PRIVACY FIRST
eigen keuzes in een vrije omgeving

Privacy in de verkiezingsprogramma's van 2017

Een analyse van de verkiezingsprogramma's voor de Tweede Kamerverkiezingen

Stichting Privacy First
Amsterdam

Opgesteld door Esther Gruppen

9 maart 2017

Tel. 020 – 8100279. Correspondentie: info@privacyfirst.nl. Postbus 16799, 1001 RG Amsterdam. Privacy First is een ANBI-erkende stichting.

Inhoudsopgave

GroenLinks, D66, Partij voor de Dieren en Piratenpartij doen het goed als het om Privacy gaat

Met de naderende verkiezingen heeft Privacy First de verkiezingsprogramma's onder de loep genomen. In welke mate erkennen de partijen die volgens de peilingen zetels zullen krijgen in de Tweede Kamer, het belang van privacy? Zijn zij zich ervan bewust dat burgerrechten zoals privacy steeds meer onder druk komen te staan? De overheid krijgt steeds meer macht over de burger door het verzamelen, analyseren en het gebruik van persoonsgegevens. Vaak wordt terrorismebestrijding of veiligheid aangedragen als legitieme reden om het recht op privacy te beperken. Van de nadelige gevolgen hiervan zijn veel politieke partijen zich niet voldoende bewust. Ook de macht van bedrijven neemt toe: zij gebruiken 'Big Data' voor commerciële doeleinden en dringen op deze wijze diep door in onze persoonlijke levenssfeer, zonder dat wij ons hiervan bewust lijken te zijn. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van privacywetgeving bij zowel de overheid als bedrijven, maar helaas staan hun werkzaamheden onder druk door de beperkte capaciteit.

Aangezien de Tweede Kamer de wetgevende macht is, zullen zittende politieke partijen er goed aan doen om burgerrechten, waaronder ook het recht op privacy, niet te beperken maar juist te bevorderen en te promoten. Helaas nemen politieke partijen het echter niet altijd even nauw met burgerrechten, zoals ook bleek uit een onlangs uitgebracht rapport van de Nederlandse Orde van Advocaten, waarin duidelijk werd dat veel verkiezingsprogramma's op gespannen voet met de rechtsstaat staan. Privacy First gaat hierop door en zet de programma's specifieker af tegen het recht op privacy. De resultaten zijn divers: van schokkend tot veelbelovend.

Volgens Privacy First is er grofweg een driedeling te maken. Er zijn partijen die een voortrekkersrol innemen door niet alleen met (nieuwe) initiatieven te komen om privacy beter te waarborgen, maar door ook actief bij te dragen aan de bewustwording van het belang ervan. Hiermee onderscheiden zij zich van de tweede categorie partijen waarbij bewustwording en een voortrekkersrol minder (of niet) aanwezig zijn. De laatste categorie brengt het er slecht vanaf: voorgestelde maatregelen zijn in tegenspraak met het privacyrecht of het onderwerp komt überhaupt niet ter tafel.

De partijen die zich sterk maken voor privacy

Privacy First is vooral enthousiast over de verkiezingsprogramma's van GroenLinks en D66. De Partij voor de Dieren en, niet verbazingwekkend, de Piratenpartij zijn goede opvolgers. Dat de Partij van de Dieren (PvdD) geen one-issue partij is blijkt duidelijk uit hun verkiezingsprogramma. Innovatie en technologie brengen kansen en voordelen, maar ook uitdagingen en risico's met zich mee, bijvoorbeeld bij de inzet van Big Data en profiling.

Daarnaast vindt de PvdD, net als de SP en GroenLinks, dat communicatie beter beschermd moet worden. De PvdD wil dat de overheid luistert naar de wensen van de burger 'zonder

die burger af te luisteren'. Hiermee verwijst ze naar de vele taps die in Nederland geplaatst worden. Dat dit aan banden gelegd moet worden, wordt gedeeld met GroenLinks. Nederland tapt het telefoonverkeer aanzienlijk vaker dan omringende landen. Dit is onnodig en moet veranderen. Inlichtingen- en veiligheidsdiensten mogen niet langer taps plaatsen zonder tussenkomt van de rechterlijke macht, aldus GroenLinks. Ook benadrukt ze dat de communicatie van journalisten en die tussen advocaat en cliënt niet mag worden afgeluisterd. Beiden zijn immers essentieel voor de persvrijheid en een functionerende rechtsstaat.

GroenLinks draagt verreweg de meeste privacy-onderwerpen aan, maar D66 doet er niet veel voor onder. D66 ziet graag dat Nederland koploper wordt met de beste digitale infrastructuur. Er wordt daarom groots ingezet op innovatie, waarbij een open, vrij en veilig internet essentieel is. Verder leggen ze het immer actuele rapport iOverheid van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) uit 2011 niet zomaar naast zich neer. De WRR deed destijds de aanbeveling tot het opzetten van een iPlatform. Een commissie zal dan jaarlijks bijeenkomen om de relatie tussen technologie en burgerrechten, zoals privacy, te bespreken in de Eerste en Tweede Kamer. Dit is wenselijk, omdat technologische ontwikkelingen snel gaan en het juridische aspect dit amper kan bijbenen. Technologische vooruitgang mag nooit voorbijgaan aan het belang van burgerrechten, zo vindt Privacy First.

Een voorbeeld van technologische vooruitgang is ook de drone. D66 besteedt hier, net als GroenLinks, aandacht aan. Drones kunnen tegenwoordig door particulieren, de overheid en het bedrijfsleven gebruikt worden voor verschillende doeleinden. Het is hierbij belangrijk om de voorwaarden voor dit gebruik onder de loep te nemen. Mogen filmopname in uw privé-omgeving die gemaakt zijn door een drone, zonder randvoorwaarden gemaakt worden? Welke rechten heeft u over dit gemaakte materiaal, zodat u hiertegen bezwaar kan maken? Dit zijn belangrijke vragen waarover meer duidelijkheid dient te komen. D66 en GroenLinks zien deze noodzaak en vragen privacywaarborgen rondom drones.

De Piratenpartij sluit zich erbij aan dat we niet overal gefilmd mogen worden. Zij wil daarom dat we paal en perk stellen aan cameratoezicht. Daarnaast is ze voorstander van de mogelijkheid om anoniem te kunnen betalen én reizen. Privacy First vindt het goed om te zien dat de Piratenpartij zich kritisch opstelt tegenover automatische nummerplaatherkenning (ANPR) en tegenstander is van RFID-chips in kentekens en kilometerheffing. Daarnaast is de Piratenpartij, net als Privacy First, voorstander van de mogelijkheid om anoniem te kunnen parkeren. Het is niet verbazingwekkend dat de Piratenpartij een grote nadruk legt op privacy, aangezien burgerrechten één van hun peilers zijn. Dit blijkt ook uit het feit dat de Piratenpartij voorstander is van asielverlening aan Edward Snowden.

De partijen die zich bewust zijn van het belang van privacy

Partijen die in de middencategorie vallen zijn de SP, de ChristenUnie, en de PvdA. De CU is kort in haar verhaal over privacy, maar desalniettemin wordt een duidelijk verhaal neergezet waarin ze ons bewust maakt van de risico's die technologische vooruitgang met zich meebrengt. Zo zegt ze bijvoorbeeld treffend: 'Ben je nog wel onschuldig tot het tegendeel is bewezen, als je vaker geconfronteerd wordt met aanhoudingen en controles omdat je in een bepaald risicoprofiel valt?' (CU 2017, p.62). Ook de SP stelt voorop dat niemand bij voorbaat verdacht is. Ze spreekt zich daarom duidelijk uit tegen het Sleepnet, waarbij inlichtingen- en veiligheidsdiensten meer mogelijkheden krijgen ten koste van onze privacy.

Ondanks de vele positieve statements van de SP, is er ook iets om ons zorgen over te maken. De SP is namelijk voorstander van betere informatie-uitwisseling over potentiële terroristen tussen geheime diensten in de EU en VS. Hierbij merkt de Nederlandse Orde van Advocaten terecht op dat hiervoor belangrijke voorwaarden ontbreken in het SP-verkiezingsprogramma. Zonder deze uitleg komen door deze informatie-uitwisseling mogelijk fundamentele rechten zoals het recht op privacy onder druk te staan (NOvA, 2017). Dit is het enige punt waarop de SP niet consequent handelt ten aanzien van privacy. Tevens lijkt ze hiermee eerdere uitspraken als tegenstander van het sleepnet tegen te spreken. Desalniettemin is de SP op tal van andere punten, evenals de PvdA en CU, wel eenduidig: bij alle voorgestelde maatregelen die mogelijk een inbreuk zijn op ons privéleven, wordt het privacyrecht als randvoorwaarde benoemd.

De partijen die het belang van privacy nauwelijks lijken in te zien

De partijen die het slechtst uit de bus komen, besteden amper of geen aandacht aan het privacyvraagstuk. Dit zijn 50Plus, het CDA, de PVV en de SGP. De VVD benoemt privacy, maar vindt veiligheid vaak belangrijker. Het opsporen van criminaliteit of terrorisme is van groots belang voor de VVD. Hier is de SGP het mee eens. Privacy First stelt echter dat dit problematisch kan zijn indien duidelijke randvoorwaarden ontbreken. Als er geen duidelijkheid is wanneer veiligheid zwaarder weegt, dan levert dit strijd op met het recht op privacy. Het is namelijk niet geoorloofd dat veiligheidsdiensten zomaar een inbreuk kunnen maken op ons privéleven. Een ander verontrustend punt komt van 50Plus. Zij zien graag de introductie van een digitaal paspoort waardoor anoniem internetten onmogelijk wordt.

Het CDA noemt het belang van privacy slechts één keer. Dit is in het kader van de inlichtingen- en veiligheidsdiensten. Verder lijkt het waarborgen van ieders privéleven van weinig belang te zijn voor het CDA. Nog zorgwekkender is het PVV-verkiezingsprogramma waarin met geen enkel woord gerept wordt over privacy. Zou het voor deze partijen niet zoveel uitmaken of duizenden onschuldige burgers met de invoering van een sleepnet bij voorbaat al behandeld worden als verdachte? En dat een perfecte bescherming van onze persoonsgegevens noodzakelijk is, zodat ze niet zomaar op straat komen te liggen of in verkeerde handen vallen?

VVD

De VVD in het kort

In het verkiezingsprogramma van de VVD wordt weliswaar aandacht besteed aan het privacyvraagstuk, maar veiligheid lijkt al snel zwaarder te wegen. Is er sprake van (een dreiging van) geweld, dan weegt het privacyrecht beduidend minder zwaar. Ook cameratoezicht wordt aangemoedigd, zonder duidelijke randvoorwaarden hiervoor te scheppen. Verder is de VVD er voorstander van om (toch vaak privacygevoelige) data te delen en beschikbaar te stellen aan derden met als doel vaak innovatie, bijvoorbeeld de ontwikkeling van nieuwe applicaties voor het (openbaar) vervoer. In de zorg moedigt ze het delen van data ook aan, terwijl aangenomen mag worden dat het delen van medische gegevens toch wel extra privacymaatregelen vereist. De VVD wil alle medische gegevens op een veilige manier in één dossier. De communicatie kan dan makkelijker en zorg beter, aldus de VVD. Ze benadrukt dat de gegevens eigendom blijven van de patiënt, hij toestemming moet verlenen voor het inzien ervan en zicht heeft op wie de gegevens inziet. Toch is ze hier minder duidelijk in dan bijvoorbeeld de SP.

Het standpunt van de VVD met betrekking tot privacy is niet overtuigend. Ze benadrukken in hun paragraaf weliswaar dat vrijheid en dus privacy essentieel is. Echter, voortellen doen anders vermoeden en noodzakelijke privacymaatregelen ontbreken vaak. Ook spreken ze zich in de Tweede Kamer positief uit over het sleepnet: een constructie die op grote schaal privacy-rechten schaadt. Net als Privacy First, ervaart de Nederlandse Orde van Advocaten het verkiezingsprogramma van de VVD op dit front als zorgwekkend. Het geven van een speciale opsporingsbevoegdheid aan de politie om cybercrime tegen te gaan, ‘kan zonder nadere waarborgen schending van het recht op privacy van burgers met zich brengen’ (NOvA 2017, p.30).

De samenstelling van relevante punten

‘De vrije samenleving die wij graag willen, is alleen mogelijk in een veilig land’ (p12). In een van hun aandachtspunten geven zij hiervoor als mogelijk middel: ‘Overlastgevende relschoppers moeten sneller te maken krijgen met preventief fouilleren, cameratoezicht, samenscholings- en gebiedsverboden’ (p.13). De VVD legt tevens een grote focus op dreiging van buitenaf (lees terrorisme en jihadstrijders). Autoriteiten zoals politie, antiterreureenheden en krijgsmacht zouden meer middelen en personeel moeten krijgen, zodat ze kunnen afgaan op elke melding van mogelijk extreem geweld (p.13). ‘Ook in het kader van cybersecurity doen ze heel belangrijk werk. De bevoegdheden van de veiligheidsdiensten moeten aangepast worden aan nieuwe technologische ontwikkelingen en communicatiemiddelen, zodat zij dat belangrijke werk ook in de toekomst kunnen blijven doen. Ook criminelen gaan met hun tijd mee. Steeds meer misdaad vindt plaats via internet. Cybercrime willen we opsporen en strenger bestraffen. Daarnaast willen we het voorkomen, bijvoorbeeld door voorlichting over veilig internetgebruik. Maar ook door het inzetten van gespecialiseerde teams van politie en justitie, die hacken als speciale

opsporingsbevoegdheid hebben en nauw samenwerken met banken en bedrijven. De beschikbare kennis bij politie en justitie op het gebied van cybercrime en computer gerelateerde misdaad moet worden vergroot om de opsporing te verbeteren. Onze belangrijkste digitale systemen en netwerken moeten zo goed mogelijk worden beveiligd. We mogen criminelen niet de kans geven om Nederland plat te leggen met een cyberaanval' (p.13).
'Ontwikkelingen in cyberspace gaan razendsnel. Daarin moet Defensie meegaan en bij voorkeur vooroplopen. Cybercapaciteiten (zowel offensief als defensief) zijn onmisbaar in de conflicten van vandaag en morgen. Nederland wordt nu al dagelijks geconfronteerd met digitale aanvallen. De afgelopen jaren is geïnvesteerd in de digitale weerbaarheid van Defensie. Om ook in de toekomst ons mannetje te staan tegen digitale dreigingen, moeten we deze capaciteit de komende jaren verder uitbreiden (p.28)'.

Over veiligheids- en inlichtingendiensten zegt de VVD: 'deze teams gaan af op elke melding van mogelijk extreem geweld, zoals een aanslag. Omdat we er alles aan willen doen om geweld of de dreiging van geweld zo snel mogelijk te stoppen, willen we deze antiterreureenheden uitbreiden' (p.13). Hierbij rijst de vraag in hoeverre we het streven naar veiligheid en het voorkomen van dreiging ten koste mogen laten gaan van privacy. De steun van de VVD voor het sleepnet doet vermoeden dat privacy in dergelijke zaken van ondergeschikt belang is.

In het hoofdstuk ondernemerschap en innovatie staat: 'Het beveiligen en weerbaar maken van digitale systemen en netwerken is belangrijk om onze economie en samenleving draaiende te houden en om privacy en bedrijfsgeheimen te beschermen tegen cybercriminelen, hackers en andere actoren op het internet. Dit is een gedeelde verantwoordelijkheid tussen overheid en bedrijfsleven. Nederland heeft door haar sterke positie als digitale mainport, en haar kennis op het gebied van veiligheid, een kans zich te ontwikkelen en te profileren als 'safe place to do business'. Nieuwe, innovatieve methoden, een actieve rol van de overheid en een sterke samenwerking tussen overheid en bedrijfsleven zijn nodig om bedreigingen af te wenden. Het beveiligen en weerbaar maken van digitale systemen en netwerken is essentieel om onze economie en samenleving draaiend te houden, en om privacy en bedrijfsgeheimen te beschermen tegen cybercriminelen, hackers en andere actoren op het internet' (p.45).

Ook is er het belang om een onderwerp te vernoemen waar de VVD zelf niet privacy benoemt, maar dit wel van toepassing is, namelijk bij technologische ontwikkelingen van de zorg. Wanneer men de zorgen in het achterhoofd houdt over privacy met betrekking tot het elektronisch patiëntendossier (EPD) en de toegang van zorgverzekeraars hiertoe, dan kunnen er bedenkingen zijn over de volgende stukken uit het verkiezingsprogramma: 'E-health en andere technologische toepassingen kunnen helpen de regie op je eigen leven te houden en de kwaliteit van leven te verbeteren. Ook kun je door verschillende toepassingen op een laagdrempelige, snelle en veilige manier in contact komen met een arts. Deze vernieuwingen willen we daarom zo veel mogelijk stimuleren. Wij juichen toe dat

zorgverzekeraars bewezen effectieve en veilige e-Health-toepassingen en andere vernieuwende vorm van zorg ruim baan geven in hun inkoopbeleid. Om de benodigde technologische zorgvernieuwing breed uitgerold te krijgen in de hele zorg zijn echter ook andere, private financieringsconstructies nodig dan alleen de financiering via zorgverzekeraars. Zo kunnen verzekerden profiteren van deze nieuwe mogelijkheden. We moedigen zorgverleners ook aan om het gebruik van E-health en andere technologische toepassingen in hun medische richtlijnen en protocollen op te nemen. Voor de beste behandeling is het belangrijk dat alle medische gegevens op een veilige manier in één dossier[1] terechtkomen. Of het nu gaat om de metingen die iemand zelf thuis heeft verricht of de resultaten van de onderzoeken in het ziekenhuis. Daardoor wordt communicatie makkelijker, kan de kwaliteit verbeteren en nemen de administratieve lasten voor zorgverleners af. De medische gegevens moeten echter altijd eigendom van de patiënt blijven. Hij of zij moet zelf kunnen bepalen met wie de medische gegevens worden gedeeld, en heeft altijd zicht op wie de gegevens inziet. Alleen bij noodgevallen mogen zorginstellingen je gegevens opvragen en moeten je dan actief daarover informeren' (p.64).

Dat de balans van privacy enerzijds en veiligheids- of commerciële belangen anderzijds nogal eens ten koste gaat van privacy blijkt ook uit de verkiezingspunten met betrekking tot vervoer. 'Op dit moment zijn overheden nog verantwoordelijk voor het verkeersmanagement en het vaststellen van omleidingsroutes. Door het beschikbaar stellen van deze informatie voor gebruik in apps, navigatiesystemen en routeplanners wordt ruim baan geboden aan innovatie en slimme(re) toepassingen. Hierdoor wordt het gebruiksgemak voor de reiziger verbeterd, kunnen samenwerkingen tussen overheid en markt leiden tot het tijdig opsporen en aanpakken van belangrijke knelpunten of kunnen nieuwe, innovatieve oplossingen worden gezocht om de bereikbaarheid te verbeteren. Ook openbaarvervoerbedrijven moeten hun reizigersinformatie en **data delen en beschikbaar stellen.** Zo kunnen nieuwe applicaties worden ontwikkeld die bijvoorbeeld met één druk op de knop het verschil in totale reistijd kunnen berekenen tussen een rit per auto, openbaar vervoer of fiets. Waarbij ook rekening kan worden gehouden met loopafstanden, actuele vertrektijden van het openbaar vervoer en filelengtes' (p.75).

'Bij alle vormen van openbaar vervoer geldt dat we er veilig gebruik van moeten kunnen maken. Het is onacceptabel dat er medereizigers zijn die het OV-personeel agressief benaderen. De mensen die zich hieraan schuldig maken, zijn vaak zwartrijders. Die willen we daarom nog strenger aanpakken. De boete voor zwartrijden moet omhoog, er moet **meer camerabewaking** komen en op meer treinstations moeten de toegangspoortjes dicht. Mensen die niet met hun handen van OV-personeel kunnen afblijven, krijgen bovendien een permanent OV-verbod. Omdat blijkt dat zwartrijders ook vaak andere vormen van criminaliteit vertonen, willen we OV-bestanden en politiebestanden beter koppelen. Zo kunnen we deze mensen sneller en effectiever aanpakken' (p.76).

[1] Hiermee wordt hoogstwaarschijnlijk een EPD bedoeld.

Nu is het verhaal, tot nu toe, niet erg positief als het gaat om het recht op privacy. De VVD lijkt zich hier weinig om te bekoren. Echter, op de valreep doet ze hoopvollere uitspraken. Er wordt namelijk in een aparte paragraaf aandacht besteed aan privacy en de bescherming van persoonsgegevens. Zo stelt de VVD: 'Wat je thuis, op je werk of op je computer doet, gaat de overheid niets aan. Ook als bedrijven en overheid gegevens van je hebben, zoals informatie van boordcomputers en navigatiesystemen, dan blijft dat jouw informatie. Om potentiële terroristen te stoppen of aanslagen te voorkomen, moet het mogelijk zijn om te weten wie in welk vliegtuig stapt. Maar wat goedwillende mensen thuis doen en laten, of hoe het met je kinderen gaat, is informatie die gewoon van jezelf is. Wij vinden het dus heel belangrijk dat die gegevens niet zomaar op een gemeentehuis rondslingeren.

Of je iets voor jezelf wilt houden, bepaal je zelf.
• Als je digitaal communiceert met de overheid, gaat het vaak om privacygevoelige gegevens.
De verdere ontwikkeling van het DigiD-systeem moet daarom niet alleen gebruikersvriendelijk, maar ook heel goed beveiligd zijn. Dit betekent ook dat gegevens niet langs omwegen alsnog bij particuliere bedrijven terecht kunnen komen. Om ook de persoonsgegevens van zzp'ers optimaal te kunnen beschermen, willen wij dat voor zzp'ers het Burgerservicenummer (BSN) losgekoppeld wordt van hun BTW nummer.
• Wij willen een beter toezicht op overheden, instellingen en bedrijven die persoonsgegevens verzamelen. De toezichthouder (de Autoriteit Persoonsgegevens) toetst dan niet meer per geval. In plaats daarvan wordt bij iedere instelling – óók bij overheidsinstellingen – gecontroleerd of de bescherming van de persoonsgegevens op orde is. Bij veilig omgaan met persoonsgegevens hoort ook het minder verspreiden van persoonsgegevens. We willen dat er voortdurend kritisch gekeken wordt naar alle organisaties die gegevens ontvangen uit de Basisregistratie Personen (zgn.'afnemers'). In het bijzonder willen we dat kerken geen automatische toegang meer krijgen tot persoonsgegevens.
• Bedrijven en particulieren hebben een eigen verantwoordelijkheid (en de plicht) om persoonsgegevens goed te beveiligen. Dit geldt uiteraard ook voor gegevens die de overheid opslaat. Die gegevens moet de overheid goed beveiligen. Ook de werkplekken van de overheid moeten goed worden beveiligd. Alleen een antivirusprogramma is niet genoeg. Digitale inbraken moeten te zien zijn op het netwerk, zodat de overheid tijdig kan ingrijpen. De privacywetgeving komt uit de tijd dat de bescherming was gericht op de opslag van gegevens. Deze regelgeving wordt herzien, waarbij het gebruik van gegevens centraal komt te staan. Nederland zet zich ook in Europees verband hiervoor in.
• De hoeveelheid en de beschikbaarheid van onze data groeit enorm door de digitalisering van onze samenleving. Wij volgen deze ontwikkeling op de voet zodat deze ontwikkeling niet de vrijheid van mensen beperkt. Zonder privacy bestaat immers geen vrijheid. Ook geeft de overheid voorlichting over de gevolgen van deze digitalisering. Nederland moet een voorloper blijven als 'dataneutraal' land, zodat bedrijven en particulieren onbespied hun eigen keuzes kunnen blijven maken.

• Het recht op privacy is echter niet absoluut. Als iemand een terroristische daad of een andere ernstige misdaad heeft gepleegd – of als er zeer sterke aanwijzingen zijn dat hij dat gaat doen – verspeelt hij zijn recht op privacy. De veiligheid van Nederland en van individuele Nederlanders staat dan immers voorop. Dit mag niet willekeurig worden toegepast, maar alleen bij gerichte opsporingsactiviteiten en operaties. Het aftappen van telefoons van bijvoorbeeld terrorismeverdachten valt daaronder.
• In het bijzonder willen we de privacy van kinderen waarborgen. Zeker als ze in een kwetsbare positie zitten en onder toezicht van jeugdzorg staan. Alleen ambtenaren die betrokken zijn bij de zorg krijgen in beveiligde systemen toegang tot de gegevens van kinderen. Andere ambtenaren niet. Gemeenten moeten dit zo snel mogelijk op orde brengen. Burgemeesters hebben wel toegang, zodat ze eventueel kunnen ingrijpen als het mis dreigt te gaan' (p.97).

PvdA

De PvdA in het kort

De PvdA laat op verschillende momenten merken dat ze aan privacy en burgerrechten denkt. Zo benoemen ze privacy in het kader van technologische ontwikkelingen, maar ook wanneer het gaat over terrorismebestrijding. Bij laatstgenoemde promoten ze weliswaar extra investeringen (in technologie) voor inlichtingendiensten, maar inlichtingendiensten moeten zich te allen tijde houden aan de EVRM (waaronder dus ook privacy gerelateerde burgerrechten).

Daarnaast wordt privacy expliciet benoemd in een aparte paragraaf. De PvdA geeft met name aan dat er meer transparantie moet komen voor burgers. Zij hebben recht op meer zicht op wat er met hun data gebeurt bij de overheid, het bedrijfsleven en banken. 'Big Data' biedt kansen en voordelen, maar grootschalige gegevensverwerking moet op verantwoorde wijze gebeuren, waarbij privacy en dataveiligheid voorop staan. Tevens is de PvdA zich ervan bewust dat het koppelen en analyseren van bestanden het risico in zich heeft tot uitsluiting of stigmatisering.

De samenstelling van relevante punten

In het openingswoord van enkele pagina's staat:
'Technologische vernieuwing roept ook vragen op, op het terrein van de onderlinge communicatie, het functioneren van de democratie en de privacy. Oude, nieuwe en sociale media brengen ons een doorlopende stroom van nieuws, meningen en geruchten van over de hele wereld, in een veel hogere snelheid en intensiteit dan voorheen. Ons beeld van de werkelijkheid wordt met de minuut bijgesteld en geactualiseerd. Iedere burger wordt als 'nieuwsconsument' geacht daarin het kaf van het koren te kunnen scheiden. Steeds vaker zien wij dat normale onderlinge communicatie een commerciële waarde vertegenwoordigt, en dat raakt niet alleen aan de essentie van vrije communicatie, maar ook onze **privacy.** Omdat de samenleving alleen goed kan functioneren bij de gratie van een goede en evenwichtige informatievoorziening, zijn er nieuwe vaardigheden nodig om als burger door de bomen het bos te blijven zien. Voor een verbonden samenleving is het van groot belang dat we technologische vernieuwing inzetten om de kwaliteit van de samenleving als geheel te verbeteren' (p.7).

Op pagina 20 over terrorisme wordt gezegd:
'Betere samenwerking van veiligheidsdiensten in Europees verband tegen terrorisme is nodig om een nog sterkere vuist te maken tegen de internationale onveiligheid. De inlichtingendiensten mogen extra **investeringen doen in meer capaciteit en nieuwe technologie.**
• Vroegsignalering via school, leerplichtambtenaar, familie, politie, gebedshuizen, enzovoort is noodzakelijk om radicalisering tegen te gaan. Projecten in het kader van deradicalisering krijgen meer steun.

• We focussen op de strijd tegen IS en aanverwante organisaties. Dat is op dit moment de grootste terroristische bedreiging voor Europa.
• De PvdA houdt zich te allen tijde aan het Europees Verdrag van de Rechten van de Mens. Ook als het om terrorismebestrijding gaat' (p.20).

Dit zijn stukken uit de paragraaf over privacy:
3.4 Privacy
• Iedereen moet kunnen inzien wat de overheid van hen weet. Bij inloggen op mijn.overheid.nl moet duidelijk te zien zijn wat de overheid over je opslaat. Ook moet hier te zien zijn welke gegevens de overheid doorgeeft aan derden. Ook bedrijven moeten openheid gaan geven over wat zij van individuen weten.
• De overheid en het bedrijfsleven verzamelen steeds meer gegevens, in exponentieel groeiende databestanden. Deze 'Big Data' kan het werk van opsporingsdiensten makkelijker maken of een bijdrage leveren aan betere gezondheidszorg en onderwijs. De voordelen en kansen van grootschalige gegevensverwerking moeten op verantwoordde wijze de ruimte krijgen, zonder de risico's voor privacy en dataveiligheid uit het oog te verliezen. Het doel van verzameling en verwerking kan niet onbeperkt worden opgerekt. Het koppelen en analyseren van bestanden mag niet leiden tot uitsluiting of stigmatisering' (p.21).

Over de financiële sector zegt de PvdA:
• Betaalgegevens zijn van de klant, niet van de bank. Banken beschikken alleen over de gegevens, omdat zij een nutsfunctie hebben: het veilig en goed laten verlopen van het betalingsverkeer. Banken mogen betaalgegevens niet verkopen aan derden. De gedragscode waarin de omgang met betaalgegevens is geregeld, willen wij aanpassen, waarbij de bescherming van privacy voorop staat' (p.25).

50Plus

50Plus in het kort

De 50Plus-partij geeft zijn verkiezingsprogramma weer aan de hand van -hoe toepasselijk- 50 punten. Op twee punten komt het onderwerp privacy naar voren. Ten eerste onder punt 35 waarin staat dat ‘anoniem internetgebruik moet worden tegengaan door de invoering van een digitaal paspoort’ (p.11). Dit levert echter mogelijk strijd op met het recht op privacy. Deze zorg wordt gedeeld met de Nederlandse Orde van Advocaten.
Ten tweede is er een rubriek met ‘wat 50Plus verder vindt…’ waarin staat dat ‘naast de rijksoverheid ook bedrijven en organisaties moeten investeren in cyberveiligheid’. Korter kunnen we het haast niet maken, daarom is een samenstelling van relevante punten ook onnodig.

SP

De SP in het kort

De SP is duidelijk: niemand is bij voorbaat verdacht en dient daarom ook niet als dusdanig behandeld te worden. Daarom spreekt ze zich expliciet negatief uit over het sleepnet. Daarnaast wil ze net als de PvdA meer transparantie over wat er met onze data gebeurt en de mogelijke gevaren hiervan. Opmerkelijk is dat de SP meermaals benadrukt dat digitale privécommunicatie dezelfde (grondwettelijke) bescherming dient te krijgen als papieren post. Daarnaast moet de Autoriteit Persoonsgegevens worden versterkt, zodat zij beter op kunnen treden bij privacy overtredingen. Tot slot, de SP is – veel meer dan de VVD – erg kritisch naar het EPD en de risico's voor privacy die hiermee gepaard gaan.

Er is echter één onderwerp waarbij de SP het belang van privacy maatregelen over het hoofd ziet, zo stelt de Nederlandse Orde van advocaten: 'Geheime diensten in Europa en onder meer de VS moeten volgens de SP meer ruimte krijgen om zonder voorwaarden informatie te delen over potentiële terroristen' (p.30). Onduidelijk blijft wie bepaalt wie als een potentiële terrorist moet worden aangemerkt en wanneer informatie vrij gewisseld mag worden met buitenlandse inlichtingendiensten. Zonder nadere uitleg komen daarmee fundamentele rechten zoals het recht op privacy en het recht op een behoorlijk proces onder druk te staan', aldus de Nederlandse Orde van Advocaten (NOvA 2017, p.28).

De samenstelling van relevante punten

Privacy wordt meermaals benoemd in het SP verkiezingsprogramma, waarvan de eerste keer in het kader van banken en hun verantwoording om de privacy van hun klanten te waarborgen. 'Betaalgegegevens mogen daarom niet commercieel gebruikt worden', volgens de SP (p.17). Vervolgens krijgt privacy uitgebreid de aandacht in de paragraaf 'Een veilig en vrij Internet'.
Als het om privacy gegevens gaat is de SP duidelijk: **'Mensen die nergens van worden verdacht, moeten ook niet bang hoeven zijn dat ongevraagd gegevens over hen worden verzameld' (p.39)**. Daarom dient de AIVD ook geen sleepnet te krijgen om zoveel mogelijk gegevens van zoveel mogelijk mensen binnen te halen. 'Overheden en bedrijven mogen geen persoonsgegevens doorverkopen of doorgeven zonder uitdrukkelijke toestemming van de betrokkenen. Overheden gaan niet automatisch gegevens aan elkaar koppelen voor datamining en profiling en zijn open en transparant over eventuele inzet van deze middelen voor maatschappelijke doelen' (p.39). **Voor banken, verzekeraars en andere bedrijven moeten ook duidelijkere regels komen over data.** Het moet duidelijk zijn wat banken, verzekeraars en andere bedrijven over mensen mogen verzamelen en mogen besluiten op basis van statistische analyses van persoonsgegevens. **Verder krijgen 'E-mails, persoonlijke berichten en andere privécommunicatie op het internet dezelfde (grondwettelijke) bescherming als de papieren post nu heeft'** (p.39).

Over de bescherming van privacy wordt verder gezegd: ‘Overheden maken zoveel mogelijk gebruik van open source en zorgen ervoor dat hun systemen leverancier onafhankelijk zijn, onder meer door het gebruik van open standaarden. Software voor de overheid wordt zoveel mogelijk eerst intern ontwikkeld, om de afhankelijkheid van externen te beperken’ (p.39). **Daarnaast moet de Autoriteit Persoonsgegevens worden versterkt**, zodat beter kan ‘worden opgetreden wanneer de privacy van mensen in het geding is’ (p.40).

Tot slot, over het EPD is de SP expliciet in zijn standpunt: ‘Patiëntengegevens en medische dossiers worden veilig bewaard en mogen alleen worden uitgewisseld met uitdrukkelijke toestemming van de patiënt. Uitwisseling van gegevens moet altijd veilig en versleuteld plaatsvinden. We stoppen met het LSP (landelijk schakelpunt)’ (p.40).

ChristenUnie

CU in het kort

De CU neemt de problemen rondom privacy serieus. Ze legt duidelijk uit waar de gevaren liggen wanneer we privacy niet voldoende beschermen. Deze uitleg wordt met concrete voorbeelden versterkt waardoor de CU niet alleen zijn standpunt naar voren brengt maar ook bewustwording probeert te creëren onder publiek dat niet zoveel stilstaat bij mogelijke gevolgen van 'Big Data' en profiling. Zo zegt ze treffend: 'Ben je namelijk nog wel onschuldig tot het tegendeel is bewezen, als je vaker geconfronteerd wordt met aanhoudingen en controles omdat je in een bepaald risicoprofiel valt?' (p.62).

Eén van de maatregelen die genomen dient te worden is bijvoorbeeld de oprichting van een expertisecentrum ('waar burgers en het bedrijfsleven met vragen terecht kunnen over (Big) data en de bescherming van privacy'). Dit is een uniek idee van de CU. Tegelijkertijd moet er meer transparantie vanuit de overheid en controle van de Autoriteit Persoonsgegevens komen.

De CU is weliswaar kort in zijn standpunt over privacy, maar wel krachtig en durft tevens initiatief te tonen. Elders in het verkiezingsprogramma staat weinig met betrekking tot privacy, maar dit lijkt simpelweg omdat de focus ligt op (religieuze) waarden en een sociale samenleving. Het is bondig, maar tegelijkertijd wordt nergens het belang op privacy tegengesproken en blijft de CU dus consequent in haar privacy standpunten.

De samenstelling van relevante punten

In één van haar paragrafen besteedt de ChristenUnie uitgebreid aandacht aan het privacyvraagstuk.
'Behoefte aan privacy is inherent aan het mens-zijn. Zelf bepalen met wie we onze gedachten en gevoelens delen stelt ons in staat relaties aan te gaan met mensen om ons heen en ons te ontwikkelen. De uitspraak 'ik heb niets te verbergen' ontkent deze noties. **Privacy is waardevol en verdient daarom ook in het digitale tijdperk onze bescherming.** De toegenomen hoeveelheid data en verwerking ervan biedt veel gemak in het dagelijkse leven (sociale media, apps op smartphones) en kansen voor bedrijven en overheden. Zo kan een postbezorger met het oog op efficiëntie voor elk adres in Nederland bijhouden wanneer iemand thuis is. Dit is vanuit privacy- en veiligheidsoverwegingen echter een gevaarlijke ontwikkeling. En de mogelijkheden van "big data" voor de bestrijding en opsporing van misdaad en fraude zijn nuttig, maar leveren ook een dilemma op voor privacy en de onschuldpresumptie. **Ben je namelijk nog wel onschuldig tot het tegendeel is bewezen, als je vaker geconfronteerd wordt met aanhoudingen en controles omdat je in een bepaald risicoprofiel valt?** Bijvoorbeeld door jouw postcodegebied of etnische afkomst. De kansen van "big data" dienen niet onbenut te blijven, maar worden in een democratische rechtsstaat wel aan controle onderworpen.
De ChristenUnie stelt daarom de volgende maatregelen voor:

- De overheid richt een **expertisecentrum** in waar burgers en het bedrijfsleven met vragen terecht kunnen over (big) data en de bescherming van privacy.
- Toegang en controle eigen gegevens. Gegevensverwerkingssystemen van de overheid kunnen eenvoudig worden geraadpleegd door de burger en geven zo controle over de verzamelde gegevens.
- Controle door de Autoriteit Persoonsgegevens. **De overheid is transparant** over de data die zij verwerkt en welke analysemethoden en algoritmen zij gebruikt bij “big data” in de context van opsporing. De Autoriteit Persoonsgegevens krijgt de bevoegdheid en middelen om dit te controleren.
- Cybersecurity op de agenda. Nederland scoort hoog als het gaat om digitalisering van de economie, zoals internetbankieren. Maar we zijn daarmee ook kwetsbaar voor dreigingen in het cyberdomein. De cybersecurity-sector is belangrijk voor preventie en herstel na moedwillige en schadelijke activiteiten op ICT-terrein. Start-ups in deze sector worden fiscaal gestimuleerd.
- Voorkomen van informatiedementie van de overheid door wetgeving op het terrein van privacy, transparante overheid en archieven aan te passen aan het digitale tijdperk’ (p.62).

GroenLinks

GroenLinks in het kort

Net als de SP wilt GroenLinks dat digitale privéberichten dezelfde rechten krijgen als post. Verder wil GroenLinks, net als enkele andere partijen, meer capaciteit voor de Autoriteit Persoonsgegevens, meer transparantie rondom Big Data en geen sleepnet. Maar GroenLinks gaat wat stappen verder en is in een drietal punten uniek ten opzichte van andere partijen. Zo wil ze bijvoorbeeld dat de overheid jaarlijks het aantal geplaatste taps publiceert. Daarnaast wordt de mogelijkheid van het plaatsen van taps verder aan banden gelegd. Plaatsen van taps op journalisten of de communicatie tussen advocaat en cliënt moet worden gebonden aan voorafgaande rechtelijke toestemming. Dit wordt voor journalisten aangevuld met een wettelijke bronbescherming die zij dienen te krijgen (laatst genoemde delen ze met de Piraten Partij).

Verder moet er meer regelgeving komen voor drones (drones worden ook door D66 genoemd) en GroenLinks ziet, net als de PvdD, graag de identificatieplicht verdwijnen. Privacy First vindt het goed om te zien dat GroenLinks de bewaarplicht van telecomgegevens wil afschaffen. Dit is een belangrijke onderwerp voor Privacy First.

Kortom, het verkiezingsprogramma gaat verder dan die van eerder genoemde partijen (VVD, PvdA, 50Plus, SP, CU), door te komen met nog niet eerder benoemde initiatieven.

De samenstelling van relevante punten

GroenLinks is zich bewust van het gevaar van privacy schending in de zorg: ‘Het medisch beroepsgeheim blijft gewaarborgd. Zonder toestemming van de patiënt krijgen zorgverzekeraars geen toegang tot medische dossiers’ (p.39).

In het kader van veiligheid wordt gezegd: ‘Zonder af te doen aan onze vrijheid moeten terrorisme en criminaliteit bestreden worden. We moeten voorbereid zijn op de reële dreigingen die er zijn. GroenLinks wil investeren in recherchewerk om zeer gericht criminaliteit op te sporen en terrorisme te voorkomen’ (p.62).
Bij de bestrijding van terrorisme komt de nadruk te liggen op het verzamelen van inlichtingen uit menselijke bronnen en ‘**gerichte digitale surveillance in plaats van massasurveillance**. De veiligheidsdiensten zetten geen ‘sleepnet’ in om grootschalig communicatie af te tappen. Zij publiceren jaarlijks het aantal taps dat zij hebben geplaatst. Nederland maakt zich sterk voor betere uitwisseling van informatie tussen veiligheidsdiensten en betere samenwerking tussen opsporingsdiensten binnen de Europese Unie’ (p.64).

‘We beschermen vrijheid in een digitale samenleving. Zonder internet is onze samenleving niet meer denkbaar. Het internet moet open en vrij zijn. Dat vraagt om scherpere uitwerking van onze grondrechten. Of het nu via e-mail of WhatsApp is, ook op internet hebben wij

recht op privacy. Het is het briefgeheim van de 21e eeuw. Onze persoonlijke gegevens mogen niet misbruikt worden ten koste van onze privacy. Ook het internet moet beschermd worden tegen misbruik en criminaliteit. De overheid investeert in cyber security en stelt eisen aan bedrijven en organisaties' (p.61).

- '11. Privacy is het uitgangspunt bij bouw en beheer van alle gegevensbestanden. De overheid geeft openheid over het gebruik van big data en profilering. De overheid ziet toe op een veilig en privacyvriendelijk ontwerp van apparaten die met het internet verbonden zijn en op bescherming van persoonsgegevens die via het internet der dingen worden verzameld. Persoonsgegevens die door de overheid worden verzameld worden opgeslagen in Nederland.
- 12. Grondrechten gelden ook op het internet. **Het briefgeheim in de Grondwet wordt uitgebreid tot een communicatiegeheim** dat ook verkeersgegevens en opgeslagen communicatie omvat**. De bewaarplicht voor telecom- en internetgegevens wordt definitief afgeschaft.** In plaats daarvan krijgen opsporings- en veiligheidsdiensten de mogelijkheid om gegevens van verdachte personen te laten bewaren en, met toestemming van de rechter, te bekijken.
- 13. Ook bij cyber security worden grondrechten gerespecteerd. De beveiliging van de computersystemen van (semi-)overheidsinstellingen wordt aan periodieke audits onderworpen. **De overheid bevordert kennis en gebruik van veilige encryptie**, zonder achterdeurtjes.
- 14. Nederland maakt zich sterk voor een open en neutraal internet, ook binnen de Europese Unie. Hyperlinken en embedden blijven vrij. Er komt een einde aan geoblocking zodat programma's ook in het buitenland toegankelijk zijn. Binnen de Europese Unie zet Nederland zich in voor afschaffing van het **downloadverbod.**
- 15. **Journalisten krijgen een wettelijke bronbescherming**, inclusief het verschoningsrecht om te weigeren vragen te beantwoorden. Het aftappen van journalisten en van de communicatie tussen **advocaten en hun cliënten** wordt gebonden aan voorafgaande rechterlijke toestemming.
- 16. Regelgeving voor **civiele drones** beschermt de persoonlijke levenssfeer, alsmede de veiligheid van het luchtruim en bewoond gebied. Hulp- en opsporingsdiensten gebruiken de door drones verzamelde informatie slechts voor het doel waarvoor de vlucht is uitgevoerd.
- 17. De overheid is terughoudend in het aantasten van de vrijheid van meningsuiting op internet en past geen automatische filters en voorafgaande controle toe. Aanbieders van sociale media worden niet ingezet als hulppolitie richting hun gebruikers en worden geacht hun gedragsregels transparant en consequent toe te passen, om discriminatie en willekeur tegen te gaan.
- 18. Om de digitale communicatie van iedereen veilig te houden, maken alle overheidsinstellingen beveiligingsproblemen in computersystemen altijd op verantwoorde wijze openbaar.

- 19. De Autoriteit Persoonsgegevens krijgt meer capaciteit om privacy schendingen aan te pakken en gaat ook instellingen en bedrijven begeleiden bij het organiseren van de opslag van persoonsgegevens' (p.67).

Opvallend is dat GL stelt dat de **identificatieplicht** moet worden afgeschaft (p.64).

D66

D66 in het kort

D66 heeft ambities met Nederland. In 2030 moet Nederland digitale koploper en een veilige datahaven zijn. Hiervoor is het belangrijk dat er door de overheid een iPlatform wordt ingevoerd waarin burgers en organisaties kritisch kunnen reflecteren op de digitale samenleving. Ook wordt hierin jaarlijks besproken wat de relatie is tussen technologie en grondrechten zoals privacy. Dit platform is een aanbeveling van het WRR-rapport 'iOverheid' uit 2011. Verder stelt D66 dat data vergaring en gebruik transparanter moet ten einde innovatie te stimuleren.

Over bijvoorbeeld CETA en civiele drones is D66 duidelijk; beide zijn alleen wenselijk indien privacy en gegevensbescherming gewaarborgd zijn. Wanneer het brandstofaccijns en autobelasting betreft, sluit D66 zich bij GroenLinks aan. Betalen naar gebruik is een goed idee, mits dit het recht op privacy niet schaadt. In alle initiatieven die D66 neemt, past ze consequent de randvoorwaarden voor privacybescherming toe. Desalniettemin zijn er een aantal privacy gerelateerde zaken waar D66 niet over spreekt, in tegenstelling tot bijvoorbeeld GroenLinks en de Piratenpartij die ook tagging en het plaatsen van taps naar voren brengen.

De samenstelling van relevante punten

'Nederland wordt de digitale koploper in Europa met de beste digitale infrastructuur en vaardigheden. Daarbij hoort een open, vrij en veilig internet' (p.8).
In het kader van een robuuste rechtsstaat zegt d66: 'Wij zorgen voor bescherming van privacy en beschikking over digitale privégegevens' (p.10).

Net als de VVD, wil D66 dat niet-privacy gevoelige informatie vrijkomt voor innovatie. Hierover zeggen zij: 'Alle niet persoonlijke of gevoelige overheidsdata moet worden ontsloten als open data. Informatiebestanden die met belastinggeld zijn aangelegd moeten vrij toegankelijk zijn. Dit maakt niet alleen controle op de overheid makkelijker, maar leidt ook tot innovaties' (p.72). Hierbij benoemt ze het belang van privacy: 'Big data biedt veel mogelijkheden voor wetenschappelijk onderzoek. D66 wil die mogelijkheden benutten, uiteraard met oog voor de privacy van mensen en patiënten' (p.72).

'De digitale agenda raakt vele beleidsterreinen en departementen. Dat vraagt om coördinatie. D66 wil dat de regering een Digitale Driehoek voor technologie- en internetbeleid vormt, bestaande uit de ministeries van Binnenlandse Zaken, Justitie en Economie en Technologie, waarbij ook de digitale markt en digitale handel op de agenda staan. Naast deze drie ministeries zijn er vijf sterke en onafhankelijke toezichthouders: het NCSC (cybersecurity), de CTIVD (inlichtingendiensten), het BIT (projecttoetsing), de AP (persoonsgegevens) en de ACM (mededinging). **Op basis van de aanbevelingen van het WRR-rapport 'iOverheid' uit 2011 wordt een iPlatform ingesteld** waar burgers en

organisaties kritisch kunnen reflecteren op de digitale samenleving en er komt een jaarlijkse bespreking van de relatie tussen technologie en grondrechten, zoals privacy, in beide Kamers, die wordt voorbereid door een speciale commissie' (p.73).

Bij meerder orderwerpen houdt D66 het belang van o.a. privacy in het oog. Dit blijkt ook uit hun steun voor handelsverdragen zoals CETA, waarbij ze aangeven dat privacy een belangrijke voorwaarde zal zijn.
'Tegelijkertijd eist D66 heldere waarborgen voor milieu, privacy, consumentenbescherming en de voortdurende zeggenschap hierover voor Europese en Nederlandse beleidsmakers. Wanneer meer details bekend zijn, kunnen wij ons oordeel pas echt vellen' (p.75).

'D66 wil af van de ingewikkelde combinatie van autobelastingen als accijnzen, aanschafbelasting en wegenbelasting. We willen naar betalen voor gebruik van de auto in plaats van betalen voor bezit. Daarbij kan de daadwerkelijke CO2-uitstoot meegewogen worden. Daarvoor is nu ook nieuwe technologie beschikbaar die weinig investeringen vergt en waarbij de privacy van weggebruikers gewaarborgd is' (p.82).

'De maatschappelijke voordelen van de inzet van **civiele drones** kunnen groot zijn, mits de veiligheid en de privacy- en gegevensbescherming geborgd zijn. Extra inzet op handhaving is noodzakelijk' (p.86).

'Belang van privacy en medisch beroepsgeheim
Mede als gevolg van digitalisering, innovaties rond e-Health, preventie en de toenemende kracht van big data is er meer en meer mogelijk. Dit biedt enorme kansen voor gezondheid, maar brengt ook risico's voor privacy met zich mee. Dit kan beperkingen opleveren voor het delen van tot de individuele patiënt herleidbare gezondheidsinformatie, maar dat mag niet verworden tot een oneigenlijk argument tegen zorginnovatie. De patiënt heeft altijd het recht te beschikken over zijn medische gegevens. D66 streeft naar een gedecentraliseerde uitwisseling van gegevens, zodat medische informatie niet buiten het zicht van arts en patiënt uitgewisseld kan worden en het medisch beroepsgeheim onaangetast blijft' (p.106).

'Privacy in een digitale wereld
Vrijheid begint met het recht op de eigen levenssfeer. We kunnen ons ontwikkelen en ontplooien doordat we in vrijheid en veiligheid op onszelf en met anderen kunnen zijn en communiceren. Onbespied en onbewaakt kunnen leven en zelf kunnen bepalen wie welke informatie over ons krijgt, is een kernwaarde in een open en vrije samenleving. Privacy als grondrecht betekent daarmee persoonlijke vrijheid en veiligheid. In een digitale wereld neemt het risico op verlies aan privacy snel toe. Door toenemende dataregistratie en voortschrijdende techniek staat privacy in onze samenleving steeds meer onder druk. Er worden steeds meer persoonsgegevens en andere persoonlijke informatie verzameld, bekeken en gedeeld met bekende maar ook onbekende derden of zelfs doorverkocht. Dit doen we zelf, het gebeurt door de overheid en ook door bedrijven. Er is sprake van een transparantieparadox, waarbij burgers steeds transparanter worden, terwijl overheden en

bedrijven juist steeds meer gesloten te werk gaan. Die paradox zullen we moeten doorbreken. Het verzamelen van gegevens gebeurt vaak zonder dat mensen het weten of zich bewust zijn van wat er met hun gegevens gebeurt of kan gebeuren. Zowel wijzelf als de overheid en bedrijven hebben daarmee een verantwoordelijkheid om zorgvuldig met onze privacy om te gaan. D66 wil daarom geen ongebreidelde dataverzamelingen door de overheid of door bedrijven, geen sleepnetten aan informatie over willekeurige mensen. Een adequate en zorgvuldige bescherming van persoonsgegevens door waarborgen, bewustwording en regels is nodig. Nederland is altijd een voorloper geweest in het streven naar een open en veilig internet. Het was het tweede land ter wereld dat netneutraliteit wettelijk verankerde. We liepen voorop met de leidraad Responsible Disclosure om ethische hackers te beschermen en zetten ons in voor sterke encryptie. **D66 heeft, hierop voortbouwend, de ambitie om Nederland in 2030 digitale koploper en veilige datahaven te laten zijn.** Dat kan alleen als grondrechten, zoals privacybescherming, gelijke pas houden met de technologische ontwikkelingen die we een warm hart toedragen. Om maximaal gebruik te kunnen maken van nieuwe technologieën zijn maatregelen nodig die gegevens van consumenten beschermen tegen inbreuken. We moeten waken voor de opkomst van een 'data proletariaat' waarin burgers afhankelijk zijn geworden van bedrijven en overheden die hun data beheersen en voor misbruik van kwetsbare groepen. Daarvoor is van belang dat consumenten en burgers weten wat de overheid en bedrijven aan gegevens over ons verzamelen, wat zij met die informatie doen en welke zeggenschap consumenten en burgers daar zelf over hebben. Punten van zorg zijn vooral dataveiligheid, databewustzijn, bescherming van de digitale persoonlijke identiteit en normen voor cyber-omgang. D66 vindt namelijk dat het individu zelf invloed moet kunnen uitoefenen op welke gegevens worden gedeeld met anderen. Maak mensen bewust van de hoeveelheid gegevens die wordt gedeeld en hoe zij invloed kunnen uitoefenen op welke gegevens met wie gedeeld worden, hoe en waarvoor die gegevens worden gebruikt en door wie. Daarmee ontstaat keuzevrijheid voor de consument om gegevens wel of niet te delen en krijgt de consument een positie ten opzichte van de overheid en bedrijven die constant gegevens vragen aan de burger en de consument. Die keuzevrijheid en autonomie dragen bij aan de persoonlijke vrijheid en veiligheid van mensen' (p.123-124).

CDA

CDA in het kort

Met een 105 pagina's tellend verkiezingsprogramma, zou je verwachten dat privacy als onderwerp wel ruimte krijgt. Helaas is dit nauwelijks het geval. De enige aandacht die het krijgt, is in het kader van veiligheid en de AIVD. Verruiming van zijn bevoegdheden moeten hand in hand gaan met het waarborgen van privacy. Echter, het CDA verzaakt om nadere toelichting te geven op de noodzakelijke waarborgen voor bescherming van het recht op privacy.
Een vluchtige zoekfunctie naar woorden als (big) data, transparantie, E-health, sleepnet, identificatieplicht krijgen geen enkele hit. Daarnaast lijkt het belang van privacy niet ergens impliciet vermeld te worden. Gezien de omvang en de zorg die aan dit verkiezingsprogramma is besteed, spant het CDA de kroon als het gaat om slecht privacybeleid.

De enige privacygerelateerde quote:

'Waar nodig worden de bevoegdheden van de AIVD of de andere diensten verruimd, bijvoorbeeld in het onderscheppen en ontsleutelen van communicatie. Verruiming van deze bevoegdheden moet wat het CDA betreft hand in hand gaan met extra waarborgen voor de privacy' (p.33).

SGP

SGP in het kort

De SGP wil investeren in bewustwording. Men moet beter op de hoogte zijn van de gevaren die verbonden zijn aan de publicatie van persoonlijke gegevens. Verder moet het strafrecht zodanig worden aangepast dat digitale vormen van afpersing tegen gegaan kunnen worden (p.36). Ook moet de beveiliging van overheidswebsites verbeteren en mogen persoonlijke gegevens niet zonder meer worden opgeslagen. Er is echter een paradox in het verhaal van de SGP. Zo zegt ze: 'Bescherming van mensenlevens in het kader van de strijd tegen terrorisme vraagt om onorthodoxe maatregelen. Juist om het privéleven te beschermen zijn soms ingrijpende inbreuken noodzakelijk. De waarborgen van de rechtsstaat zijn hierbij leidend' (p.36). De SGP geeft echter geen opheldering over de rol van deze waarborgen van de rechtsstaat en hoe deze afwegen tegen het recht op privacy.

De samenstelling van relevante punten

'Mensen hebben recht op de bescherming van hun privéleven tegen een al te opdringerige overheid, 'nieuwsgierige' bedrijven en anderen die in willen breken in andermans doen en laten. Inbreuken op de persoonlijke levenssfeer zijn alleen te rechtvaardigen als het gaat om de veiligheid van personen of de staat. De wetgeving hierover moet evenwichtig zijn en, als er sprake is van overtredingen, worden gehandhaafd. De voortgaande digitalisering vraagt wel extra alertheid.

- Bewustwording welke gevaren verbonden zijn aan het publiceren van allerlei persoonlijke gegevens is belangrijk. In opvoeding en onderwijs moet hiervoor voldoende aandacht zijn.
- De strafwet op het terrein van zeden biedt de nodige bescherming. Aanscherping is echter nodig om bijvoorbeeld ook digitale vormen van afpersing en dreiging met het publiceren van seksuele beelden krachtig tegen te kunnen gaan.
- Bescherming van mensenlevens in het kader van de strijd tegen terrorisme vraagt om onorthodoxe maatregelen. Juist om het privéleven te beschermen zijn soms ingrijpende inbreuken noodzakelijk. De waarborgen van de rechtsstaat zijn hierbij leidend.
- De beveiliging van overheidswebsites moet verbeteren, zodat onbevoegden geen inbreuk kunnen doen op de privacy van burgers.
- Persoonlijke gegevens van burgers worden in principe niet opgeslagen, tenzij hiervoor noodzaak is. Dat geldt in het bijzonder voor de bescherming van persoonsgegevens via DigiD. Burgers moeten zelf kunnen vaststellen welke gegevens bij de overheid zijn geregistreerd' (p.36).

De Partij voor de Dieren

De PvdD in het kort

De PvdD besteed uitgebreid aandacht aan privacy in haar verkiezingsprogramma. De onderregel van het hoofdstuk *Privacy, Veiligheid, Burgerrechten en integer bestuur* luidt dan ook: 'Een overheid die luistert naar de wensen van de burger (zonder die burger af te luisteren)' (p.30). De partij voor de Dieren draagt verschillende maatregelen aan om privacy te kunnen waarborgen en is groot voorstander van meer transparantie vanuit de overheid. Net als GroenLinks is ze voor het afschaffen van de identificatieplicht en voor het afschaffen van de bewaarplicht van telecomgegevens, maar er zijn ook twee nieuwe - niet eerder genoemde - voorstellen. Eén hiervan is dat systemen die privacy niet kunnen waarborgen moeten worden afgeschaft, waaronder landelijke elektronische dossiers voor patiënten, leerlingen en prostituees. Het andere voorstel is dat we moeten stoppen met het verplichten van vingerafdrukken in reisdocumenten en het opslaan hiervan in databases.
Naast deze nieuwe initiatieven, toont de PvdD zich ook consequent in andere zaken zoals slimme energiemeters, de kilometerheffing en handelsverdragen zoals CETA. Voor alle drie geldt dat deze nooit ten koste mogen gaan van het recht op privacy.

De samenstelling van relevante punten

'Privacy is veiligheid. De Partij voor de Dieren staat voor de vrije persoonlijke levenssfeer van burgers. Wanneer we onze privacy opgeven, geven we een belangrijk deel van onze veiligheid op. Privacy biedt ons veiligheid en beschermt ons tegen de staat. Inperking van de rechten van burgers mag alleen in uiterste gevallen. Bij het bieden van veiligheid is er een groot verschil tussen een grote broer die over je waakt en een Big Brother die je bespiedt. De Partij voor de Dieren staat voor een samenleving waarin burgers zich vrij kunnen voelen en waarin rechten op privacy en zelfontplooiing worden gerespecteerd. Een integere overheid betrekt haar burgers en biedt ze perspectief.
• Inzet van cameratoezicht mag alleen tijdelijk, in een door de rechter aangewezen risicogebied.
• Etnisch profileren wordt tegengegaan door onder meer een registratiesysteem waarin vermeld wordt waarom iemand staande is gehouden.
• Al het Nederlandse en Europese beleid op het gebied van aftappen, verzamelen en opslaan van gegevens van burgers wordt scherp herzien in het belang van de privacy. Het verzamelen en opslaan van gegevens van burgers en bedrijven door Amerikaanse en andere buitenlandse inlichtingendiensten is onacceptabel. Nederland treft maatregelen om deze privacyschendingen zo spoedig mogelijk te stoppen en nieuwe afluisterpraktijken te voorkomen.
• Zo komt er een einde aan de bewaarplicht voor telefoon- en internetgegevens en het doorgeven van passagiersgegevens aan de Verenigde Staten. De VS krijgen niet langer inzage in Europese banktransacties.
• We stoppen met de verplichte opname van vingerafdrukken in reisdocumenten en het opslaan daarvan in een database.

• Nederland krijgt een instantie die feitelijk en gedetailleerd rapporteert over specifieke incidenten op het gebied van inbreuken op de veiligheid van onze digitale infrastructuur.
• Cybersecurity bereik je niet met het schenden van grondrechten. Opsporingsinstanties mogen niet rondsnuffelen in computers zonder dat daar een zwaarwichtige, door de rechter getoetste reden voor is. Er komen strengere normen voor het aftappen van telefoons.
• Nederland gaat persoonsgegevens op het hoogste niveau beschermen. De overheid gaat structureel investeren in softwareprojecten om de digitale infrastructuur beter te beveiligen. De Autoriteit Persoonsgegevens (AP) krijgt de bevoegdheid en middelen die nodig zijn om zijn taak goed uit te voeren, vergelijkbaar met de bevoegdheden van de Autoriteit Consument en Markt.
• Alleen wanneer sprake is van een concrete verdenking die door de rechter wordt getoetst, mogen politie, justitie en inlichtingendiensten gegevens over burgers opvragen bij bedrijven. Burgers krijgen meer zicht op de gegevens die over hen zijn opgeslagen en betere mogelijkheden zich uit datasystemen te laten verwijderen. Bedrijven melden hoe vaak ze gegevens ten behoeve van justitie openbaar hebben moeten maken.
• Burgers hebben recht op een vrij internet zonder filters, blokkades of doorgifte van gegevens door providers.
• Onlinediensten zijn toegankelijk zonder dat je getrackt wordt. Ook is geen enkele vorm van het verzwakken van de mogelijkheden tot versleuteling van informatie acceptabel.
• Internetaanbieders worden niet gebruikt als verlengstuk van de opsporingsdiensten. De bewaarplicht van gegevens van burgers wordt afgeschaft. Het communicatiegeheim wordt beschermd en gerespecteerd.
• De overheid mag bedrijven niet meer zomaar vragen om ‘vrijwillig’ gegevens te verstrekken of handelingen te verrichten. Ze mag dat alleen doen als dat geregeld is in een wet en dan alleen met alle wettelijke waarborgen rondom privacy die daarbij horen. • Bedrijven worden verplicht om burgers in te lichten als hun gegevens zijn gelekt. Hackers die beveiligingslekken blootleggen krijgen bescherming.
• Nieuwe beleids- en wetsvoorstellen worden getoetst op de gevolgen voor de privacy. Wanneer deze de bescherming van de persoonlijke levenssfeer aantasten, worden ze aangepast of gaan van tafel.
• Systemen die de privacy niet kunnen waarborgen worden afgeschaft, zoals de landelijke elektronische dossiers voor patiënten, leerlingen en prostituees.
• De identificatieplicht wordt afgeschaft’ (p.30-31).

De Piratenpartij

De Piratenpartij in het kort

De Piratenpartij richt zich hoofdzakelijk op burgerrechten. Daarom is het niet opmerkelijk dat privacy ruimschoots aan bod komt in hun verkiezingsprogramma. De PiratenPartij draagt veel soortgelijke maatregelen aan van eerder genoemde partijen, maar de Piratenpartij gaat op sommige punten verder dan andere partijen. Zo wil ze dat anoniem reizen weer mogelijk wordt. In het OV betekent dit dat anoniem reizen niet méér zou moeten kosten dan de OV-chipkaart en op de weg houdt dit in: geen automatische nummerplaatherkenning (ANPR), geen RFID-chips in kentekens, geen kilometerheffing en de mogelijkheid voor anoniem parkeren. Daarnaast moet cameratoezicht beperkt worden, de mogelijkheid voor tagging aan banden worden gelegd, er asiel worden verleend aan Snowden (p.13) en een verbod komen voor korting bij een dienst/product in ruil voor gegevens.

Bij elke voorgesteld maatregel of verandering is de Piratenpartij zich bewust van de mogelijke gevolgen voor burgerrechten. Hierdoor blijft ze consequent in haar handelen rondom privacy. In combinatie met het indienen van allerlei nieuwe initiatieven, neemt ze absoluut een voortrekkersrol als het privacy betreft. Dit wordt versterkt doordat hun programma duidelijk gericht is op bewustwording van het privacy-belang en hierbij een correcte informatievoorziening verstrekt. Ze sluiten hun verkiezingsprogramma overigens geheel in stijl af met de zinnen: ‘Deze tekst is vrij te kopiëren. De Piratenpartij nodigt iedereen, maar in het bijzonder overige politieke partijen, uit om de standpunten van de Piratenpartij te kopiëren, over te nemen, of anderszins te verspreiden’ (p.26).

De samenstelling van relevante punten

‘Er wordt regelmatig om onze privégegevens gevraagd. Bijvoorbeeld bij een inschrijving, of een bestelling. Als onze gegevens gebruikt worden zonder onze toestemming of zonder ons medeweten verliezen we een stuk privacy en daarmee ook een stuk van onze vrijheid’ (p.9).

‘Koppeling en gebruik persoonsgegevens.
De laatste jaren is analyse- en datamining technologie enorm gegroeid. Databases worden groter en databases worden gekoppeld. Het analyseren en doorzoeken van al die big data is steeds makkelijker en sneller te doen. Het is veelal onduidelijk wie het analyseren en doorzoeken doet. Wat er geanalyseerd en doorzocht wordt is vaak onbekend. Voor burgers is informatie weliswaar makkelijker te vinden maar helaas ook veel moeilijker te verwijderen. Daarom is het belangrijk dat we privacybeschermende maatregelen uitbreiden en dat we de naleving daarvan strikt controleren en waarborgen. De opsporings-, inlichtingen- en veiligheidsdiensten hebben de beschikking over vele databases met persoonsgegevens. Een voorbeeld van een dergelijke database is CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) waar automatisch gegevens van gebruikers van alle providers worden opgeslagen. Keer op keer weer blijkt dat er geen adequate beveiliging is tegen ongeoorloofde zoekopdrachten. Enige controle op naleving van

wetgeving omtrent dit alles is minimaal. Wij willen de hoeveelheid zoekopdrachten uit dergelijke databases sterk aan banden leggen' (p.10)

'Slimme meters
Energiemeters meten gebruik per seconde maar geven deze geaggregeerde data zelfstandig per maand of kwartaal door aan de energiemaatschappij. Energiemaatschappijen en distributiebedrijven mogen niet op eigen initiatief zelf kastjes kunnen aansturen. Publicatie van de broncode van software in meetkastjes moet verplicht worden. **Het moet altijd mogelijk zijn om een slimme meter te weigeren'** (p.11).

'Overheid: open, inzichtelijk en efficiënt
Een open en transparante overheid is een basisvoorwaarde voor een goede democratie. Alleen wanneer burgers het functioneren van haar overheid ter discussie kunnen stellen en ze de overheid kunnen controleren is een goede volksvertegenwoordiging mogelijk. Partijbelangen staan broodnodige maatschappelijke beslissingen in de weg en lobbyisme maakt steeds meer de dienst uit. Om het vertrouwen in de politiek te herstellen is het belangrijk dat de overheid zich openstelt naar haar burgers. Het is belangrijk dat wat de overheid doet door burgers en journalisten kan worden opgevraagd en bekeken. Ook moet de communicatie tussen de overheid en lobbyisten transparanter worden. Alleen zo kunnen burgers geïnformeerde beslissingen nemen' (p.11).

'Privacy in het onderwijs
- Scholen moeten een privacybeleid en/of privacyreglement hebben.
- Scholen moeten transparant zijn over de opslag en het gebruik van de gegevens van leerlingen.
- Het maken van foto's of video's kan alleen met toestemming ouders en kind.
- De privacy van leerlingen moet altijd gewaarborgd blijven bij het uitwisselen van gegevens.
- Gegevens van leerlingen dienen adequaat beveiligd te zijn' (p.33).

'Anoniem reizen
- De OV-chipkaart dient opgewaardeerd te kunnen worden met contant geld.
- Anoniem reizen, bijvoorbeeld met een eenmalige OV-chipkaart mag nooit duurder zijn dan een met een normaal kaartje, of een persoonlijke OV-chipkaart.
- Het gebruik van automatische nummerplaatherkenning (ANPR) - waarmee voertuigen precies kunnen worden gevolgd - moet sterk aan banden worden gelegd. Persoonlijke gegevens mogen alleen worden opgeslagen bij een overtreding.
- Er worden bovendien geen RFID-chips in kentekens geplaatst, waarmee het volgen van voertuigen nog makkelijker zou worden. Problemen rondom gestolen kentekens kunnen ook worden opgelost zonder maatregelen die privacy schenden, zoals een kenteken wat slechts eenmalig geplaatst kan worden en breekt bij verwijdering (een Engels systeem). Je kunt ook wisselen naar een nieuw kentekennummer.

• Er komt geen verplichte zwarte doos in auto's. Als een auto toch een zwarte doos heeft dan mogen de gegevens alleen worden uitgelezen bij een ongeluk of misdrijf.
• Anoniem parkeren moet altijd mogelijk zijn zonder kentekenregistratie.
• Er komt geen kilometerheffing. Daar zijn systemen voor nodig die privacy schenden en daar zijn wij als partij principieel tegen.
• De fiets is het laatste vervoermiddel waarvan niet iedere beweging automatisch geregistreerd wordt. Daarom worden ook fietsen niet voorzien van kentekens, RFID-chips, en andere soortgelijke systemen om fietsers te volgen' (p.36).

'Privatisering informatie
De maatschappij betaalt mee aan wetenschappelijk onderzoek en scholing. Het is dus logisch dat de burger daar ook van mee kan profiteren. Het internet zorgt voor een snelle verspreiding van kennis en dit mag als een groot goed worden gezien. Vrijheid van informatie en de privacy van burgers gaan vóór op commerciële belangen. Commerciële partijen zullen weer innovatief moeten zijn en op andere verdienmodellen en de verandering van de maatschappij moeten inspelen. Op geen moment mag vrijheid van informatie onder druk staan, of inbreuk gemaakt worden op de privacy van burgers' (p.42).

De PVV

De PVV in het kort

Bij 50Plus dachten we het niet korter te kunnen maken. Toch wel. Met een verkiezingsprogramma dat 1 A4'tje beslaat, besteedt Wilders geen enkele aandacht aan het belang van privacy.

De samenstelling van relevante punten

Geen

Bronvermelding

Nederlandse Orde van Advocaten (2017). *Verkiezingsprogramma's op gespannen voet met de rechtsstaat.* Geraadpleegd van https://www.advocatenorde.nl/12310/consumenten/verkiezingsprogramma-s-op-gespannen-voet-met-de-rechtsstaat

Voor de overige verwijzingen met pagina nummers is gebruikt gemaakt van het verkiezingsprogramma zoals gepubliceerd door de desbetreffende partij op hun officiële website.