

DATA IN DEN HAAG

**Een analyse van de verkiezingsprogramma's
in 2021 op datagebied**

De Datavakbond

18 februari 2021





- 03** Voorwoord
- 04** De partijen in het kort
- 06** Grote dataplatformen
- 09** Data van de consument
- 12** Data van de burger
- 15** Data in de gezondheidszorg
- 18** Data in onderwijs, cultuur en wetenschap
- 21** Data in economie en milieu
- 24** Data bij politie en justitie
- 27** Data bij defensie
- 30** Data, democratie en recht
- 33** Verantwoording

VOORWOORD

Data in Den Haag is geen stemwijzer, het is een standpuntenvergelijking. Wij hebben niet van tevoren een aantal stellingen bepaald en toen de antwoorden gezocht, we willen juist een zo volledig mogelijk overzicht geven van alle datagerelateerde standpunten in de verkiezingsprogramma's van deelnemende partijen. Wat daaruit al snel opviel, is dat er grote verschillen zijn tussen partijen. Sommige partijen hebben slechts een handjevol standpunten op datagebied, terwijl anderen tientallen paragrafen volschrijven. Dit is ook goed te zien in de tabellen in dit document: elke lege cel vertegenwoordigt een maatschappelijk vraagstuk dat door een politieke partij niet wordt genoemd. We hopen natuurlijk dat bij volgende verkiezingen veel van deze lege plekken zullen zijn ingevuld!

Op een paar punten is er duidelijke overeenstemming, en we hopen dit dan ook terug te zien in het beleid na 17 maart: er is opvallende eensgezindheid over het eigenaarschap van persoonsgegevens: dit moet bij de betreffende persoon blijven, en niet zoals nu bij het verzamelende bedrijf. Ook willen bijna alle partijen strenger optreden tegen grote techplatforms en meer transparantie van algoritmes, bij de overheid en bij bedrijven. Ook is er veel steun om altijd offline met overheden te kunnen communiceren.

Bij het schrijven van deze vergelijkingen moesten we ook een paar lastige keuzes maken: welke partijen nemen we op, en welke standpunten? Qua partijen hebben we ons beperkt tot alle partijen die in februari in een peiling op tenminste één zetel staan, dit zijn er 16 (uit in totaal 37 deelnemende partijen). Qua standpunten

hebben we zo breed mogelijk gewerkt. Ruwweg alles dat te maken heeft met persoonsgegevens en digitale technologie is opgenomen, ook als het woord 'data' niet genoemd wordt, of het niet in een datagerelateerde paragraaf staat.

Wat ons ook opviel is hoe verschillend partijen aankijken tegen datakwesties. De een ziet het vooral als een vervelend obstakel in de vorm van onnodige cookiemeldingen, de ander juist als de oorzaak van schadelijke monopolies. Sommige partijen concentreren zich op data bij bedrijven, anderen hebben vooral ideeën voor datagebruik bij de overheid. Nieuwe digitale innovaties worden soms gezien als een economisch wondermiddel, en soms als een bedreiging voor fundamentele waarden. We hebben een korte samenvatting geschreven voor elke partij, maar de verschillen zijn pas echt goed te zien op de themapagina's, waar standpunten over dezelfde kwesties naast elkaar zijn gezet.

Dit project is ontstaan binnen de werkgroep Inhoud van de Datavakbond. Er zijn heel veel uren in dit project gestoken, van het eerste idee tot de uiteindelijke presentatie. Mijn grote dank aan Peter voor zijn professionele inzicht, Tijs voor zijn toewijding en Levien voor zijn diverse bijdragen. Bedankt aan Reinier voor zijn vele telefoontjes, opzetten van de website en veel meer, dank aan Wiljan voor de communicatie en ondersteuning, en aan Carla voor het mooie design. Alvast bedankt aan de gastsprekers bij de presentatie, en aan alle anderen die hielpen bij schrijven en delen van Data in Den Haag. Hopelijk is het niet de laatste keer dat we dit doen!

Rogier Hurman, secretaris van de Datavakbond



PARTIJEN IN HET KORT

VVD Op het gebied van data heeft de VVD een redelijk uitgewerkt programma. Er is veel aandacht voor het creëren van een gelijke datamarkt en mededinging bij grote dataplatformen. Ook besteedt de partij veel aandacht aan veiligheid bij het delen van data. De VVD wil wel graag data delen om lijsten met fraudeurs op te stellen. Tot slot ligt er een nadruk op het versterken van innovatie en bijvoorbeeld het gebruik van digitale technologie in de gezondheidszorg en onderwijs.

PVV Het verkiezingsprogramma van de PVV is beknopt, en bevat nauwelijks standpunten over gebruik van data. Alleen bij het hoofdstuk politie en justitie zijn datagerelateerde standpunten, en hier kiest de PVV voor handhaving ten koste van dataprivacy.

CDA Het CDA ondersteunt digitale innovaties via ondersteuning van ondernemers. Daarbij legt de partij de nadruk dat iedereen mee kan doen met het gebruik van digitale technologie. De partij wijst ook op de keerzijde van digitale ontwikkelingen: een slechtere positie voor werknemers, een verstoord debat en beveiligingsrisico's.

D66 D66 heeft haar datastandpunten het meest gedetailleerd uitgewerkt. Op de meeste beleidsterreinen wordt ook gekeken naar de digitale aspecten. Bijvoorbeeld door te kijken hoe de consument of burger tegen datamisbruik beschermd kan worden (maar is niet zo kritisch als andere partijen). D66 komt als enige met diverse ideeën in het onderwijs, de zorg en bij de overheid.

GROENLINKS GroenLinks wil streng optreden tegen grote techplatforms, en noemt in het verkiezingsprogramma, en noemt diverse maatregelen om hun datamacht te beteugelen. Ook pleit de partij voor open en toegankelijke data bij de overheid. Op andere thema's zijn hier en daar enkele datastandpunten, zoals tegen meekijksoftware in het onderwijs of voor privacyvriendelijk rekeningrijden.

SP De SP heeft relatief weinig in het verkiezingsprogramma staan als het om privacy en data gaat. De punten die het heeft zijn wel daadkrachtig. Commerciële dataplatforms moeten worden gereguleerd en belast, en persoonsgegevens goed beschermd. Over data bij de overheid wordt niets gezegd.

PvdA Het programma van de Partij voor de Arbeid heeft vooral datastandpunten op het gebied van Big Tech, ter bescherming van consumenten, maar ook ter bescherming van werknemers. Er zijn daarnaast standpunten over het beschermen van privacy door de overheid, maar op meerdere thema's komen geen datastandpunten voor.

CU De ChristenUnie beschrijft haar digitale standpunten zonder concrete oplossingen te formuleren. De nadruk ligt op meer wetgeving rond de bescherming van grondrechten en het borgen van het publieke belang.

PvdD De Partij voor de Dieren ruimt twee volle pagina's in voor haar digitale standpunten. Ze willen de data van burgers zowel tegen grote bedrijven als tegen overheden beschermen, en praten niet over mogelijke nieuwe toepassingen van data.

50 PLUS De datapolitieke standpunten van 50PLUS zijn beperkt typische behoeften van ouderen: onderwijzen van digitale vaardigheden, niet-digitale toegang tot de overheid behouden, en internetcriminaliteit bestrijden.

SGP De SGP heeft een uitgebreide verzameling datastandpunten en bespreek bepaalde thema's zeer gedetailleerd. Met name over defensie en infrastructuur schrijft de SGP veel meer dan andere partijen. Daarnaast hecht de partij aan de mogelijkheid om internettoegang zelf te kunnen filteren, en noemt de partij als enige 5G een risico.

DENK DENK heeft nauwelijks digitale standpunten, behalve op het gebied van discriminatie. Aan de ene kant wil de partij discriminerend gebruik van bijvoorbeeld algoritmes beperken, aan de andere kant wil de partij sociale media scannen op discriminerende inhoud.

FvD In het verkiezingsprogramma van het Forum voor Democratie wordt grote nadruk gelegd op de gevaren van Big Tech voor het publieke debat. De partij wil dat platformen zo min mogelijk uitingen censureren. Voor de rest wil de partij regulering op datagebied terugdringen, behalve voor digitale beveiliging.

BIJ1 Digitalisering, technologie en de relatie ervan met grondrechten zijn diepgravend uitgewerkt in het programma van BIJ1. De partij pleit voor een verbod op gezichtsherkenningsoftware. Ook ligt er een sterke nadruk op het waarborgen van diversiteit, onder andere door diversiteitscommissies en quota, wat juist weer verwerking van bepaalde data inhoudt. BIJ1 is kritisch op de veiligheidsdiensten, een voorstander van open source, en ziet toegang tot het internet als een basisrecht.

JA21 JA21 heeft op de meeste beleidsterreinen één, soms meerdere standpunten met datarelevantie. De partij zet zich af tegen dataverzameling door zowel bedrijven als overheid, behalve bij de bestrijding van extremisme.

Volt Volt heeft een beknopt programma, ook op datagebied. De partij praat niet over gevaren of onrecht, maar ziet vooral mogelijkheden voor de overheid om betere digitale dienstverlening te leveren, en voor de toepassing van nieuwe technologieën zoals kunstmatige intelligentie en e-health.



GROTE DATAPLATFORMEN

Op het internet zijn een handjevol datareuzen zeer machtig geworden met de data van hun gebruikers. Wat willen partijen doen aan deze machtspositie, zowel economisch als in beïnvloeding van het publieke debat?

GROTE DATAPLATFORMEN

		 PARTIJ VOOR DE VRIJHEID						
Hoe moeten mededingingsregels aangepast worden voor BigTech?	Ingrijpen en hoge boetes door EC. Openbreken bedrijven mogelijk. Interoperabiliteit verplichten. (p14-15)		Geharmoniseerde belasting, opsplitsing mogelijk. Klanten en werknemers beter beschermen. (p56)	Mededingingsrecht updaten voor marktmacht en netwerkeffecten. Collectief organiseren mogelijk maken. (p106)		Grote internationale techbedrijven opsplitsen. (p12)	Big Tech opbreken. (p15)	
Waar moeten grote techbedrijven belasting betalen?	Belasting op plek waar techbedrijven klanten hebben, mogelijk digitaal dienstenbelasting. (p14-15, 20)			Eerlijke belasting techbedrijven in landen waar ze ondernemen, op Europees niveau regelen. (p106)	Digitaks invoeren, op nationaal niveau totdat Europese variant wordt ingevoerd. (p54)	Belasting op digitale diensten. (p29)	Digitaks invoeren. (p16)	
Wat mogen techbedrijven tonen en weren aan hun gebruikers?			Fatsoensnormen introduceren in het digitale domein. (p57)	Onafhankelijke redactie en transparantie over algoritmes. Ongewenste buitenlandse invloed tegengaan. (p106)	Netneutraliteit en dataportabiliteit. Duidelijke richtlijnen voor en toezicht op inzet van filters. (p77)	Optreden tegen algoritmes die eenzijdige informatievoorziening creëren. (p12)		
Wat zeggen de partijen nog meer?				Techgiganten moeten journalistieke organisaties eerlijk betalen voor het gebruik van hun inhoud. (p124)				

GROTE DATAPLATFORMEN








	 Partij voor de Dieren							
Hoe moeten mededingingsregels aangepast worden voor BigTech?			Mededingingsregels aanpassen. Aandacht voor macht grote communicatieplatforms. (p140)	Gelijk speelveld voor taxibedrijven en Uber. (p73)	Ruime mogelijkheden voor alternatieve platformen. (p100)	Macht van techgiganten aan banden leggen op Nederlands en Europees niveau. (p117)		Mededingingsregels herzien in samenwerking met de EU. (p27)
Waar moeten grote techbedrijven belasting betalen?					Internetbedrijven moeten een eerlijker belastingtarief betalen. (p51)			
Wat mogen techbedrijven tonen en weren aan hun gebruikers?	Meer transparantie over wat gebruikers te zien krijgen. Geen microtargeting. (p92)		Zelf voor filtering kiezen moet mogelijk blijven. Terughoudend met tot nepnieuws bestempelen. (p91, 141, 165)	Racismedetector op sociale media voor discriminerende inhoud. (p16)	Openbaarheid van algoritmes, geen censuur en beroepsmogelijkheden op sociale media. (p102)	Wetgeving over smaad, laster en haat zaaien streng naleven, nepnieuws bestrijden. (p96)	Inhoud van sociale platformen laten beoordelen door rechter, niet door platformen zelf. (p45)	
Wat zeggen de partijen nog meer?								



DATA VAN DE CONSUMENT

Bedrijven verzamelen steeds meer gegevens van hun gebruikers. Waar moeten de grenzen worden gesteld? Wat wordt de machtsverhouding tussen gebruiker en verwerker?

DATA VAN DE CONSUMENT

								
Hoe worden werknemers beschermd tegen de risico's van digitale technologie?			Extra handhaving en regulering in de platformeconomie, betere arbeidsvoorwaarden. (p57)	Geen discriminatie met algoritmes bij werving en selectie. (p138)	Meer inspraak voor werknemers bij inzet van nieuwe technologie. (p57)		Digitale platforms zijn werkgevers, tenzij ze het tegendeel bewijzen. (p10)	
Hoe mogen bedrijven gegevens van gebruikers verzamelen en gebruiken?	Data van kinderen beter beschermen en kindermarketing tegengaan. (p15)			Geen massale surveillance op socialemediaplatforms om auteursrechten te beschermen. (p106)	Verbod op persoonlijke advertenties. (p77)		Digitale gepersonaliseerde advertenties verbieden. Data verzamelen op ander platform verbieden. (p78)	Opkomen voor de privacy van burgers. Kinderen beschermen tegen dataverzameling en online reclame. (p35)
Wat voor macht krijgt de gebruiker over zijn data?	Big Tech-bedrijven moeten betalen voor het gebruik van persoonlijke data. (p15)		In Europees verband vastleggen dat persoonsgegevens eigendom van de persoon blijven. (p56)		Verbod op handel in persoonsgegevens. (p77)	Bescherming van persoonlijke data analoog bescherming van betaalde diensten. (p12)	Verkoop van persoonsgegevens aanpakken. Recht om netwerk mee te nemen. (p78-79)	
Hoe mogen biometrische gegevens worden verzameld?				Gebruik van camera's met gezichtsherkenning verbieden. (p121)	Automatische verzameling van biometrische gegevens in de openbare ruimte verbieden. (p78)		Biometrische gegevens alleen lokaal opslaan. (p79)	
Hoe worden data veilig en transparant opgeslagen?	Verplichte opslag persoonlijke data Europeanen in Europa zelf. Investeren in Europees alternatief. (p15)			Europese regels voor de veiligheid van digitale apparaten, fysiek uitschakelen mogelijk. (p122)				
Wat willen de partijen nog meer?								

DATA VAN DE CONSUMENT



Hoe worden werknemers beschermd tegen de risico's van digitale technologie?	Meekijksoftware voor thuiswerkende werknemers verbieden. (p93)		Garantie bij platformen van minimale arbeidsvoorwaarden zoals de rusttijden. (p79)					
Hoe mogen bedrijven gegevens van gebruikers verzamelen en gebruiken?			Privacywetgeving voor kleine bedrijven herzien om administratieve rompslomp te verminderen. (p90)	Discriminerende algoritmes verbieden. (p16)	Cookiewet afschaffen. (p100)			
Wat voor macht krijgt de gebruiker over zijn data?	Alleen gegevens verzamelen met nadrukkelijke toestemming. Externe toegang tot rekeningen afschaffen. (p92-93)		Individueel eigenaarschap van data, bedrijven moeten transparant zijn over het gebruik van data. (p140)		Burgers de baas over eigen data in plaats van Big Tech-bedrijven. Nederlandse variant van AVG maken. (p100)		Handel in persoonsgegevens inperken. (p45)	
Hoe mogen biometrische gegevens worden verzameld?						Gezichtsherkenningsoftware en soortgelijke software verbieden. (p117)		
Hoe worden data veilig en transparant opgeslagen?	IoT beter beveiligen. Transparantie bij opslag en gebruik data. Dat zoveel mogelijk in NL opslaan. (p92-93)		EU-coördinatie voor bescherming van privacy en veiligheid. (p165)		Verplichting tot privacy en security by design. (p100)	End-to-endversleuteling waarborgen. (p117)	Overheid en bedrijven verantwoordelijk stellen voor datalekken. (p45)	
Wat willen de partijen nog meer?					Mensen krijgen de mogelijkheid geen statisch IP-adres te nemen. (p100)		Contante betalingen in stand houden. (p45)	



DATA VAN DE BURGER

De overheid is traditoneel een datagigant, en nu ook grotendeels digitaal. Deze concentratie van data geeft nieuwe mogelijkheden, maar ook nieuwe risico's. Hoe kijken partijen hier tegenaan?

DATA VAN DE BURGER

								
Hoe blijft de overheid toegankelijk voor wie digitaal niet meekan?	Contact met de overheid per post blijft mogelijk, eventueel aangetekend. (p93)			Fysieke servicepunten of thuis hulp voor wie moeite heeft met digitaal contact. (p120)	Recht op betekenisvol menselijk contact vanuit de overheid. Communicatie voor iedereen toegankelijk. (p70)			
Moeten overheden vrije software gebruiken?				Overheidsdiensten gebruiken open standaarden en opensourcesoftware. (p119)	Overheden bevorderen en gebruiken open standaarden, vrije en opensourcesoftware en open hardware. (p77)			
Hoe wordt overheidsdata openbaar gemaakt?				Data worden waar mogelijk open, inzichtelijk en gedeeld. (p121)	Openheid van data wordt de norm, publieke data zijn openbaar toegankelijk. (p77)			
Welke gegevens van burgers moeten worden bijgehouden (en gedeeld)?	Zwarte lijsten van fraudeurs opstellen en gegevens tussen overheden en private partijen delen. (p65)			Databases met persoonsgegevens evalueren en begrenzen. Controle op dataverzameling in het openbaar. (p119-120)				
Hoe gebruikt de overheid algoritmes?				Algoritmewaakbond bij de Autoriteit Persoonsgegevens. (p121)	Algoritmen regelmatig toetsen op de beginselen van behoorlijk bestuur. (p78)			
Wat doen we tegen de wildgroei aan overheidsidentiteiten?	Eén online identiteit voor iedere Nederlander om zich online te kunnen identificeren. (p93)						Betrouwbaar systeem voor digitale basisidentiteit. (p79)	
Hoe beheren we ICT-systemen bij de overheid?				Voldoende interne technologiekennis bij de overheid. ICT-contracten opknippen in kleine stukken. (p120)				Algoritmekeurmerk voor algoritmes die privacy en digitale veiligheid respecteren. (p35)

DATA VAN DE BURGER



Hoe blijft de overheid toegankelijk voor wie digitaal niet meekan?	Fysieke balie voor wie moeite heeft met digitaal contact. Communicatie per post blijft mogelijk. (p92)	De overheid ook per telefoon en schriftelijk te benaderen. (p12)				Toegankelijkheidseisen meenemen. Alternatieve kanalen voor wie moeite heeft met digitaal contact. (p116)		
Moeten overheden vrije software gebruiken?	Overheden gebruiken waar mogelijk open standaarden, opensourcesoftware en open hardware. (p92)				Dataverzameling vanuit de overheid beperken. Datadossier opvragen door burger mogelijk. (p100)			Overheden gebruiken intern en voor contact met burgers open software. (p46)
Hoe wordt overheidsdata openbaar gemaakt?								
Welke gegevens van burgers moeten worden bijgehouden (en gedeeld)?						Registratie van etniciteit en sekswerkers beperken, genderregistratie afschaffen. Diversiteit meten. (p14, 22, 60, 61)	Niet op elk moment burgers volgen, sturen en controleren. (p9)	
Hoe gebruikt de overheid algoritmes?				Verbod op discriminerende algoritmes. (p15-16)		Actief beleid tegen discriminatie en etnisch profileren in digitalisering, vanaf het ontwerp. (p117)		
Wat doen we tegen de wildgroei aan overheidsidentiteiten?			Eén uitvoeringsorganisatie met alle informatie over asielzoekers. (p69)					Eén digitale Europese identiteit voor iedere Nederlander. Digitaal portaal voor ondernemers. (p23-24, 48)
Hoe beheren we ICT-systemen bij de overheid?					Verplichting tot privacy en security by design. (p100)	Digitaliseringsbeleid waarin de rechten en behoeften van de burger centraal staan. (p117)		



DATA IN GEZONDHEIDSZORG

De zorg is een dataintensief vakgebied, met zeer gevoelige gegevens, en een groot belang om data snel én veilig op de juiste plek te krijgen. De laatste jaren zien we nieuwe digitale initiatieven in de zorg, zoals het Elektronisch Patiëntendossier en de inzet van kunstmatige intelligentie.

DATA IN GEZONDHEIDSZORG

								
Hoe moet zeggenschap over gezondheidsgegevens/patientgegevens worden geborgd?	Uitwisseling van medische gegevens verplicht in elektronische vorm. (p37)		Duidelijke richtlijnen en de patiënt altijd de baas over het eigen medische dossier. (p28)	Veilige uitwisseling, meldplicht bij datalekken, de patiënt houdt de regie over de eigen gegevens. (p169-170)				
Waar kunnen medische gegevens behalve voor de behandeling voor worden gebruikt?	Geanonimiseerde data delen met verzekeraars en onderzoekers, persoonlijke data bij toestemming. (p36)			Biobanken met DNA, lichaamsmateriaal en medische gegevens gebruiken binnen een wettelijke regeling. (p114, 170)				
Wat is de rol voor digitale hulpmiddelen in de zorg?	Breed stimuleren van digitale zorg en ondersteunen van zorgmedewerkers, voor betere betaalbaarheid. (p38, 40)		Inzetten op innovatie: videoconsults met je arts en het gebruik van data en nieuwe technologie. (p26)	Apps, digitale consulten en robotica, keuzes coördineren. Patiëntbelang toetsen bij AI. (p153, 162, 168)				AI toepassen zolang het niet tussen arts en patiënt komt, commercieel gebruik van data uitgesloten. (p47)
Wat zeggen de partijen nog meer?		Administratie automatiseren, standaardiseren of afschaffen. (p17)		Complexere gezondheidszorg vraagt om nieuwe opleidingen op het snijvlak van zorg en IT. (p153)				

DATA IN GEZONDHEIDSZORG










Hoe moet zeggenschap over gezondheidsgegevens/patientgegevens worden geborgd?	Alleen privacyveilige systemen gebruiken. Medisch dossier niet delen zonder expliciete toestemming. (p93)							
Waar kunnen medische gegevens behalve voor de behandeling voor worden gebruikt?					Zorgresultaten en patiënttevredenheid meten en openbaar maken. (p83)			
Wat is de rol voor digitale hulpmiddelen in de zorg?				Inzetten op innovatie door e-health en domotica te stimuleren. (p25)				Digitale hulpmiddelen, zoals diagnosesystemen en videocontact, in de zorg stimuleren. (p37)
Wat zeggen de partijen nog meer?								



DATA IN ONDERWIJS, CULTUUR EN WETENSCHAP

In onderwijs, cultuur en wetenschap valt veel te winnen door data goed te delen en bijvoorbeeld digitale leermiddelen in te zetten. Maar hoe wordt de privacy van leerlingen en studenten beschermd? En hoe worden burgers bewust van hun digitale rechten en mogelijkheden?

DATA IN ONDERWIJS, CULTUUR EN WETENSCHAP

								
Hoe ontwikkelen we digitale vaardigheden en datageletterdheid?	Digitaal vaardigheden opnemen in het onderwijsprogramma. (p30)		Prominente plaats voor digitaal burgerschap. (p55)	Aandacht voor KI, privacy, ethiek. Extra financiering voor leerlingen uit kansarme gezinnen. (p17)	Leraren zich digitaal laten ontwikkelen op het gebied van digitalisering en onderwijs op afstand. (p43)		Meekijksoftware voor thuiswerkende werknemers verbieden. (p93)	
Hoe waarborgen we de privacy van leerlingen en studenten?				Onderwijsinstellingen moeten privacy verankeren, bijv. door open source. (p25)				
Welke digitale middelen kunnen worden gebruikt in het onderwijs?	Extra uitleg via instructiefilmpjes voor zieke en hoogbegaafde leerlingen. Online hoorcolleges. (p30)			Digitaal en campusonderwijs combineren. Nationale standaarden ontwikkelen en betere ondersteuning. (p25)	Alleen veilige en privacyvriendelijke elektronische onderwijssystemen gebruiken. (p43)		Standaard open source bij inkoop van soft- en hardware in het onderwijs. (p79)	
Hoe delen we data en resultaten in de wetenschap?				Vrije toegang tot publiek gefinancierd onderzoek (Coalition S). Recht om data openbaar te maken. (p31)				
Wat moet er gebeuren met auteursrecht?	Thuiskopieheffing afschaffen. (p32)			Auteursrecht online hervormen, eerlijk deel van de opbrengsten naar de makers. (p39)	Auteursrecht moderniseren en inkorten. (p73)		Streamingheffing voor grote digitale platforms om makers fatsoenlijk te betalen. (p84)	
Hoe gaan we om met digitale cultuur?				Eén online platform voor alle Nederlandse erfgoedlocaties. Kwalitatief hoogstaand bibliotheekaanbod. (p39)	Iederen in Nederland toegang tot een volwaardige bibliotheek. (p73)		Stimuleringsfonds bibliotheken uitbreiden. (p82)	

DATA IN ONDERWIJS, CULTUUR EN WETENSCHAP










		Gratis tablet voor arme ouders. Digitaliseringslessen door lokale instanties. (p12)				Onderwijsprogramma's ontwikkelen voor bewustzijn van digitale rechten en privacyrechten. (p116)		Medialessen over nepnieuws en veilige omgang met sociale media en persoonsgegevens. (p32)
Hoe ontwikkelen we digitale vaardigheden en datageletterdheid?								
Hoe waarborgen we de privacy van leerlingen en studenten?	Studenten mogen meekijksoftware weigeren. Hulp voor organiseren veilige tentamens. (p92)							
Welke digitale middelen kunnen worden gebruikt in het onderwijs?					Onderzoek naar negatieve gevolgen digitalisering op leerprestaties. (p83)			
Hoe delen we data en resultaten in de wetenschap?						Investeren in open acces, digitale infrastructuur opzetten en internationaal lobbyen. (p47)		
Wat moet er gebeuren met auteursrecht?	Auteursrecht moderniseren, passende vergoeding voor makers. (p92)	Meer online mogelijkheden voor gezamenlijke activiteiten. (p16)						
Hoe gaan we om met digitale cultuur?								



DATA IN ECONOMIE EN MILIEU

Door op slimme technologieën in te zetten kunnen we de economie stimuleren en ook het milieu beschermen. Welke technologieën gebruiken we, en hoe? Hoe gaan we om met de negatieve effecten op de samenleving en milieu?

DATA IN ECONOMIE EN MILIEU

								
Hoe bevorderen we digitale innovaties?	Startups toegang geven tot data van publieke kennisinstellingen. Investeren in AI. (p12-13)							
Hoe kunnen we door data onze infrastructuur beter benutten?					Rekeningrijden invoeren op een privacyvriendelijke manier. (p23)			Privacyvriendelijke kilometerheffing. Betere doorstroming door slimme autotechnologie. (p116)
Hoe voorkomen we de negatieve effecten van data-gebruik?								
Wat zeggen de partijen nog meer?								

DATA IN ECONOMIE EN MILIEU



<p>Hoe bevorderen we digitale innovaties?</p>	<p>Open source stimuleren en gebruiken om kennis te delen. Terughoudend met dataexperimenten. (p92)</p>		<p>Potentie van AI binnen ethische kaders benutten. Investeren in digitale technologie en weerbaarheid. (p140, 151)</p>			<p>Ontwikkeling van open source en open standaarden in de publieke en private sector faciliteren. (p116)</p>	<p>Investeren in de digitale infrastructuur om de ICT-economie en het transport van data te stimuleren. (p61)</p>	<p>Met de EU investeren in AI en ethische richtlijnen bepalen. (p24)</p>
<p>Hoe kunnen we door data onze infrastructuur beter benutten?</p>			<p>Intelligente infrastructuur in verkeer. Data delen in logistieke sector. Digitalisering in de bouw. (p107, 111, 129)</p>					<p>Digitalisering voor een circulaire economie. (p23)</p>
<p>Hoe voorkomen we de negatieve effecten van data-gebruik?</p>			<p>Besparen op energiegebruik van datacentra. OV toegankelijk houden zonder digitale vaardigheden. (p. 103,</p>					
<p>Wat zeggen de partijen nog meer?</p>								



DATA BIJ POLITIE EN JUSTITIE

Politie, justitie en inlichtingendiensten verwerken veel data van burgers. Hoe wegen de partijen de belangen van verdachten of geobserveerden met de openbare veiligheid? En welke nieuwe digitale middelen kunnen worden ingezet?

DATA BIJ POLITIE EN JUSTITIE

								
Welke digitale middelen kan de politie inzetten?	Extra cameratoezicht probleemwijken. Beelden politieagenten en hulpverleners openbaren strafbaar. (p63)							
Hoe pakken we cybercriminaliteit aan?	Vergroten aantal cyberexperts. Beschermen tegen webwinkelfraude. Spoedprocedure internetterreur. (p63, 65)	Cybercrime-offensief. (p21)		Predictive policing alleen zonder discriminatie. Toepassing sensortechnologie melden bij minister. (p121)		Meer mensen en middelen voor de aanpak van digitale criminaliteit. (p21)		
Welke data mogen inlichtingendiensten verzamelen?				Supersnelrecht om online inhoud te kunnen verwijderen bij cybercriminaliteit. (p121)				
Hoe kan data van verdachten worden gebruikt en gedeeld?	Vrij delen relevante info door justitie en overheden. Financiële instellingen kunnen gegevens delen. (p61-62)	Digitale schandpaal voor daders van gewelds- en zedenmisdrijven. (p21)						
Wat willen de partijen nog meer?								

DATA BIJ POLITIE EN JUSTITIE



Welke digitale middelen kan de politie inzetten?	Cameratoezicht alleen tijdelijk. Geen camera's met gezichtsherkenning in de openbare ruimte. (p93)		Filmen van politie en hulpverleners tegengaan. (p90)	Racistenlokkers bij de politie om op internet racisten uit te lokken en te vervolgen. (p16)	Cameratoezicht uitbreiden om criminaliteit en overlast te bestrijden. (p29)	Cameratoezicht in openbare ruimte niet uitbreiden. Bodycams worden de norm. (p117)	Flexibel cameratoezicht en controlemiddelen inzetten. (p15)	
Hoe pakken we cybercriminaliteit aan?		Meer middelen tegen internetcriminaliteit, en hogere straffen. (p16)	Burgers beschermen tegen digitale afpersing. Laagdrempelige voorziening tegen internetcriminaliteit. (p91, 135)				Extra capaciteit en bevoegdheden om digitale criminaliteit doelmatig te bestrijden. (p15)	
Welke data mogen inlichtingendiensten verzamelen?	Beleid voor surveilleren van burgers herzien. Communicatiegeheim beschermen. Geen Sleepwet of WGS. (p93)		Nationale veiligheid gaat voor privacy van burgers, toegang tot de rechter waarborgen. (p91)		Intrekken van de Sleepwet. (p100)	Betere controle veiligheidsdiensten. Ongeëvalueerde data niet delen. Delen met buitenland inperken. (p. 97, 117)		
Hoe kan data van verdachten worden gebruikt en gedeeld?	Toetsing door rechter bij opvragen gegevens bij bedrijven. Sterker recht om vergeten te worden. (p93)		Inbreuken op de privacy alleen gerechtvaardigd bij noodsituaties. (p89)			Meer data over politiecontacten, o.a. etniciteit. Niet afkomst gebruiken in risicoprofielen. (p104)	Samenwerken tussen instanties, niet gehinderd door bureaucratie, tegen radicalisering en extremisme. (p15)	Informatie voor bestrijding van criminaliteit, terrorisme en cyberdreigingen beter delen in Europol. (p18)
Wat willen de partijen nog meer?						Geweldsincidenten gebaseerd op gender-identiteit en seksualiteit centraal registreren. (p105)		



DATA BIJ DEFENSIE

Defensie is een digitaal vraagstuk geworden. Hoe beveiligen we vitale digitale infrastructuur, wat is de rol van Defensie hierin, en welke middelen kunnen we inzetten?

DATA BIJ DEFENSIE

								
Hoe gebruiken we kunstmatige intelligentie in wapensystemen?	Inzetten, waarbij de mens betekenisvolle controle over de inzet houdt. (p45)					Streven naar een internationaal verbod op autonome wapensystemen. (p97)		
Hoe beveiligen we onze IT-sector tegen cyberdreigingen?	Import en export bij vitale sectoren en sleuteltechnologie screenen en mogelijk verbieden. (p16)		Beter voorbereiden op een massieve verstoring van het digitale domein. (p57)	Informatie NCSC delen. Ethisch hacken professionaliseren. Regels voor de veiligheid van apparaten. (p121-122)	Geen kwetsbaarheden in stand houden, bedrijven met slechte beveiliging verantwoordelijk houden. (p93)			Investeren in het Cyber Defensie Commando en in nauwe samenwerking met de private sector. (p141)
Hoe beveiligen we vitale infrastructuur?	Samenwerking tussen de overheid en het bedrijfsleven versterken en beveiligingsstandaarden verhogen. (p65)			Jaarlijks cyberafhankelijkheidsbeeld voor de samenleving. Investeren in digitale veiligheid. (p121)	Vitale infrastructuur beschermen tegen cyberaanvallen. (p93)			Investeren in cyberveiligheid om vitale infrastructuur te beschermen. (p140)
Hoe bereiden we ons voor op digitale oorlogsvoering?	NCSC, DCSC en inlichtingendiensten versterken. (p65)		Meerjarig cybersecurityprogramma onder leiding van een aparte Nationale Cybersecurity Coördinator. (p57)	Opslag en verwerking van data van Europese burgers in de VS op termijn stoppen. (p106)				Inzetten op schaarse en hoogtechnologische capaciteiten. (p140)
Wat is de rol voor de inlichtingendiensten?	Investeren in het Cybercommando van Defensie en de inlichtingendiensten. (p45)							

DATA BIJ DEFENSIE

	 Partij voor de Dieren	 50 PLUS	 SGP	 DENK		 BIJ1	 JA ²¹	 Volt
Hoe gebruiken we kunstmatige intelligentie in wapensystemen?			Zelf investeren in kunstmatige intelligentie. Internationale kaders voor menselijke rol in wapens. (p140, 156)					
Hoe beveiligen we onze IT-sector tegen cyberdreigingen?	Kritisch zijn op buitenlandse invloed op technologie en het internet. (p93)		Veiligheidsdiensten tegen economische spionage. Meer digitale soevereiniteit. Ondernemers steunen. (p138, 140, 150, 165)					
Hoe beveiligen we vitale infrastructuur?	Structureel investeren in softwareprojecten om digitale infrastructuur beter te beveiligen. (p93)		Investeren in goede beveiliging en betere ICT-systemen. Hogere veiligheidsstandaarden en afspraken. (p106, 140, 153, 165)		Geen gebruik maken van Huawei en andere riskante Chinese apparatuur. (p100)			
Hoe bereiden we ons voor op digitale oorlogsvoering?			Vorbereiden op een hyperwar met slimme sensoren en geautomatiseerde besluiten over wapeninzet. (p151, 153)		Investeringen in defensie via innovatieve startups laten terugvloeien in de Nederlandse economie. (p43)	Verbod op export van goederen waarmee mensenrechten geschonden worden. (p87)	Innovatie stimuleren om gericht informatiegestuurd op te treden. (p73)	
Wat is de rol voor de inlichtingendiensten?	Robuuste taskforce tegen spionage. Gegevens van burgers terughoudend delen met buitenland. (p93)							



DATA, DEMOCRATIE EN RECHT

Wie data heeft, heeft macht. Databeleid is geen los thema, maar neemt een steeds centralere rol in in de regering. Hoe sturen we het aan, en hoe gebruiken we data in onze democratie?

DATA, DEMOCRATIE EN RECHT

								
Onder welk ministerie valt databeleid?				Eén minister voor digitaal beleid. Transparantie verplichten bij IT-systemen van de overheid. (p119-120)				
Wat worden de rollen en middelen voor toezichhouders?	Toezichhouder voor algoritmes in publieke en private sector. (p93)			Hoger budget Autoriteit Persoonsgegevens en sterke, onafhankelijke Europese toezichthouder. (p106, 121)	Nationaal coördinator dataverzameling en meer capaciteit bij Autoriteit Persoonsgegevens. (p77)		Voldoende financiering voor AP, afdeling privacy en machtsmisbruik, en serieuze boetes. (p79)	AP omvormen tot Waakhond Digitale Veiligheid met voldoende technische kennis en middelen. (p35)
Hoe beschermen we mensenrechten op digitaal gebied?	Beïnvloeding van buitenaf en transacties vanuit onvrije landen signaleren en tegengaan. (p58)		Digitale grondrechten toevoegen aan de Grondwet. Ook internationale verdragen aanpassen. (p56)					
Wat is het databeleid rondom verkiezingen?				Verkiezingsapparaat aanmerken als vitale infrastructuur. (p122)		Commissie om te adviseren over maatschappelijke gevolgen en digitale burgerrechten. (p12)	Privacy meewegen bij aanbestedingen en subsidies. (p97)	
Wat willen de partijen nog meer?			Ethische en juridische normen voor gebruik IT en data door bedrijven en overheden. (p56)	AI in rechtspraak reguleren. Rechterlijke uitspraken altijd door mens. (p113)				Betere wetgeving rond digitale technieken en grondrechten. Internationale normen voor cyberdomein. (p35)

DATA, DEMOCRATIE EN RECHT

	 Partij voor de Dieren	 50 PLUS	 SGP	 DENK		 BIJ1	 JA ²¹	
Onder welk ministerie valt databeleid?			Eén bestaand ministerie om digitalisering te coördineren. (p140)			Ministerie van Gelijkwaardigheid om toe te zien op etnisch profileren. (p103)		Ministerie van Digitale Zaken voor dienstverlening, waarborgen privacy, betere digitale veiligheid. (p48)
Wat worden de rollen en middelen voor toezichhouders?	Autoriteit Persoonsgegevens uitbreiden voor naleving van de AVG. (p93)				Strengere sancties van de Meldplicht Datalekken onder de WBP. (p100)			
Hoe beschermen we mensenrechten op digitaal gebied?	Recht op een vrij internet zonder filters, blokkades of doorgifte van gegevens door providers. (p93)					Mensenrechtentoets voor export van surveillancesoftware. (p117)		
Wat is het databeleid rondom verkiezingen?			Duidelijke regels over digitale campagnes van politieke partijen. (p89)					
Wat willen de partijen nog meer?			Proactief opstellen en waken over de digitale veiligheid en de digitale soevereiniteit. (p140)			Internet definiëren als een nutsvoorziening, toegang tot het internet als een basisrecht. (p116, 117)		Zorgen dat digitale ontwikkelingen de kwaliteit van de samenleving ten goede komen. (p46)

VERANTWOORDING

Alle standpunten in dit document zijn (ingekort) overgenomen uit de verkiezingsprogramma's op de websites van de politieke partijen. Je kunt ze hier vinden:

- VVD** <https://www.vvd.nl/content/uploads/2020/11/Verkiezingsprogramma-concept-VVD-2021-2025.pdf> (definitieve versie was op 1 februari niet beschikbaar)
- PVV** <https://www.pvv.nl/images/09012020/verkiezingen2020/0acxyuew34z/VerkiezingsProgramma2021-Final.pdf>
- CDA** <https://d14uo0i7wmc99w.cloudfront.net/CDA/2020/TK2021/CDA-verkiezingsprogramma%5B2021-2025%5D.pdf>
- D66** https://d66.nl/wp-content/uploads/2021/01/d66_verkiezingsprogramma_een_nieuw_begin_2021_2025.pdf
- GL** <https://groenlinks.nl/sites/groenlinks/files/2021-02/verkiezingsprogramma%20spread.pdf>
- SP** https://www.sp.nl/sites/default/files/verkiezingsprogramma_2021-2025.pdf
- PvdA** <https://www.pvda.nl/wp-content/uploads/2020/11/PvdA-2021-2025-Ons-plan-voor-een-eerlijker-en-fatsoenlijker-Nederland-Printversie.pdf>
- CU** <https://insite.christenunie.nl/l/library/download/urn:uuid:284b3663-4f84-452b-8cf6-bb5c8fd53c92/concept+-verkiezingsprogramma+2021-2025.pdf>
- PvdD** <https://www.partijvoordedieren.nl/uploads/algemeen/Verkiezingsprogramma-Partij-voor-de-Dieren-Tweede-Kamerverkiezingen-2021.pdf>
- 50PLUS** https://50pluspartij.nl/images/2021/Jan_Feb/Publieksversie_programma_50PLUS_versie_13012021.pdf
- SGP** https://sgp.nl/download?docID=daae29e27ec63ff7fc9a4a20d0980ea150c73b39&name=Verkiezingsprogramma%20SGP%202021-2025%20_def_.pdf
- DENK** <https://www.bewegingdenk.nl/download/2831>
- FvD** https://d3n8a8pro7vhmx.cloudfront.net/fvd/pages/42/attachments/original/1611310614/Verkiezingsprogramma_FVD_2021.pdf?1611310614
- BIJ1** <https://cloud.bij1.org/s/DZo6n3reLLQq3jC/download>
- JA21** <https://ja21.nl/partijprogramma.pdf>
- Volt** <https://voltnederland.org/s/Volt-Verkiezings-programma-20212025.pdf>

BIJDRAGERS

Dit project kwam tot stand dankzij het harde werk van de volgende personen:

Rogier Hurman

Tijs Sikma

Peter Vieveen

Levien Nordeman

Reinier Tromp

Wiljan Linders

Laury Buijs

Carla ten Kate (grafisch ontwerp)

Dit onderzoek is tot stand gekomen met behulp van een financiële bijdrage van de Wiardi Beckman Stichting.