkelingen maken vervolgstappen in het realiseren van cybersecurity nodig. Om deze reden is in 2011 de eerste Nationale Cyber Security Strategie aan uw Kamer aangeboden en, gezien de snelle ontwikkelingen in het digitale domein, recent de tweede Nationale Cyber Security Strategie.

Cybersecurity kan niet geïsoleerd tot stand worden gebracht. Het zal in relatie moeten worden bezien met onderwerpen zoals fundamentele rechten en waarden en maatschappelijke groei. In de tweede Nationale Cybersecurity Strategie wordt een voorzet gegeven voor een nieuw governance-model waarmee de kansen die digitalisering onze samenleving biedt, volop worden benut, dreigingen het hoofd geboden en fundamentele rechten en waarden worden beschermd. Het uitgangspunt bij dat model is dat verantwoordelijkheden die in het fysieke domein gelden, ook in het digitale domein moeten worden genomen en dat alle partijen - dus overheid, maatschappelijke organisaties en bedrijfsleven - betrokken moeten worden als het om cybersecurity gaat. Er moet hierover een constante, open dialoog worden gevoerd tussen burgers, bedrijfsleven en overheid, zowel nationaal als internationaal.

Om de dialoog tussen burgers, bedrijfsleven en overheid te laten leiden naar een nieuw volwaardig niveau van cybersecurity zijn in het bijzonder de volgende drie sturingsdimensies van belang:
- (zelf)regulering,
- transparantie,
- kennisontwikkeling.

Van burgers wordt een zekere mate van zogeheten cyberhygiëne (het toepassen van de elementaire veiligheidsvereisten) en eigen verantwoordelijkheid verwacht. Van burgers kan echter niet langer worden verwacht dat ze de steeds complexere ICT-diensten en -producten, zoals aangeboden door grote internationale spelers, volledig kunnen doorgronden en beoordelen op veiligheids- en privacyaspecten. Hier ligt dan ook een duidelijke verantwoordelijkheid voor ICT-leveranciers en -producenten. "Security by design" en "Privacy by design" zouden meer dan nu standaard ontwerpbeginselen moeten zijn. Hier ligt bovendien een belangrijke kans voor het Nederlandse bedrijfsleven dat kan inspelen op de groeiende wens naar veilige producten die controle over de eigen data mogelijk maken. Het opstellen van internationale normen en standaarden voor "Security by design" en "Privacy by design", evenals het stimuleren van innovatie op dit terrein, zijn dan ook prioriteiten voor dit kabinet.

Aanbieders van ICT-netwerken en -diensten of andere op ICT gebaseerde diensten hebben een verantwoordelijkheid (zorgplicht) jegens hun klanten. Ook ICT-producten en -diensten moeten veilig zijn. Invulling van deze verantwoordelijkheid dient bij voorkeur door zelfregulering tot stand te komen. Bezien zal worden of dit in voldoende mate gebeurt of dat aanvullende vormen van toezicht of regulering nodig zijn. In het kader van de aanpak voor de bescherming van de vitale infrastructuur zal de overheid samen met vitale partijen in beeld brengen welke ICT-afhankelijke systemen, diensten en processen vitaal zijn. Hieraan is een programma gekoppeld dat op basis van risicoanalyse vereisten stelt aan de veiligheid hiervan.

De algemene verplichting om persoonsgegevens op een goede en zorgvuldige manier tegen verlies of tegen enige vorm van onrechtmatige verwerking te beveiligen, wordt versterkt in het thans al bij de Tweede Kamer aanhangige wetsvoorstel meldplicht datalekken.[22] In dit wetsvoorstel wordt voor personen en instanties die verantwoordelijk zijn voor verwerking van persoonsgegevens, de verplichting geïntroduceerd het College bescherming persoonsgegevens (Cbp) onverwijld in kennis

[22] Kamerstukken II 2012-2013, 33662, nrs. 1-3.

te stellen van een inbreuk op de beveiliging van gegevens waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens die door deze persoon of instantie worden verwerkt. Daarnaast dient in de meeste gevallen een melding aan de betrokkene te geschieden, indien de inbreuk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Het nalaten aan deze verplichtingen te voldoen kan worden gesanctioneerd met een bestuurlijke boete, op te leggen door het Cbp. De meldplicht moet bijdragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

Daarnaast wordt ingezet op het vergroten van de digitale weerbaarheid van overheid, burgers en bedrijfsleven. Dit door bewustwordingscampagnes, het vergroten van de digitale vaardigheden, onderzoek en innovatie en het ondersteunen van maatschappelijke initiatieven op dit terrein.

De overheid zal kortom een nadrukkelijker rol gaan spelen in het digitale domein. Enerzijds door zelf te investeren in de veiligheid van de eigen netwerken en systemen. Anderzijds door partijen bij elkaar te brengen en beschermend op te treden, als de veiligheid van bedrijven en burgers of fundamentele rechten en waarden worden bedreigd. Waar nodig zal kader- en normstellend worden opgetreden.

Maatregelen in het kader van cybersecurity vergen maatwerk. Dit maatwerk wordt vormgegeven door ze altijd te bezien in de bredere context van maatschappelijke groei en fundamentele rechten en waarden en door de maatregelen toe te snijden op het probleem dat ze moeten oplossen ("risk-based approach"). Een belangrijke bron hiervoor is het Cybersecuritybeeld Nederland dat jaarlijks wordt uitgebracht[23]. Dit beeld constateert dat de grootste dreiging uitgaat van staten en criminelen.

In het actieprogramma van de tweede Nationale Cybersecurity Strategie zijn reeds een aantal maatregelen voor de kortere termijn voorzien. Belangrijk daarbij zijn een versterkte aanpak op het terrein van digitale spionage, het verkennen van de mogelijkheden voor een eigen netwerk voor vitale diensten en processen en een versterking van ons cybersecurity onderwijs en onderzoek.

Het kabinet werkt, samen met de overige publieke en private partners, aan de op- en uitbouw van een Nationaal Detectie- en Responsnetwerk. Hard- en software zijn kwetsbaar; computers met besmette componenten of waar malware is binnengedrongen, worden ook ingezet voor spionage. Naast bewustwordingsprogramma's wordt gewerkt aan de ontwikkeling van een keurmerk voor veilige software.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft reeds toegezegd met ons in het kader van cybersecuritystrategieën te verkennen of een Nederlandse clouddienst mogelijk is. Aan deze toezegging zullen wij in 2014 nadere uitvoering geven.[24]

Om de pool van cybersecurity-experts te vergroten en de cybersecurityvaardigheden van gebruikers te versterken, slaan bedrijfsleven en overheid de handen ineen voor een beter aanbod van ICT-onderwijs binnen zowel het lager, hoger als professioneel onderwijs. Er zal een PPS-taskforce Cybersecurity Onderwijs worden ingesteld die zich richt op advisering over het cybersecurity-onderwijsaanbod. De taskforce richt zich onder meer op certificering en diplomering van informatiebeveiligers en het (verder) ontwikkelen van lesmodules.

Voor de middellange en langere termijn moet verder uitgedacht worden hoe we de controle over onze gevoelige en persoonlijke data kunnen versterken in een tijdperk waarin de interesse daarvoor en de waarde daarvan alleen maar zal toenemen. Traditionele instrumenten, zoals toezicht en regelgeving, kunnen hier een rol in spelen, maar zullen niet in alle gevallen een antwoord kunnen geven. Er moet ook aanhoudend worden geïnvesteerd in innovatieve oplossingen om de driehoek vrijheid, veiligheid en maatschappelijke groei optimale invulling te kunnen geven. De overheid kan dit niet alleen. Zij zal zich inzetten voor het vormen van nieuwe strategische coalities, nationaal en internationaal, die hier een rol kunnen spelen bij het vormgeven van een ook op de lange termijn open, vrij en veilig digitaal domein. De internationale cyberspace conferentie die wij in 2015 in Nederland organiseren en het EU voorzitterschap in 2016 zijn hier belangrijke mijlpalen in.

---

[23] Het laatste dateert van juli 2013. Zie kamerstukken II 2012-2013, 26643, nr. 285, bijlage.

[24] Zie ook Kamerstukken II 2013-2014, 30977, nr. 71, en motie Recourt c.s., Kamerstukken II 2013-14, 33750-VI, nr. 55.

3.2 Strafrecht en cybercrime

Naast de verhoging van de digitale weerbaarheid (zie § 3.1) is het van essentieel belang dat het strafrecht voldoende is toegesneden op de ontwikkelingen rond cybercrime. Voorkomen is beter dan genezen, maar daar waar nodig dient het openbaar ministerie over een adequaat juridisch instrumentarium te beschikken om burgers te beschermen tegen criminaliteit op het internet. Deze bescherming dient ook de privacy, omdat cybercriminelen het dikwijls hebben voorzien op de persoonsgegevens van burgers of omdat sommige mensen op andere wijze via internet de persoonlijke levenssfeer schaden.

Het wetsvoorstel computercriminaliteit III[25], dat wij binnenkort zullen indienen, beoogt de strafrechtelijke bescherming van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen verder te verbeteren. Met het voortschrijden van de informatie- en communicatietechnologie wordt het steeds eenvoudiger om gegevens uit een computer over te nemen en vervolgens op het internet te zetten. Daardoor kan het gebeuren dat vertrouwelijke gegevens snel worden verspreid en voor grote groepen mensen toegankelijk worden. Het is bovendien niet eenvoudig om via het internet verspreide gegevens daarvan volledig verwijderd te krijgen. De technologische ontwikkelingen nopen tot een verdere strafrechtelijke bescherming van gegevens. Het uit een computer overnemen van gegevens over personen, en die gegevens vervolgens op het internet zetten, zijn verwerpelijke gedragingen waartegen adequaat strafrechtelijk moet kunnen worden opgetreden, vooral met het oog op bescherming van de persoonlijke levenssfeer van degene wiens gegevens het betreft. Daarom wordt in de eerste plaats voorgesteld om het wederrechtelijk overnemen van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, strafbaar te stellen. Hiermee wordt een betere bescherming geboden tegen het overnemen van gegevens uit een geautomatiseerd werk, in die gevallen waarin de gegevens gekopieerd zijn en de rechthebbende dus de beschikking houdt over de gegevens. De rechthebbende heeft echter geen invloed op het gebruik dat vervolgens van de overgenomen gegevens kan worden gemaakt, waardoor hij benadeeld kan worden. In de tweede plaats wordt het strafbaar om niet-openbare gegevens die door misdrijf zijn verkregen voorhanden te hebben of bekend te maken. Langs deze weg wordt "heling" van de desbetreffende gegevens strafbaar gesteld. De voorgestelde strafbaarstelling heeft uitsluitend betrekking op niet-openbare gegevens. Het downloaden van openbare gegevens van internet is op grond van deze strafbepalingen dus niet strafbaar.

3.3 De Europese dimensie[26]

Ook in Brussel is aandacht voor de bestrijding van cybercrime. Het kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen is inmiddels vervangen door richtlijn 2013/40/EH van het Europees parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen. De richtlijn beoogt minimumregels vast te stellen over aanvallen op informatiesystemen. Nieuw ten opzichte van het kaderbesluit en het Cybercrimeverdrag van de Raad van Europa (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18) zijn onder meer de hoogte van de maximale gevangenisstraffen, waardoor cybercriminaliteit met hogere straffen wordt bedreigd en enkele strafverzwarende omstandigheden. Het wetsvoorstel ter implementatie van deze richtlijn is thans in voorbereiding en zal in het voorjaar van 2014 bij Uw Kamer aanhangig worden gemaakt.

De huidige Europese privacyrichtlijn schiet op onderdelen tekort om een niveau van gegevensbescherming te garanderen dat voldoende aansluit bij de behoeften van burgers en bedrijven om grensoverschrijdend zaken te kunnen doen in de hedendaagse informatiemaatschappij. Deze Europese privacyrichtlijn uit 1995 zal naar verwachting uiterlijk begin 2015 worden vervangen door een Algemene Verordening gegevensbescherming, die rechtstreekse werking binnen de lidstaten zal hebben. Parallel daaraan zal het Kaderbesluit 2008/977/JBZ worden vervangen door een Richtlijn gegevensbescherming opsporing en vervolging, die ook op gegevensverwerking op zuiver nationaal niveau betrekking zal hebben. De ontwerpverordening stelt nieuwe regels vast met betrekking tot de bescherming van de gegevens van natuurlijke personen en het vrije verkeer van persoonsgegevens. Het begrippenkader wordt verruimd. De rechten van betrokkenen worden versterkt, met name met het recht om te worden vergeten en het recht op dataportabiliteit. Het toezicht op de naleving en de handhaving van de

[25] http://www.rijksoverheid.nl/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit.html.
[26] Voor een beeld van de ontwikkelingen in een aantal ons omringende landen wordt verwezen naar bijlage 3.

regels over gegevensbescherming worden op EU-niveau vastgesteld. Er wordt voorzien in robuuste sanctionering, met name in de bevoegdheid tot het vaststellen van bestuurlijke boetes door toezichthouders.

In het algemeen overleg van 7 maart 2012 is toegezegd de Tweede Kamer periodiek op de hoogte te houden van de stand van zaken over de onderhandelingen in Brussel over de Algemene verordening gegevensbescherming en ook de Richtlijn gegevensbescherming opsporing en vervolging (zie § 4.9). Sindsdien zijn verschillende voortgangsrapportages uitgebracht.[27] Tot slot dient hier te worden vermeld dat in het kader van de Raad van Europa de herziening en modernisering van het Dataprotectieverdrag van de Raad van Europa (1981) ter hand is genomen.

3.4 Transatlantische ontwikkelingen

Aan beide zijden van de Atlantische oceaan vinden belangrijke ontwikkelingen plaats op het gebied van dataprotectie. De VS en de EU leggen daarbij verschillende accenten, ondanks dat het doel, de effectieve bescherming van gegevens, hetzelfde is. De VS leggen meer de nadruk op het zelfstandig optreden van de burger, waar in de EU de overheid een relatief sterkere rol heeft. Er moet vanuit worden gegaan dat deze verschillen in de toekomst blijven bestaan, ook als Europa straks beschikt over nieuwe Europese privacywetgeving.

Het College bescherming persoonsgegevens (Cbp) wil bezien in hoeverre deze transatlantische verschillen op pragmatische wijze zijn te overbruggen. De eerste gedachtenvorming daarover bij het Cbp is gaande. Het kabinet is daarbij betrokken, mede omdat dit onderwerp van belang kan zijn voor bespreking binnen de EU tijdens het Nederlands voorzitterschap in de eerste helft van 2016.

4. De overheid in haar omgang met persoonsgegevens

4.1 Transparantie

De toenemende complexiteit van de digitale wereld als gevolg van big data en cloud computing en de ontwikkeling van nieuwe opsporings- en analysetechnieken raken ook het zgn. transparantiebeginsel. Dit is een belangrijk beginsel bij de bescherming van persoonsgegevens. De burger moet in beginsel over voldoende informatie kunnen beschikken over wat er met zijn persoonsgegevens gebeurt. Aan het transparantiebeginsel wordt mede in het licht van de technologische ontwikkelingen steeds meer belang gehecht. Dit komt onder meer tot uitdrukking in de expliciete grondslag die dit beginsel in de voorstellen voor de nieuwe Europese privacywetgeving heeft gekregen.[28] De vraag waarvoor we staan, is hoe bij een voortgaande digitalisering in de Nederlandse samenleving op de juiste wijze inhoud kan worden gegeven aan het transparantiebeginsel op het terrein van de veiligheid.

Deze opgave is van belang, omdat transparantie kan bijdragen aan het vertrouwen dat burgers hebben in de wijze waarop overheidsdiensten op het terrein van de veiligheid gegevens verzamelen en verder verwerken. Dat belang neemt toe, omdat de gemiddelde burger niet op de hoogte zal zijn van alle moderne technische mogelijkheden op dat vlak. Toepassing van het transparantiebeginsel stuit uiteraard wel op grenzen die ingegeven zijn door bijvoorbeeld belangen van opsporing en vervolging. Zo zullen specifieke "modus operandi" niet openbaar kunnen zijn. Hetzelfde kan onder omstandigheden gelden voor de mate waarin bepaalde methoden worden gebruikt. Kennis daarvan kan criminelen immers helpen hun gedrag en keuze van communicatiemiddelen daarop af te stemmen.

Anticiperend op de komende Europese regelgeving menen wij dat het beleid van overheidsdiensten op het terrein van de veiligheid met betrekking tot de verwerking van persoonsgegevens transparant en eenvoudig toegankelijk moet zijn. Voor zover nodig, zullen deze diensten worden aangespoord in de loop van 2014 daarvoor zorg te dragen. Diensten zullen daarbij in het bijzonder aandacht moeten besteden aan "datamining" en "profiling", indien zij daarvan gebruik maken. De risico's voor de bescherming van de persoonlijke levenssfeer zijn bij toepassing van dergelijke technieken immers groter dan bij meer klassieke vormen van gegevensverwerking, onder meer

[27] Kamerstukken II 32761, nrs. 34, 44, 46 en 54.

[28] Zie de artikelen 5, onder a, en 11, van het voorstel voor een Algemene verordening gegevensbescherming, 2012/011 (COD), en artikel 10 van het voorstel voor een Richtlijn gegevensbescherming opsporing en vervolging, 2012/0010 (COD).

omdat wordt gewerkt met vooronderstellingen die aan een bepaald profiel ten grondslag liggen. Deze risico's brengen mee dat het belang van transparantie bij "datamining" en "profiling" extra groot is.

4.2 Ontwikkeling nieuwe opsporingsmethoden

Bij de ontwikkeling van nieuwe opsporingsmethoden kan de privacy in het geding zijn. Voor zover het gaat om methoden die slechts een beperkte inbreuk op de privacy maken, kan daarvoor op basis van bestaande jurisprudentie een grondslag worden gevonden in artikel 3 van de Politiewet 2012.[29] Andere nieuwe technieken zullen waar mogelijk gebaseerd worden op de regeling van specifieke opsporingsbevoegdheden in het Wetboek van Strafvordering. Dan blijven er nog nieuwe methoden over die, mede bezien in het licht van de potentie van de methode om een betekenisvolle inbreuk op de privacy van betrokkenen te maken, dusdanige risico's voor de integriteit en beheersbaarheid van de opsporing opleveren dat een bijzondere wettelijke grondslag voor het gebruik van deze opsporingsmethode noodzakelijk kan worden geacht dan wel enige andere vorm van nadere regelgeving wenselijk is.[30] Zo zijn politie en OM bezig de procedure voor de inzet van de zgn. stille sms aan te scherpen.[31] Het gaat hierbij om een vorm van "sensing": het waarnemen of verzamelen van informatie via technieken die werken op afstand van de waargenomen personen of objecten. Of er nog andere vormen van "sensing" zijn die enige vorm van regelgeving of procedurele voorschriften vergen, zal kunnen blijken uit de visie die de politie over "sensing" zal uitbrengen en het standpunt daarover van het kabinet.

4.3 Drones[32]

Een specifieke vorm van "sensing" die tegenwoordig veel aandacht krijgt, is het gebruik van camera's die bevestigd zijn aan onbemande luchtvaartuigen ("drones"). Hierbij moet onderscheid worden gemaakt tussen gebruik door de politie bij de uitvoering van de politietaak, gebruik in het belang van de openbare orde in opdracht van de burgemeester, gebruik door andere (overheids)diensten en overig gebruik door particulieren.

De drones die de politie thans voor uitvoering van de politietaak gebruikt, zijn van het type Raven. De Raven opereert op een hoogte van ongeveer driehonderd meter. Op deze hoogte is de beeldkwaliteit van de daglichtcamera onvoldoende voor gezichtsherkenning. De nachtcamera produceert een tweekleurig beeld waarbij slechts de contouren van warmtebronnen worden weergegeven. Een en ander impliceert dat de camera's wel beelden kunnen produceren waarop personen zijn te zien, doch geen beelden waarop deze personen herkenbaar zijn.[33] De ontwikkelingen op dit punt staan echter niet stil: het is zeer wel denkbaar dat een nieuwe generatie camera's vanaf drones in de toekomst personen wel herkenbaar in beeld kunnen brengen.[34] Dat kan van belang zijn voor de opsporing. Als het daarbij slechts om een beperkte inbreuk op de privacy gaat, mag op basis van jurisprudentie van de Hoge Raad worden aangenomen dat artikel 3 van de Politiewet 2012 daarvoor als algemeen taakstellend artikel voor de politie een voldoende wettelijke grondslag bieden.[35] Pas als het cameragebruik het karakter van stelselmatige observatie krijgt, moet aan de daarvoor geldende voorwaarden van artikel 126g van het Wetboek van Strafvordering worden voldaan. De politie doet op dit moment onderzoek naar de effectiviteit van de inzet van drones. Zodra het onderzoek is afgerond, zal het kabinet zijn standpunt daarover aan uw Kamer aanbieden.

---

[29] Vgl HR 19 december 1995, NJ 1996, 249 (Zwolsman-arrest).

[30] Zie voor dit criterium o.a. Hof Den Bosch 15 augustus 2013, ECLI:NL:GSHE:2013:4046.

[31] Zie Aanhangsel kamerstukken II 2013-2014, nr. 9.

[32] PM Aanpassen als motie Schouw (kamerstukken II 2013-2014, 33750-VI, nr. 67) wordt aangenomen.

[33] Aanhangsel kamerstukken II 2012-2013, nr. 2216.

[34] Defensie heeft sinds kort de Scan Eagle in gebruik. Het zal evenwel nog enige tijd duren totdat de Scan Eagle ook gereed is voor ondersteuning van civiele autoriteiten, zoals de politie. De Scan Eagle beschikt over een infrarood- of een daglichtcamera. De daglichtcamera is van betere kwaliteit dan die van de Raven. Dit is nodig vanwege de grotere hoogte waarop de Scan Eagle opereert. De Scan Eagle kan vliegend op de operationele hoogte personen niet herkenbaar in beeld brengen. Als de Scan Eagle erg laag vliegt en de persoon in kwestie omhoog kijkt, is dit mogelijk wel het geval. Opereren op een dergelijk lage hoogte is echter zeer ongebruikelijk en in de meeste gevallen niet toegestaan uit veiligheidsoverwegingen. Zie Aanhangsel kamerstukken II 2012-2013, nr. 2985.

[35] HR 19 december 1995, NJ 1996, 249 (Zwolsman-arrest)

Het gebruik van camera's in het belang van de openbare orde in situaties waarin (nog) geen sprake is van een actuele verstoring van de openbare orde dan wel dreiging daarvan, is op grond van artikel 151c van de Gemeentewet nu alleen toegestaan met behulp van vaste camera's. Dit impliceert dat de inzet van drones in het belang van de handhaving van de openbare orde, zonder dat er sprake is van een actuele verstoring van de openbare orde dan wel dreiging daarvan, nu nog niet is toegestaan. Het kabinet heeft een wetsvoorstel ingediend waarin de burgemeester de bevoegdheid krijgt bij het houden van toezicht ter handhaving van de openbare orde ook mobiele camera's – dus eventueel ook drones - in te zetten.[36] In het algemeen kan worden gesteld dat – vanwege de ruimere mogelijkheden en de inherente privacygevaren – de inzet van vliegende camera's als een zwaarder middel kan worden aangemerkt dan de inzet van statisch opgestelde camera's. Het ligt om die reden voor de hand dat de inzet van vliegende camera's minder snel toelaatbaar is dan de inzet van – al dan niet nagelvast bevestigde – statisch opgestelde camera's. Tegelijkertijd is het echter niet ondenkbaar dat – bijvoorbeeld door snelle verplaatsingseffecten – in bepaalde gevallen de inzet van vliegende camera's noodzakelijk is ter handhaving van de openbare orde.[37]

Naast de politie en de burgemeester maken nationale en lokale (overheids)diensten gebruik van drones. Zij doen dit vooral door commerciële dienstverleners in te huren. Het gaat daarbij onder meer om foto- of videorapportages vanuit de lucht van gebouwen, terreinen of evenementen, inspecties van industriële objecten, windmolens, hoogspanningsmasten, pijpleidingen, luchtobservaties van mensenmassa's, branddetectie en -monitoren, milieuhandhaving in natuurgebieden, opsporen van drenkelingen, en landmeetkundige diensten voor o.a. gemeenten. Aangezien de kwaliteitseisen aan drones en hun operators nog in ontwikkeling zijn, wordt alleen gevlogen boven bewoond gebied als er sprake is van een groot maatschappelijk belang (te duiden door de (regio)burgemeester) in combinatie met een operationeel plan waaruit blijkt dat de risico's tot het minimum zijn beperkt (betrouwbaar systeem, zeer ervaren vliegers, georganiseerd werkend bedrijf). De inzet van onbemande vliegtuigen door particulieren gebeurt hierdoor nagenoeg altijd op afstand (minimaal 150 meter) van mensenmenigten, bebouwd gebied, kunstwerken, industrie- en havengebieden, openbare wegen en spoorlijnen.[38] Uit de aard van dit werk vloeit derhalve voort dat de daarbij gebruikte camera's er niet op zijn gericht om personen herkenbaar in beeld te brengen.

Als bij het maken van afbeeldingen met behulp van drones door particulieren afbeeldingen worden gemaakt die herleidbaar zijn tot personen, valt het maken daarvan onder de Wet bescherming persoonsgegevens, tenzij het gaat om het maken van afbeeldingen ten behoeve van uitsluitend persoonlijke of huishoudelijke doeleinden. Daarnaast bieden de artikelen 139f en 441b van het Wetboek van Strafrecht de mogelijkheid om op te treden tegen het heimelijk inzetten van camera op een drone, als het oogmerk en de mogelijkheid bestaat daarmee een persoon herkenbaar in beeld te brengen. Op dit moment werkt het ministerie van Infrastructuur en Milieu aan regelgeving die de toelaatbaarheid van het recreatief vliegen met modelvliegtuigen boven plekken waar zich zichtbaar vaak of veel mensen bevinden, sterk inperkt. Dit heeft als bijkomend gevolg dat de kans op het herkenbaar in beeld brengen van personen vanaf modelvliegtuigen kleiner wordt. Voor onbemande luchtvaartuigen voor beroepsmatig gebruik door particulieren geldt in de praktijk al dat vluchten boven gebieden met aaneengesloten bebouwing en mensenmenigten niet zijn toegestaan, tenzij daarvoor een dringende maatschappelijke reden bestaat.[39]

Wij achten de geldende en aanstaande wet- en regelgeving hiermee vooralsnog voldoende toegerust om rekening te houden met het beschermen van de privacy bij het huidige gebruik van op drones gemonteerde camera's. Wij willen het echter niet bij deze constatering laten, nu het gebruik van op drones gemonteerde camera's nog steeds in ontwikkeling is.[40] Wij willen ons daarom bezinnen op de vraag of de huidige wettelijke kaders voor het gebruik van camera's op drones met het oog op die ontwikkeling ook voor de toekomst toereikend zijn. Het ligt voor de hand daarbij in ieder geval de uitkomst te betrekken van het onderzoek dat de politie op dit moment naar de effectiviteit van de inzet van drones uitvoert. De mate van effectiviteit is immers

[36] Kamerstukken II 2012-2013, 33582, nrs. 1-3.
[37] Kamerstukken II 2012-2013, 33582, nr. 6, blz 9.
[38] Aanhangsel Kamerstukken II 2012-2013, nr. 2216.
[39] Aanhangsel Kamerstukken II 2012-2013, nr. 2691.
[40] Zie in dit verband ook: Bart Schermer en Marjolein van der Heide, "Privacyrechtelijke aspecten van drones" in: Nederlands Juristenblad 2013/1605.

medebepalend voor het antwoord op de vraag of de inzet van drones, als daarmee personen in de toekomst mogelijk wel herkenbaar in beeld worden gebracht, als een noodzakelijke beperking van de privacy kan worden aangemerkt. Wij zullen voor onze oordeelsvorming over de eventuele noodzaak van nadere regelgeving ook een vergelijking uitvoeren van de wet- en regelgeving in ons omringende landen met betrekking tot het gebruik van drones. Daarbij zal in het bijzonder worden gekeken naar vereisten ten aanzien van de effectiviteit en proportionaliteit van het gebruik. Ook zullen wij in kaart brengen wat de verwachte kansen en bedreigingen van drones zijn voor de nationale veiligheid en criminaliteit. Met deze onderzoeken willen wij tevens uitvoering geven aan de motie Schouw en Segers over het gebruik van drones.[41]

4.4 Privacy Impact Assessments

In mei 2011 heeft de Eerste Kamer de motie-Franken aangenomen. In deze motie wordt de regering verzocht bij wetsvoorstellen, waarbij van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer sprake is, een aantal criteria in de afweging en besluitvorming te betrekken. Het betreft hier onder meer de duiding van de noodzaak, effectiviteit en hanteerbaarheid van een maatregel, het opnemen van de resultaten van een Privacy Impact Assessment (PIA) en het opnemen van een evaluatie- en eventueel een horizonbepaling bij een maatregel.[42]

In navolging van deze motie is in het regeerakkoord van het huidige kabinet vastgelegd dat bij de bouw van systemen en het aanleggen van databestanden bescherming van persoonsgegevens uitgangspunt is en dat een PIA daar standaard bij hoort.[43] Het kabinet heeft aan deze motie uitvoering gegeven door onder meer het uitvoeren van een PIA bij het wetsvoorstel ANPR.[44] Het kabinet heeft ter uitvoering van de motie-Franken inmiddels een PIA-toetsmodel Rijksdienst vastgesteld, dat vanaf 1 september 2013 standaard wordt toegepast bij de ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien.[45] Met gebruikmaking van dit toetsmodel zullen PIA's worden uitgevoerd bij de voorbereiding van onder meer het eerdergenoemde wetsvoorstel computercriminaliteit III en bij de voorbereiding van een wetsvoorstel verruiming gebruik private camerabeelden ter ondersteuning van de opsporing.

4.5 Digitale informatieverzameling

In een digitale samenleving wint digitale informatieverzameling enorm aan belang. Een duidelijk voorbeeld van maatschappelijk verantwoord innoveren op dit terrein is iColumbo. In dit traject wordt op een geavanceerde manier informatie op een zodanige manier verzameld en geanalyseerd dat de gegevensverwerking conform artikel 11 Wbp zowel toereikend als niet bovenmatig is. Het betreft hier een dienst binnen het Internet Research Network (iRN) van de politie waarmee automatisch informatie van Internet wordt verzameld, geanalyseerd en op een "slimme manier" gepresenteerd aan eindgebruikers. Hiermee zien gebruikers per onderzoek de informatie die voor hen interessant is, zonder dat ze handmatig informatie moeten verzamelen en combineren. iColumbo wordt ontwikkeld vanuit de gedachte dat het toetsbaar en transparant moet zijn wat er binnen deze dienst gebeurt, hoe de resultaten bereikt worden en dat het aan juridische grenzen en voorwaarden voldoet ("Legal by design"). iColumbo is vanaf begin 2013 als bètaversie beschikbaar en wordt voortdurend verder ontwikkeld.[46]

4.6 Gebruik private camerabeelden ter ondersteuning van de opsporing

Camerabeelden van strafbare feiten blijken een nuttig hulpmiddel bij de opsporing van deze feiten. Wanneer echter niet alle mogelijkheden om de beelden optimaal te gebruiken worden benut, dan

---

[41] Kamerstukken II 2013-2014, 33750-VI, nr. 67.

[42] Vgl. de motie Franken (kamerstukken I 2010-2011, 31051, D).

[43] Kamerstukken II 2012-2013, 33410, nr. 15, blz. 27. Ook de komende Algemene verordening gegevensbescherming van de Europese Unie zal mogelijk een verplichting tot het uitvoeren van een PIA bevatten. Zie artikel 33 van het voorstel voor deze verordening, 2012/0011 (COD).

[44] Kamerstukken II 2012-2013, 33542, nr. 3, bijlage.

[45] Kamerstukken II 2012-2013, 26643, nr. 282 herdruk. Het model is inmiddels ook opgenomen in het Integraal Afwegingskader voor beleid en regelgeving.

[46] Zie http://columbo.nl/info/?lang=nl. Zie ook: Bert Jaap Koops e.a., Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo en HDIeF-tools, 2012, blz. 7.

leidt dat tot gevoelens van frustratie en teleurstelling bij de slachtoffers en mogelijk ook tot het verminderen van het vertrouwen in opsporing en vervolging. Dit kan ertoe leiden dat burgers overgaan tot het zelfstandig plaatsen van camerabeelden op internet zonder betrokkenheid van politie en justitie. De effecten daarvan kunnen onder omstandigheden echter negatief zijn. Soms worden personen op ondoordacht verspreide beelden ten onrechte in verband gebracht met strafbare feiten. Er is dan sprake van een onnodige schending van de privacy van deze burgers. Ook bestaat het risico dat de opsporingsbelangen worden doorkruist. Het is heel goed denkbaar dat de opsporingsbelangen in een individuele zaak vergen dat geen publiciteit wordt gegeven aan een bepaald strafbaar feit.

Waar het vooral om gaat is dat de wetgeving het gebruik van camerabeelden door particulieren als ondersteuning van de opsporing niet meer, maar ook niet minder moet reguleren dan strikt noodzakelijk is om een evenwichtige benadering tussen de bescherming van persoonsgegevens en de belangen van opsporing en vervolging van strafbare feiten te bereiken. De maatschappelijke discussie die bij tijd en wijle hoog oploopt, vergt dat een wat ruimer gebruik van camerabeelden door particulieren als ondersteuning van de opsporing mogelijk wordt, zonder de belangen van de bescherming van persoonsgegevens te verminderen. Daartoe zal in het eerste kwartaal van 2014 een wetsvoorstel voor internetconsultatie worden uitgebracht, dat met de nodige waarborgen ruimer gebruik daarvan mogelijk maakt. Met dit wetsvoorstel geeft het kabinet ook uitvoering aan de motie van de leden van de Tweede Kamer Oskam en Van Oosten over het effectief gebruik van camerabeelden bij de opsporing.[47]

4.7 Evaluatie Wet politiegegevens

Op grond van de Wet politiegegevens (Wpg) moet aan de Staten-Generaal elke vier jaar verslag worden gedaan over de doeltreffendheid en de effecten van deze wet in de praktijk. In dit kader werd, in opdracht van het WODC, in november 2012 een evaluatie van de Wpg gestart. Deze evaluatie had een tweeledige vraagstelling: wat heeft de wetgever met de Wpg beoogd, en hoe wordt de wet in de praktijk uitgevoerd? Bij het onderzoek is met name aandacht besteed aan de signalen vanuit die uitvoeringspraktijk. Deze signalen hadden onder meer betrekking op organisatorische aspecten (bewustwording, cultuur, scholing e.d.), infrastructurele problemen, vooral op het terrein van de ondersteunende ICT-voorzieningen, de complexiteit van de Wpg, alsmede enige onwenselijke (neven)effecten bij de uitvoering van die wet. Bij dat laatste moet vooral worden gedacht aan de (veelal als te kort ervaren) bewaar- en vernietigingstermijnen.

In oktober 2013 is het evaluatierapport opgeleverd. Naast een reconstructie van de beleidstheorie en een verslag van de uitvoeringspraktijk gaat het rapport in op de vraag of die uitvoeringspraktijk overeenkomstig de doelstellingen en verwachtingen van de wetgever geschiedt, welke knelpunten zich voordoen en hoe die knelpunten kunnen worden verklaard. Ook wordt ingegaan op de vraag hoe de Wpg zich verhoudt tot andere wet- en regelgeving. In het eerste kwartaal van 2014 zal het rapport, voorzien van een beleidsreactie, aan beide kamers der Staten-Generaal worden aangeboden.

4.8 Gegevensverwerking bij forensische zorg

Eén van de principes die aan gegevensbescherming ten grondslag liggen, is contextuele integriteit van persoonsgegevens (zie § 2). Het belang van contextuele integriteit brengt mee dat bij de verwerking van gegevens de combinatie van doelbinding en "informed consent" uitgangspunt dient te zijn. Er kunnen zich echter situaties voordoen waarin van dit uitgangspunt deels moet worden afgeweken. Het komt er dan op aan deze afwijking alleen toe te staan, indien de nodige waarborgen in acht zijn genomen. Zo'n situatie kan zich voordoen bij verdachten die weigeren mee te werken aan pro Justitia-onderzoek (de zgn. weigerende observandi). Vanuit het oogpunt van de veiligheid van de samenleving is het ontoelaatbaar als geen tbs kan worden opgelegd louter omdat de verdachte niet meewerkt ingeval een tbs-maatregel de passende maatregel zou zijn. Met het oog op deze situatie heeft het kabinet in het wetsvoorstel Forensische zorg een regeling opgenomen die het mogelijk maakt persoonsgegevens over de geestelijke gezondheid van weigerende observandi, ook zonder hun toestemming, van hun behandelaren te vorderen en aan deskundigen te verstrekken.

Het vorderen en verstrekken van dergelijke persoonsgegevens is met het oog op de bescherming van de persoonlijke levenssfeer en de doorbreking van het medisch beroepsgeheim met de nodige

[47] Kamerstukken II 2013-2014, 33750-VI, nr. 62.

waarborgen omkleed. Zo dient een multidisciplinaire commissie advies uit te brengen over de aanwezigheid en bruikbaarheid van de gevorderde medische gegevens voor het onderzoek. Deze gegevens blijven onder de commissie totdat de rechter onherroepelijk heeft beslist op de vordering die de officier van justitie op basis van het advies heeft ingediend om de commissie te machtigen de desbetreffende gegevens aan de deskundigen te verstrekken. Op deze manier wordt niet structureel bij alle verdachten het medisch beroepsgeheim doorbroken in dienst van het strafproces, maar alleen bij die verdachten bij wie het maatschappelijk belang zwaar weegt en de veiligheid mogelijk in gevaar is bij handhaving van het beroepsgeheim.[48]

4.9 Herziening van de Europese normen voor de gegevensverwerking door politie en justitie

Het kaderbesluit gegevensbescherming opsporing en vervolging bevat regels voor de bescherming van persoonsgegevens die worden verwerkt ten behoeve van de voorkoming, opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en het vrije verkeer van dergelijke gegevens. Het kaderbesluit is echter uitsluitend van toepassing op persoonsgegevens die tussen de lidstaten worden uitgewisseld. Op initiatief van de Commissie zal het kaderbesluit gegevensbescherming worden vervangen door een richtlijn, die van toepassing is op alle persoonsgegevens die in de lidstaten voor dit doel worden verwerkt. De regels van de richtlijn hebben betrekking op de doelbinding, de rechten van de betrokkene, de overdracht van persoonsgegevens aan derde landen en het toezicht op de gegevensverwerking. Het kabinet steunt een spoedige totstandkoming van de richtlijn, omdat een hoog niveau van gegevensbescherming binnen de EU van belang is voor de bescherming van de rechten van burgers. Zoals hierboven reeds is vermeld, wordt de Kamer door middel van periodieke voortgangsrapportages op de hoogte gehouden van de stand van zaken over de onderhandelingen in Brussel.

5 Overzicht actiepunten

In de paragrafen 3 en 4 staan verschillende actiepunten, die in onderstaand overzicht worden weergegeven, met een tijdlijn.

Actie	**Wanneer?**
1. Stimulering van privacy en security by design in de aanbestedingstrajecten van producten en diensten voor de overheid (§ 3.1)	2014-2016
2. De ontwikkeling van standaarden, zoveel mogelijk in internationaal verband, die gebruikt worden om veiligheid en privacy van ICT-producten en –diensten te bevorderen (§ 3.1)	2014 en verder
3. Versterking uitvoering zorgplicht aanbieders ICT-netwerken en –diensten voor cybersecurity door zelfregulering. Bezien of dit in voldoende mate gebeurt of dat aanvullende vormen van toezicht of regulering nodig zijn (§ 3.1)	December 2013
4. Uitvoering van een verkenning naar gescheiden ICT-netwerken en –diensten, waaronder ook een clouddienst, voor publieke en private vitale processen (§ 3.1)	Januari 2014
5. Cybersecurity opnemen in de aanpak vitale infrastructuur. Onderdeel daarvan is een periodiek beeld van welke ICT-afhankelijke systemen, dienstenen processen vitaal zijn. (§ 3.1)	December 2013 en verder
6. Versterking van het bewustzijn bij burgers, bedrijven, organisaties en overheden omtrent informatiebeveiliging en privacy, bijvoorbeeld door bewustzijnscampagnes als Alert Online, om kennis en inzicht van cyberspionage te vergroten (§ 3.1)	2014-2016 (Alert Online 27 oktober 2014 tot en met 6 november 2014)
7. Op- en uitbouwen van een Nationaal Detectie- en Responsenetwerk (§ 3.1)	2013 en verder

[48] Kamerstukken II, 2011-2012, 32398, nr. 10; kamerstukken I 2013-2014, 32398, G.

8. Oprichting van een PPS-taskforce Cybersecurity Onderwijs die zich richt op advisering over het cybersecurity-onderwijsaanbod. (§ 3.1)	2014
9. Indiening wetsvoorstel computercriminaliteit III (§ 3.2)	Eerste helft 2014
10. Indiening wetsvoorstel ter implementatie Richtlijn 2013/40 over aanvallen op informatiesystemen (§ 3.3)	Eerste helft 2014
11. Visie op mogelijkheden van pragmatische overbrugging van verschil in zienswijzen tussen EU en VS over gegevensbescherming met het oog op het Nederlands voorzitterschap van de EU in 2016 (§ 3.4)	2014-2016
12. Privacybeleid van diensten op het terrein van de veiligheid op een voor burgers transparante en eenvoudig toegankelijke wijze kenbaar maken (§ 4.1)	2014
13. Visie op "sensing" (§ 4.2)	Eerste helft 2014
14. Onderzoek naar de vraag of de huidige wettelijke kaders voor het gebruik van camera's op drones met het oog op de effecten op de privacy ook voor de toekomst toereikend zijn (§ 4.3)	2014
15. Uitvoeren PIA's bij wetsvoorstellen computercriminaliteit III en verruiming gebruik private camerabeelden ter ondersteuning van de opsporing (§ 4.4)	2013-2014
16. Doorontwikkeling iColumbo, onder meer aanbieden als dienst voor politie en andere rechtshandhavingsinstanties (§ 4.5)	December 2013 en verder
17. Internetconsultatie wetsvoorstel verruiming gebruik private camerabeelden ter ondersteuning opsporing (§ 4.6)	Eerste kwartaal 2014
18. Kabinetsstandpunt evaluatie Wet politiegegevens (§ 4.7)	Eerste kwartaal 2014
19. Regeling verstrekking gegevens weigerende observandi in wetsvoorstel Forensische zorg (§ 4.8)	Is in behandeling bij Eerste Kamer

Bijlage 1: Juridisch kader

Het recht op bescherming van de persoonlijke levenssfeer is stevig verankerd in een aantal wetten en verdragen.

Artikel 10, eerste lid, van de Grondwet erkent het recht op eerbiediging van de persoonlijke levenssfeer en schrijft voor dat inbreuken daarop bij of krachtens een wet in formele zin moeten zijn geregeld. In het tweede lid van dit artikel wordt de wetgever opgedragen regels vast te stellen met betrekking tot de bescherming van persoonsgegevens. In artikel 13 van de Grondwet is het brief-, telefoon- en telegraafgeheim vastgelegd. Het voornemen bestaat dit artikel te moderniseren en uit te breiden naar een brief- en telecommunicatiegeheim.[49]

Artikel 8 van het Europees verdrag inzake de Rechten van de Mens en de fundamentele vrijheden (EVRM) bepaalt dat een ieder recht heeft op respect voor zijn privéleven. Het tweede lid van dat artikel eist dat inbreuken op de persoonlijke levenssfeer door de overheid moeten zijn voorzien in de wet en noodzakelijk zijn in een democratische samenleving op grond van een aantal nader aangegeven gronden. Daartoe behoren onder meer het belang van de openbare veiligheid en het voorkomen van wanordelijkheden en strafbare feiten. De inbreuk moet ook voldoen aan de vereisten van proportionaliteit en subsidiariteit. Dat impliceert dat de maatregel passend en geschikt moet zijn en van de inbreuk moet worden afgezien, indien het doel dat daarmee wordt beoogd, ook langs andere weg en met minder ingrijpende middelen kan worden bereikt.

Binnen de Raad van Europa is in 1981 – in aanvulling op het EVRM – een verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens vastgesteld. Dit verdrag, het Dataprotectieverdrag[50], wordt op dit moment gemoderniseerd.

In artikel 8 van het Handvest van de grondrechten van de Europese Unie is verankerd dat persoonsgegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en met toestemming van betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Een ieder heeft volgens dat artikel recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.[51]

Waarborgen voor het recht op bescherming van persoonsgegevens, zijn verder vastgelegd in de Europese privacyrichtlijn uit 1995.[52] Deze richtlijn is in Nederland geïmplementeerd in onder meer de Wet bescherming persoonsgegevens. De richtlijn zal binnen afzienbare termijn worden vervangen door een Europese Verordening gegevensbescherming. In het voorstel voor deze verordening worden onder meer de rechten van betrokkenen versterkt, wordt het regime voor de doorgifte van persoonsgegevens aan derde landen nader gereguleerd en wordt voorzien in de bevoegdheid tot het vaststellen van bestuurlijke boetes door toezichthouders.[53]

Voor de samenwerking in strafzaken is het Kaderbesluit 2008/977/JBZ vastgesteld.[54] Dat kaderbesluit is in Nederland geïmplementeerd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Het kaderbesluit heeft een beperkt toepassingsgebied: het is uitsluitend van toepassing op grensoverschrijdende gegevensverwerking en niet op verwerkingsactiviteiten van de politiële en justitiële autoriteiten op zuiver nationaal niveau. Het kaderbesluit zal mede om die reden eveneens binnen afzienbare termijn worden vervangen door een Richtlijn gegevensbescherming opsporing en vervolging. Het voorstel voor de nieuwe richtlijn bevat de nodige waarborgen voor een zorgvuldige verwerking van persoonsgegevens door politie en justitie binnen de Europese Unie en bevat verbeteringen ten opzichte van het huidige kaderbesluit.[55]

---

[49] http://www.rijksoverheid.nl/nieuws/2012/09/28/grondwet-gaat-elektronische-vormen-van-communicatie-beschermen.html.

[50] Trb. 1988, nr. 7.

[51] Pb EU 3 maart 2010, C 83/389.

[52] Richtlijn 95/46/EG van het Europees parlement en de Raad van 24 oktober 1995, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Pb L 281.

[53] Kamerstukken I 2011-2012, 22 112, FI.

[54] Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, PbEU L 350/60.

[55] Kamerstukken I 2011-2012, 22 112, FH.

Grondwet noch verdrag kennen een grondrecht op veiligheid. Maar de overheid heeft wel van oudsher een plicht om zorg te dragen voor de veiligheid van zijn burgers. Zelfs in de nachtwakersstaat van de 19e eeuw, waarin aan de overheid een relatief beperkte taak werd toegedacht, was het bestaan van deze plicht onomstreden. Men zou zelfs kunnen zeggen dat deze plicht zo vanzelfsprekend is dat er nimmer een parlementaire meerderheid is geweest die het nodig vond om haar in de Grondwet vast te leggen.[56]

Veiligheid als te beschermen belang komt terug in artikel 67 van het Werkingsverdrag van de Europese Unie. In het eerste lid van dat artikel is vastgelegd dat de Unie een ruimte is van vrijheid, veiligheid en recht, waarin de grondrechten en de verschillende rechtsstelsels en -tradities worden geëerbiedigd. Ingevolge het derde lid streeft de Unie ernaar een hoog niveau van veiligheid te waarborgen, door middel van maatregelen ter voorkoming en bestrijding van criminaliteit, en van racisme en vreemdelingenhaat, maatregelen inzake coördinatie en samenwerking tussen de politiële en justitiële autoriteiten in strafzaken en andere bevoegde autoriteiten, alsmede door de wederzijdse erkenning van rechterlijke beslissingen in strafzaken en, zo nodig, door de onderlinge aanpassing van de strafwetgeving.[57]

[56] Een initiatiefvoorstel van het toenmalige lid van de Tweede Kamer Rietkerk (CDA) om het recht op veiligheid in de Grondwet vast te leggen, werd in 2008 ingetrokken (kamerstukken II 28036, nrs. 1-4),
[57] PbEU 2010, C 83/47.

Bijlage 2: Relevante technologische ontwikkelingen

1. Big data

Een eerste ontwikkeling die impact op de verhouding tussen veiligheid en privacy heeft, is het ontstaan van "big data". Dit staat voor het fenomeen dat de hoeveelheid data exponentieel groeit, dataverzamelingen steeds groter en complexer worden en relevante data als gevolg daarvan niet meer fysiek of logisch in één locatie of in één systeem kunnen worden opgeslagen. We genereren met elkaar immers steeds meer data door het gebruik van computers, internet, social media, smartphones en camera's. Om een indruk van deze groei te geven: in 2013 bereikt de totale hoeveelheid aan data een volume van 4 zetabytes[58], een verviervoudiging ten opzichte van 2010. Tot 2020 neemt het volume naar verwachting verder toe met een factor tien naar 40 zetabytes. Dit komt neer op een groei naar meer dan 5200 gigabytes per hoofd van de bevolking.[59] Voor een relatief ontwikkeld land als Nederland zal dat naar verwachting op een nog veel hoger getal uitkomen. De veronderstelling lijkt gerechtvaardigd dat van een navenante groei sprake zal zijn van dat deel van de totale hoeveelheid data dat uit persoonsgegevens bestaat.[60]

2. Cloud computing

De groei van de hoeveelheid data wordt mede mogelijk gemaakt door een ander relatief nieuw fenomeen: cloud computing. Cloud computing is het uitbesteden van gegevensbeheer of computerapplicaties aan een dienstverlener, waarbij gegevens – meestal zonder regie over de precieze locatie – verspreid over verschillende servers worden opgeslagen. Verschijningsvormen die "typisch" cloud computing zijn, zijn emaildiensten als Gmail en Hotmail, diensten voor opslag of delen van bestanden als DropBox en applicatiediensten als Google Docs.[61] De verwachting is dat in 2020 bijna 40% van de informatie in de digitale wereld ergens op zijn reis van producent naar ontvanger zal zijn opgeslagen of verwerkt in de cloud.[62]

3. Social media

Social media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. Bekende voorbeelden van social media zijn Facebook, Twitter, YouTube, LinkedIn, Google+, Instagram en Wikipedia. Social media zijn volledig geïntegreerd in het dagelijks leven. Bijna 8 op de 10 Nederlanders maakt gebruik van één of meer social media. Van bijvoorbeeld Facebook maken bijna 8 miljoen Nederlanders gebruik, waarvan 5 miljoen dagelijks.[63] Social media zijn hiermee zeer belangrijke communicatiemiddelen geworden.

4. *Sensing*

Innovatie op technologisch vlak doet zich ook voor bij de ontwikkeling van nieuwe opsporingstechnieken. Daarbij kan men denken aan het (verder) ontwikkelen van methoden van "sensing", het waarnemen of verzamelen van informatie via technieken die werken op afstand van de waargenomen personen of objecten. Het kan hierbij gaan om waarneming door camera's, richtmicrofoons en warmtezoekers. Aan de verdere ontwikkeling van dergelijke technieken wordt voortdurend gewerkt. Zo is de ontwikkeling van "smart" camera's in volle gang. Het gaat hier om camera's waarbij met behulp van speciale software gezichten of bepaald gedrag worden herkend. Ook kan men denken aan de inzet van zgn. stille sms, een methode om met het verzenden van een voor de gebruiker van de telefoon niet waarneembaar sms-bericht te bepalen binnen welk zendmastgebied hij zich bevindt.

---

[58] Een zetabyte is 10^{21} bytes (1.000.000.000.000.000.000.000 bytes).

[59] IDC, Predictions 2013 en The Digital Universe in 2020.

[60] Het IDC schat in dat het deel van de data dat bescherming behoeft – en daartoe behoren ook privacygevoelige data – zal groeien van minder dan een derde in 2010 naar 40 % in 2020.

[61] Bert-Jaap Koops, Ronald Leenes, Paul De Hert en Sandra Olislaegers, Misdaad en opsporing in de wolken, 2012, blz. 6.

[62] IDC, The Digital Universe in 2020.

[63] Newcom, Social media in Nederland 2013, http://www.newcom.nl/publicatie/2/31/Social-media-onderzoek-2013.

Bijlage 3: Ontwikkelingen in ons omringende landen

Verenigd Koninkrijk

Bij haar aantreden in 2010 heeft de Britse coalitieregering aangekondigd meer aandacht te hebben voor de privacy van haar burgers. Dit is opgenomen in het regeerakkoord tussen de twee coalitiepartijen, de Conservatieve Partij en de Liberal Democrats. Hiermee kwamen zij tegemoet aan de klacht dat de Britse overheid onder de Labourregering te veel bevoegdheden had gekregen om burgers te volgen of persoonsgegevens vast te leggen, bijvoorbeeld door het schrappen van de door Labour aangekondigde introductie van de verplichte identiteitskaart.

Communicatie via internet en mobiele telefonie hebben de Britse regering gedurende de eerste drie jaar van haar regeertermijn met nieuwe uitdagingen geconfronteerd. Met name het wetsvoorstel om data op te slaan met het oog op vergemakkelijking van opsporing (communications data bill) geeft de regering veel stof tot denken. De ontwerpwetgeving verplicht internet- en telefoonbedrijven data voor een bepaalde periode op te slaan en geeft politie- en opsporingsdiensten bevoegdheden om deze data te gebruiken. Het gaat dan vooral om het vaststellen van de locatie van mobiele telefoons en computers, de verzender en de ontvanger van de data, de hoeveelheid uitgewisselde informatie en het tijdstip van communicatie. Het voorstel betreft niet direct de inhoud van de informatie. Het wetsvoorstel heeft een forse discussie opgeleverd in zowel het Britse Lager- als Hogerhuis. De belangrijkste discussiepunten betreffen proportionaliteit, waarborgen voor privacy, definities van datacommunicatie, toetsingskaders voor het gebruik van de data door opsporingsdiensten en het aantal diensten dat toegang zou kunnen krijgen tot de data. Inmiddels is het door discussie binnen de coalitie onduidelijk of de Britse regering deze kabinetsperiode nog met aangepaste wetgeving zal komen.

De 'Independent Reviewer of Terrorism Legislation', die toegang heeft tot informatie van veiligheidsdiensten en publiek en parlement informeert over het effect en de toepassing van anti-terrorismewetgeving, heeft een onderzoek aangekondigd naar de arrestatie van de heer Miranda (de partner van de Guardian-journalist met de Snowden-primeur) en de toepassing daarbij van Schedule 7 van de Britse Terrorism Act. Schedule 7 geeft de politie en ambtenaren belast met grenstoezicht de mogelijkheid om bij grensdoorlaatposten personen staande te houden, te onderzoeken en voor maximaal 9 uur vast te houden en te ondervragen, zonder voorafgaande toestemming of 'reasonable suspicion'. De uitkomst van beide onderzoeken wordt thans afgewacht.

Duitsland

Net als in veel Europese landen wordt in Duitsland het debat rond de balans tussen veiligheid en privacy momenteel prominent gevoerd. Gegeven de Duitse historie is dit thema, zowel politiek als maatschappelijk, in Duitsland eigenlijk altijd wel min of meer actueel. De NSU-moorden (nationaal socialistische ondergrondse), de NSA-onthullingen en de recente Bondsdagverkiezingen maken het echter tot een van de belangrijkste politieke en maatschappelijke discussies van de laatste tijd. Los van deze zaken zijn het ook de technologische ontwikkelingen die de Bondsregering nopen tot een herdefiniëring van de balans tussen privacy en veiligheid. Het zoeken naar die balans is een continu proces en vindt voor een belangrijk deel plaats in wisselwerking tussen de verantwoordelijke overheden, maatschappelijke organisaties en het Constitutioneel Hof.
De discussie krijgt momenteel onder andere vorm door de implementatie van het zogenaamde acht-punten-programma van de regering Merkel van 19 juli 2013, waarin maatregelen voor een betere bescherming van de privacy van de burger zijn opgenomen. Ook de evaluatie van de Duitse anti-terrorismewetgeving, die na de aanslagen van september 2011 werd ingevoerd, kan in dit licht worden bezien. Daarbij staat telkens de vraag centraal of de burger voldoende beschermd wordt tegen misbruik van zijn of haar gegevens door overheid of derde partijen, zonder dat deze bescherming de veiligheid van de maatschappij in zijn algemeenheid schade berokkent. Naast dataprotectie en cybersecurity is ook transparantie een thema dat nadrukkelijk door de Bondsregering wordt opgepakt. Een voorbeeld hiervan is het recent afgeronde regeringsprogramma "Vernetzte und transparente Verwaltung" dat ziet op de modernisering van het openbaar bestuur.

Frankrijk

De discussie over veiligheid (inclusief criminaliteitsbestrijding) versus privacy is een discussie, die in Frankrijk, net als in Nederland, wordt gevoerd op veel verschillende deelterreinen. In die zin is er niet veel verschil met de Nederlandse situatie. Er is één groot verschil: in Frankrijk lijkt de discussie zich vooral te richten op inbreuken op de privacy vanuit het buitenland. De discussie op binnenlandse onderwerpen wordt minder gevoerd.

De "Commission Nationale de l'Informatique et des Libertés" (CNIL), die binnenslands de privacy bewaakt, heeft een instructieve studie uitgebracht, "La vie privée à l'horizon 2020", over de verhouding tussen persoonsgegevens, veiligheid en vrijheden. Daarin wordt ook aandacht besteed aan (nieuwe) technologische ontwikkelingen. De CNIL heeft veel gezag en daarom vertrouwt de burger sterk op deze organisatie als het om bewaking van de privacy gaat. In het voorjaar(april 2013) is het zgn. "Livre Blanc" op het gebied van de "défense nationale" van het Ministerie van Defensie verschenen. Hierin wordt niet alleen aandacht besteed aan de klassieke verdediging van het eigen grondgebied, maar ook aan de strijd tegen terrorisme, mensenhandel en mensensmokkel. Verder ook aan het belang van investeren in cybersecurity.

Voor wat betreft inbreuken op de privacy vanuit het buitenland is de tendens dat de politiek en burgers zich sterk maken voor kaders en maatregelen in Europees verband, en ook voorstander zijn van intergouvernementele afspraken met bijvoorbeeld de VS.