



Universiteit
Leiden
The Netherlands

Gedeelde Gegevens, Gedeeld Vertrouwen? Een studie naar studenten en digitale overheidsdiensten

Weersch, Orin van

Citation

Weersch, O. van. (2025). *Gedeelde Gegevens, Gedeeld Vertrouwen?: Een studie naar studenten en digitale overheidsdiensten*.

Version: Not Applicable (or Unknown)

License: [License to inclusion and publication of a Bachelor or Master Thesis, 2023](#)

Downloaded from: <https://hdl.handle.net/1887/4261395>

Note: To cite this publication please use the final published version (if applicable).

Gedeelde Gegevens, Gedeeld Vertrouwen? Een studie naar studenten en digitale overheidsdiensten

Orin van Weersch

s2771020

Universiteit Leiden

MSc Politiek, Beleid en Management

Begeleider: prof.dr.ir. Anne Fleur van Veenstra

Aantal woorden: 9998

Inhoudsopgave

Voorwoord	3
1. Inleiding	4
1.1. Wetenschappelijke relevantie	5
1.2. Maatschappelijke relevantie	5
2. Theoretisch Kader	7
2.1. Literatuur	7
2.1.1. Rationele afweging	8
2.1.2. Institutioneel vertrouwen	10
2.2. Samenvatting modellen	13
2.3. Verantwoording van theoriekeuze	14
2.4. Studenten en digitale overheidsdiensten	15
2.5. Conceptueel model en verwachtingen	16
3. Methodologie	18
3.1. Casusselectie	18
3.2. Methode van dataverzameling	19
3.3. Operationalisatie	19
3.4. Validiteit en betrouwbaarheid	20
4. Bevindingen	22
4.1. Digitale vaardigheden	22
4.2. Privacybewustzijn en attitude	23
4.3. Institutionele afhankelijkheid	25
4.4. Institutioneel vertrouwen	26
4.5. Privacy calculus	27
5. Analyse	29
6. Conclusie en discussie	34
6.1. Beantwoording van de onderzoeksvraag	34
6.2. Discussie	35
6.3. Aanbevelingen voor toekomstig onderzoek en beleid	36
7. Literatuurlijst	38
8. Appendix	45

Voorwoord

Het schrijven van deze scriptie was een intensief, soms stressvol, maar uiteindelijk ook verrijkend proces. Ik ben trots op het eindresultaat en kijk met plezier terug op het afnemen van de interviews – ook al duurde het soms dagen voordat iemand bereid was mee te werken. Eén van de meest memorabele ervaringen was dat ik werd weggestuurd van een mbo-school in Den Haag toen ik daar studenten probeerde te interviewen!

Wat ik persoonlijk als het lastigste onderdeel van dit proces heb ervaren, is het academisch schrijven in het Nederlands. Na jarenlang in het buitenland te hebben gewoond – onder andere op Aruba, waar ik voornamelijk Engels sprak – en een Engelstalige bacheloropleiding te hebben gevolgd, heb ik mijzelf bewust uitgedaagd om mijn master in het Nederlands te doen, als voorbereiding op mijn carrière in Nederland. Ik hoop dat mijn worstelingen met de Nederlandse taal niet al te zichtbaar zijn in deze scriptie.

In periodes van hoge druk was ik bijzonder afhankelijk van de emotionele steun van mijn vriendin Jade en mijn ouders. Hun geduld, liefde en aanmoediging hebben voor mij een wereld van verschil gemaakt – daarvoor ben ik hen oprecht dankbaar. Ook had ik deze scriptie niet kunnen afronden zonder de inhoudelijke begeleiding van mijn scriptiebegeleider Anne Fleur en de waardevolle feedback en steun van mede-student Lisa. Ook hen wil ik hartelijk danken.

Met veel genoegen presenteer ik hierbij het resultaat van mijn onderzoek. Ik wens de lezer dan ook veel leesplezier.

1. Inleiding

In een tijdperk waarin de digitalisering van overheidsdiensten zich vordert in een steeds sneller tempo, staat de bescherming van persoonsgegevens meer dan ooit onder druk. In de afgelopen decennia heeft digitalisering een prominente plaats ingenomen binnen de Nederlandse overheid. De hoeveelheid publieke diensten die online beschikbaar zijn wordt elk jaar groter, en daarmee ook de efficiëntie en toegankelijkheid voor burgers. In 2023 werden 96% van alle Nederlandse overheidsdiensten digitaal aangeboden, ver boven het Europees gemiddelde van 84% (Consultancy, 2023).

Deze overgang naar digitale dienstverlening brengt echter ook uitdagingen met zich mee. Recente incidenten – zoals de Toeslagenaffaire – hebben het vertrouwen in de digitale dienstverlening aangetast (Kanne & Driessen, 2021). Afgelopen maanden is er ook steeds meer kritiek op de opslag van data bij Amerikaanse cloud providers, wat vragen oproept over privacy en gegevensbescherming (BNNVARA, 2025).

Een specifiek voorbeeld dat de complexiteit van digitalisering en gegevensverwerking door de overheid illustreert is de recente kwestie rondom de Dienst Uitvoering Onderwijs (DUO). DUO gebruikte een algoritme om te controleren of studenten misbruik maakten van de uitwonendenbeurs (Tweede Kamer, 2024). Dit algoritme bleek discriminerend en onrechtmatig te zijn, doordat het bepaalde studenten – zoals jongeren met een migratieachtergrond – onevenredig vaak selecteerde voor controles en huisbezoeken (Autoriteit Persoonsgegevens, 2024). Deze werkwijze heeft geleid tot aanzienlijke financiële en emotionele schade bij de betrokken studenten en heeft het vertrouwen in de digitale processen van de overheid verder ondermijnd.

Deze incidenten benadrukken de noodzaak voor een kritische evaluatie van de digitalisering binnen de overheid, met speciale aandacht voor ethische implicaties en privacybescherming. Het is essentieel om te onderzoeken hoe burgers – en in het bijzonder studenten – omgaan met het delen van persoonlijke gegevens binnen deze steeds grotere digitale dienstverlening. De centrale onderzoeksvraag is: *“Wat beïnvloedt de bereidheid van studenten om hun persoonlijke gegevens te delen met de overheid voor gepersonaliseerde diensten?”*

1.1. Wetenschappelijke relevantie

De opkomst van digitale overheidsdiensten heeft geleid tot een toename in onderzoek naar de relatie tussen burgers en overheid in het digitale domein (van Helden et al., 2013). Steeds meer diensten worden digitaal; deze verschuiving heeft geleid tot een groeiende stroom van wetenschappelijke literatuur over onderwerpen als e-governance, digitale burgerschapsparticipatie en de maatschappelijke implicaties van datagedreven overheidshandelen (Mergel et al., 2019; OECD, 2007). Binnen deze literatuur wordt in toenemende mate aandacht besteed aan de discussie tussen de efficiëntie van digitale overheidsdiensten en de zorgen over privacy en vertrouwen.

Hoewel onderzoek over deze onderwerpen relatief uitgewerkt is (Laufer & Wolfe, 1977; Mayer et al., 2007; Bannister & Connolly, 2011), is het zeer gefragmenteerd – zeker binnen bepaalde doelgroepen zoals jongeren en studenten. Studenten zijn al vaker onderzocht in andere landen (Al-Omairi et al., 2020; Méndez-Rivera et al., 2023; Mensah, 2019) maar het onderzoek richt zich vooral op ontwikkelingslanden of landen met andere overheidssystemen zoals China, wat het moeilijk toepasbaar maakt op de Nederlandse samenleving. Studenten zelf vormen een interessante casus vanwege hun digitale vaardigheid, afhankelijkheid van digitale overheidsdiensten (zoals studiefinanciering of DigiD in het algemeen) en hun vaak onstabiele institutionele positie. Tegelijkertijd zijn studenten ondervertegenwoordigd in bestaande onderzoeken die zich vooral richten op algemene populaties of beleidsprofessionals (OECD, 2016; European Data Protection Board, 2023).

Dit onderzoek beoogt dus een gerichte bijdrage te leveren aan de wetenschappelijke discussie over digitale overheid en datagedrag op een doelgroepgerichte en contextspecifieke wijze. Door de houding van studenten ten opzichte van datadeling met de overheid te analyseren, kunnen inzichten ontstaan in hoe privacy- en vertrouwensoverwegingen samenkomen binnen deze bevolkingsgroep.

1.2. Maatschappelijke relevantie

Digitalisering van de overheid biedt grote maatschappelijke voordelen, maar stelt ook nieuwe eisen aan burgers. Het vermogen om digitaal te communiceren met de overheid is in toenemende mate een voorwaarde om toegang te krijgen tot fundamentele rechten en voorzieningen. Niet

iedere burger is daar echter in gelijke mate toe in staat. Terwijl digitalisering vaak wordt gerepresenteerd als een manier om publieke diensten efficiënter en gebruiksvriendelijker te maken, kunnen ongelijkheden in digitale geletterdheid en institutionele positie juist leiden tot nieuwe vormen van uitsluiting (Dedding & Goedhart, 2021).

Voor studenten is dit vraagstuk zeer relevant. Zij bevinden zich in een overgangsfase van afhankelijkheid naar zelfstandigheid, en zijn tegelijkertijd sterk afhankelijk van digitale overheidsdiensten voor zaken als studiefinanciering, belastingzaken en gemeentelijke registratie. Deze afhankelijkheid impliceert een structurele kwetsbaarheid: studenten kunnen zich moeilijk onttrekken aan digitale interactie met de overheid, wat maakt dat vertrouwen in deze systemen geen vrijblijvende keuze is, maar een noodzakelijke voorwaarde voor maatschappelijke participatie. Wanneer dit vertrouwen onder druk komt te staan – bijvoorbeeld door discriminerende algoritmes of gebrekkige transparantie – kunnen gevoelens van onmacht, wantrouwen of vervreemding ontstaan. Tegelijkertijd worden zij vaak gezien als ‘digital natives’, waardoor beleidsmakers geneigd zijn hun digitale vaardigheden te overschatten. Jongeren zijn vaak handig met specifieke platforms of sociale media apps, maar hebben moeite met het overdragen van deze vaardigheden naar andere omgevingen (Kennisnet, 2020).

Daarnaast toont onderzoek dat jongeren vaak hun eigen digitale vaardigheden overschatten. Een studie van de European Computer Driving License Foundation (2015) benadrukt dat blootstelling aan technologie niet gelijkstaat aan het effectief kunnen gebruiken ervan. Veel jongeren missen de noodzakelijke digitale vaardigheden – inclusief dataprivacy. Hierdoor lopen jongeren het risico om zich onvoldoende bewust te zijn van hoe en waarvoor hun gegevens worden gebruikt, wat digitale vertrouwensrelaties onder druk zet.

Het maatschappelijk belang van dit onderzoek ligt dan ook in het vergroten van begrip voor hoe studenten deze digitale relatie met de overheid ervaren, en welke voorwaarden zij stellen aan vertrouwen, privacy en gebruiksgemak. Deze inzichten kunnen bijdragen aan beleidsvorming rond transparanter en rechtvaardiger datagebruik, en helpen om digitale publieke diensten inclusiever en responsiever te maken voor jongvolwassen burgers.

2. Theoretisch Kader

Dit hoofdstuk biedt het theoretisch fundament voor de analyse van datadeelgedrag onder studenten in relatie tot de digitalisering van publieke dienstverlening. Aan de hand van bestaande literatuur worden de kernconcepten digitale vaardigheden, privacybewustzijn, institutionele afhankelijkheid, institutioneel vertrouwen en de privacy calculus uitgewerkt. Deze concepten vormen samen het analytisch raamwerk waarmee de empirische bevindingen in de daaropvolgende hoofdstukken worden geïnterpreteerd.

2.1. Literatuur

Digitale technologieën hebben een enorme invloed op de relatie tussen burgers en overheid. De tijd van fysieke loketten, vaste openingstijden en persoonlijke interactie is voorbij, en wordt steeds meer vervangen door digitale interactie, zelfbedieningsportalen en geautomatiseerde besluitvorming (Dunleavy et al., 2005). Dit proces – ook wel aangeduid als Digital Era Governance – herstructureert de organisatie van publieke dienstverlening, maar ook de manier waarop burgers interacteren met overheidsautoriteit (Meijer & Bekkers, 2015).

Vanwege digitalisering kunnen overheden steeds efficiënter en effectiever werken. De impact van digitalisering op de aard van publieke interactie is echter ook groot; we kunnen als burgers steeds minder zien wat er achter de schermen gebeurt bij de overheid, terwijl de informatieasymmetrie tussen burger en staat toeneemt. Er is steeds minder inzicht in hoe beslissingen genomen worden, en burgers moeten steeds meer vertrouwen op ‘black-box’ algoritmen en dataprocessen (Bannister & Connolly, 2011). Hierdoor zijn er steeds meer vragen over transparantie, verantwoordelijkheid en controle in het publieke domein.

De verbetering in dienstverlening komt ook met nieuwe vormen van afhankelijkheid. Het is steeds minder noodzakelijk om fysieke en menselijke interactie te hebben voor overheidszaken. Burgers moeten online hun zaken regelen, wat steeds meer digitale toegang en vaardigheden vereist. Burgers die deze vaardigheden niet hebben kunnen worden uitgesloten van essentiële overheidsdiensten, wat leidt tot meer sociale vervreemding. Digitalisering kan overheidsprocessen beter laten verlopen, maar dus ook negatieve gevolgen hebben afhankelijk van hoe ze worden ontworpen en ervaren (Margetts & Dunleavy, 2013).

Ten slotte leidt digitalisering tot een vernieuwing van de rol van de burger. Van passieve ontvanger van diensten worden burgers steeds meer geacht actieve beheerders van hun eigen data te zijn. Ze moeten beslissingen nemen over welke data ze delen, onder welke voorwaarden, en met welk vertrouwen in de overheid, als databeheerder (van Zoonen, 2016).

2.1.1. Rationele afweging

Het is belangrijk om te begrijpen waarom burgers bepaalde keuzes maken, en hoe zij afwegen welke gegevens ze bereid zijn om af te staan aan de overheid. De bereidheid van burgers om persoonlijke data te delen kan worden begrepen aan de hand van verschillende concepten. Een van deze kernconcepten is de Privacy Calculus Theory (PCT). Laufer en Wolfe (1977) presenteren privacy als een multidimensionaal en dynamisch concept. Zij onderscheiden drie dimensies: zelf-ego (individuele autonomie en controle over persoonlijke informatie), omgeving (bescherming van persoonlijke ruimtes en gegevens) en interpersoonlijke relaties (beheer van informatie in sociale interacties). Daarnaast introduceren ze een ontwikkelingsperspectief, waarbij privacyrecepties veranderen door persoonlijke en maatschappelijke evoluties. Hun werk vormt de basis voor latere studies naar privacy en de afweging tussen persoonlijke controle en externe invloeden.

Kritiek op rationele afweging

Hoewel het artikel zeer invloedrijk was, is er veel kritiek geweest op de theorie en de onderbouwing ervan. Een artikel dat direct kritiek heeft op de standpunten van Laufer en Wolfe (1997) is dat van Sigmund en Korčák (2021). Zij onderzoeken hoe altruïsme een rol speelt in privacy beslissingen en beargumenteren dat de traditionele privacy calculus theorie tekortschiet door te veronderstellen dat privacy keuzes puur op rationele kosten-batenanalyses gebaseerd zijn. Zij voegen een altruïstische dimensie toe aan de PCT en tonen aan dat privacybeslissingen niet alleen afhangen van persoonlijke risico's en voordelen, maar ook van sociale en ethische overwegingen. Uit hun onderzoek blijkt dat studenten zich bewust zijn van bredere maatschappelijke gevolgen van datadeling, zoals de impact op online surveillance en collectieve

privacy. Dit ondermijnt de klassieke PCT omdat het suggereert dat niet alleen egoïstische motieven, maar ook prosociale en morele factoren privacygedrag beïnvloeden.

Acquisti et al. (2016) gaan een stap verder, en betogen dat privacybeslissingen inherent irrationeel zijn. Zij onderzoeken hoe psychologische en gedragsmatige factoren privacybeslissingen beïnvloeden. Anders dan Laufer en Wolfe (1997), stellen Acquisti et al dat privacykeuzes niet altijd rationeel zijn maar afhankelijk van context, heuristieken en emotionele prikkels. Ze introduceren drie mechanismen: onzekerheid (waarbij mensen onzeker zijn over hoe hun data gebruikt wordt), contextafhankelijkheid (waarbij beslissingen afhankelijk zijn van sociale en emotionele prikkels) en ‘maladaptive heuristics’ (waarbij mensen irrationele shortcuts gebruiken zoals overmatig vertrouwen op standaardinstellingen zonder er over na te denken). Acquisti et al. (2016) tonen aan dat burgers vaak niet in staat zijn om rationele keuzes te maken vanwege psychologische biases of de manier waarop informatie wordt gepresenteerd.

Het artikel van van Zoonen (2016) kijkt verder dan de interne keuzes van burgers. In haar onderzoek ontwikkelde ze een raamwerk gebaseerd op twee dimensies: de mate waarin gegevens als persoonlijk en gevoelig worden ervaren, en het doel van de gegevensverzameling, met een onderscheid tussen service- en surveillancedoeleinden. van Zoonen suggereert dat privacyzorgen niet alleen afhangen van kosten-baten afweging, maar ook sterk wordt beïnvloed door de aard van de gegevens en het doel van de verzameling. Data die onpersoonlijk en geaggregeerd is zoals verkeersstromen en luchtkwaliteit worden eerder gedeeld dan persoonlijke en identificeerbare data (zoals biometrische gegevens of locatiegegevens). Burgers maken niet simpelweg een kosten-batenanalyse maar kijken volgens haar voornamelijk naar het doel van de dataverzameling.

Rationele afweging herzien

Het onderzoek van Meier en Krämer (2024) bouwt voort op het onderzoek van Laufer en Wolfe (1977) en met name de Privacy Calculus theorie. De auteurs voerden een experimenteel onderzoek uit waarbij zij hen drie zelfonthullingsscenario's lieten beoordelen met een zogenaamde ‘privacy score’, een hulpmiddel dat privacyrisico’s weergeeft. De resultaten toonden aan dat mensen vooral geneigd zijn om informatie te delen wanneer de verwachte voordelen hoog zijn, ongeacht de waargenomen privacyrisico’s. De privacy score hielp

gebruikers echter om zich meer bewust te worden van deze risico's, vooral bij intuïtieve besluitvormers. Belangrijke vernieuwingen van dit onderzoek ten opzichte van dat van Laufer en Wolfe (1977) zijn:

- Het gebruik van binnen-persoonlijke variatie: Terwijl het oorspronkelijke onderzoek vooral generalisaties op populatieniveau maakte, introduceert dit onderzoek een gedetailleerde analyse van hoe privacybeslissingen binnen één individu kunnen verschillen per situatie.
- Gebruik van experimentele manipulatie (privacy score): In plaats van alleen zelfrapportage te gebruiken, testen ze een instrument dat privacybewustzijn kan verhogen en zo privacybeslissingen kan beïnvloeden.
- Interactie met besluitvormingsstijlen: Ze koppelen privacybeslissingen aan rationele en intuïtieve besluitvorming, wat een verdere psychologische verdieping biedt ten opzichte van Laufer en Wolfe's oorspronkelijke werk.

Meier en Krämer bouwen dus voort op eerder onderzoek door het Privacy Calculus model empirisch te toetsen met een experimentele benadering en door privacybesluitvorming zowel op tussen- als binnen-persoonsniveau te analyseren. Dit biedt een betere kijk op hoe individuen in verschillende situaties omgaan met de spanning tussen privacy en zelfonthulling.

2.1.2. Institutioneel vertrouwen

Vertrouwen in diensten en de overheid is een tweede kernconcept dat invloed heeft op de bereidheid om gegevens te delen met overheidsinstanties. Mayer et al. (2007) ontwikkelden een fundamenteel model van vertrouwen, dat sindsdien veelvuldig is toegepast in onderzoek naar institutioneel vertrouwen. Het model stelt dat vertrouwen bestaat uit drie kerncomponenten: bekwaamheid (de mate waarin een organisatie zoals de overheid capabel is om goed beleid uit te voeren en data veilig te beheren, integriteit (of de overheid eerlijk en transparant handelt, en ethische normen respecteert) en welwillendheid (of burgers geloven dat de overheid handelt in het belang van de samenleving, en niet puur uit eigenbelang). Hoewel deze drie kerncomponenten een goede basis vormen voor institutioneel vertrouwen, is het niet genoeg om de bereidheid van datadelen van burgers te verklaren. Verder gaat het ook niet in op de digitalisering van overheidsdiensten en hoe dit invloed heeft gehad op institutioneel vertrouwen.

Institutioneel vertrouwen en digitalisering

Bannister en Connolly (2011) analyseren de complexiteit en mogelijke negatieve gevolgen van transparantie in elektronische overheidsdiensten. Ze stellen dat hoewel transparantie vaak wordt gezien als inherent positief, het in bepaalde contexten kan leiden tot inefficiëntie, verminderde effectiviteit en zelfs een afname in het publieke vertrouwen. Ze benadrukken dat overmatige transparantie besluitvormingsprocessen kan verstoren en publieke dienaren kan ontmoedigen om openlijk te debatteren en innovatieve ideeën te delen, uit angst voor publieke kritiek. Deze inzichten vormen een kritiek op de definitie van Mayer et al. (2007) die vertrouwen beschrijven als *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"* (p. 712). Bannister en Connolly betogen dat overmatige transparantie juist kan leiden tot een afname van vertrouwen, omdat het de natuurlijke werking van overheidsprocessen belemmert en een cultuur van wantrouwen kan creëren.

Het doel van de overheidsdienst heeft ook impact op het vertrouwen van overheidsdiensten en de algemene perceptie van burgers. Li en Shang (2023) onderzoeken de invloed van digitale overheidsdiensten op het vertrouwen in de overheid in China. Op basis van een enquête van 1668 burgers in vijf steden werd aangetoond dat digitale overheidsdienst gebruik indirect bijdraagt aan vertrouwen via betere percepties van overheidsintegriteit, prestaties en responsiviteit. Verschillende typen gebruik hebben uiteenlopende effecten: informatie zoeken vergroot de perceptie van integriteit, online transacties versterken de perceptie van prestaties, en burgerparticipatie verhoogt de externe politieke effectiviteit. Echter, hoge verwachtingen van transparantie, efficiëntie en responsiviteit matigen deze positieve effecten, waardoor teleurstelling kan optreden. Opvallend is dat digitale overheidsdienst gebruik vooral het vertrouwen in lokale overheden disproportioneel versterkt. De studie benadrukt het belang van realistische verwachtingen en transparantie in e-government beleid om vertrouwen te bevorderen. Hoewel dit artikel over institutioneel vertrouwen gaat, impliceert het toch een privacy calculus. Burgers wegen verwachte voordelen (efficiëntie, gemak) af tegen potentiële risico's (gebrek aan transparantie, teleurstelling over responsiviteit). Dit kan helpen bij het verklaren waarom sommige burgers digitale overheidsdiensten vertrouwen en gebruiken, terwijl anderen sceptisch blijven.

Six en Latusek (2023) richtten hun onderzoek niet op vertrouwen, maar wantrouwen. Als deel van het onderzoek is een universele wantrouwensequentie ontwikkeld, gebaseerd op voorgaand onderzoek. Ze stellen dat wantrouwen niet simpelweg de afwezigheid van vertrouwen is, maar een actief proces met eigen triggers en versterkende mechanismen. Hun model identificeert drie kernfactoren die wantrouwen opbouwen: incompetentie, kwaadwilligheid en misleiding. Ze benadrukken dat wantrouwen vaak hardnekkiger en emotioneel intenser is dan vertrouwen, wat het moeilijker maakt om te herstellen. Daarnaast analyseren ze hoe wantrouwen zich verspreidt, bijvoorbeeld via sociale netwerken en digitale platformen, en hoe dit institutioneel wantrouwen kan voeden. Dit artikel bouwt voort op voorgaande literatuur zoals dat van Mayer et al. (2007) over vertrouwen en verbreedt het op een conceptueel niveau. In tegenstelling tot Mayer et al. wordt wantrouwen als meer gezien dan de afwezigheid van vertrouwen of een passieve toestand, maar als een dynamisch en escalatie-gevoelig proces.

Institutioneel vertrouwen herzien

Het grootste overkoepelende onderzoek over vertrouwen in digitale overheidsdiensten is een literatuuronderzoek van Alzahrani et al. (2017), die factoren analyseren die vertrouwen in digitale overheidsdiensten verklaren. Dit is gebaseerd op een aangepaste versie van het DeLone & McLean IS Succes Model (DeLone & McLean, 2003). De zes componenten van het originele model (systeemkwaliteit, informatiekwaliteit, gebruik, gebruikerstevredenheid, individuele impact en organisatorische impact) zijn gecondenseerd tot vier factoren die invloed hebben op vertrouwen in digitale overheidsdiensten. Ze identificeren vier kernaspecten: technische kwaliteit, overheidsvertrouwen, burgerspecifieke kenmerken en risicoperceptie. Deze vier factoren beïnvloeden vertrouwen in digitale dienstverlening, wat op zijn beurt de intentie om digitale dienstverlening te gebruiken vergroot. Ik zal de bijdragen aan vertrouwen in digitale overheidsdiensten kort beschrijven.

De studie van Welch et al. (2004) toont dat negatieve ervaringen met offline overheidsdiensten vaak leiden tot wantrouwen voor digitale overheidsdiensten. Dit geldt ook wederzijds; burgers die vertrouwen hebben in traditionele overheidsdiensten zijn eerder geneigd digitale diensten te gebruiken (Colesca, 2009). Overheden met een sterke reputatie op het gebied

van gegevensbescherming en privacybeleid krijgen ook sneller vertrouwen van burgers (Wang & Lo, 2013).

Individuele kenmerken, eigenschappen en eerdere ervaringen van burgers spelen ook een rol in het vertrouwen van digitale overheidsdiensten. Gebruikers met meer ervaring met digitale technologieën tonen hogere niveaus van vertrouwen in digitale overheidsdiensten (Srivastava & Teo, 2009). Digitaal vaardige gebruikers zijn minder bezorgd over het gebruik van online overheidsdiensten. De achtergrond van burgers speelt ook een rol: individuen die autoriteiten van nature wantrouwen zijn minder snel geneigd digitale overheidsdiensten te vertrouwen of te gebruiken (Warkentin et al., 2002). Leeftijd en opleidingsniveau zijn hier niet van uitgezonderd. Oudere en lager opgeleide burgers hebben vaak meer terughoudendheid bij het gebruik van digitale overheidsdiensten (Carter & Belanger, 2005), wat beleidsmakers dwingt om gebruiksvriendelijke en inclusieve platforms te ontwikkelen die door een bredere lagen van burgers gebruikt kan worden.

De factor “risico’s en beveiliging” verwijst naar de waargenomen gevaren en zorgen die burgers hebben over privacy en gegevensbescherming bij het gebruik van digitale overheidsdiensten. Hoge privacyzorgen verminderen het vertrouwen in digitale dienstverlening aanzienlijk (Bélanger & Carter, 2008). Mensen zijn terughoudend om persoonlijke gegevens te delen als ze twijfelen aan de beveiliging van digitale systemen. Wang en Lu (2010) tonen ook aan dat de perceptie van risico’s vaak zwaarder weegt dan werkelijke risico’s. Overheden moeten daarom actief communiceren over beveiligingsmaatregelen en transparantie bevorderen.

2.2. Samenvatting modellen

De bovenstaande wetenschappelijke artikelen bieden verschillende verklaringen voor de bereidheid van burgers om persoonlijke data te delen met de overheid. Waar de theorie van rationele afweging uitgaat van een kosten-batenanalyse op individueel niveau, richt de benadering van institutioneel vertrouwen zich op de bredere context van vertrouwen in digitale overheidsdiensten. Om de verschillen en overeenkomsten tussen deze perspectieven overzichtelijk weer te geven, wordt in figuur 1 een vergelijking gepresenteerd.

Figuur 1*Vergelijkende tabel Privacybeslissingen*

	Herziene Institutionele vertrouwen	Rationele afweging (Privacy Calculus)
Kernidee	Burgers baseren hun bereidheid om informatie te delen met overheden op verscheidene factoren	Burgers wegen privacyrisico's en voordelen af voordat ze persoonlijke informatie delen
Factoren die invloed hebben op privacybeslissingen	Technische kwaliteit, overheidsvertrouwen, gebruikersspecifieke kenmerken, risicoperceptie	Perceptie van risico's en voordelen, rationaliteit, contextafhankelijkheid
Type besluitvorming	Vertrouwen in overheidsdiensten als drijvende factor	Kosten-batenanalyse door individuen
Kritiek	Te veel transparantie kan vertrouwen schaden, wantrouwen heeft eigen mechanismen (Six & Latusek, 2023)	Beslissingen zijn niet altijd rationeel; psychologische factoren beïnvloeden keuzes (Acquisti et al, 2016)
Empirische benadering	Gebruik van modellen zoals het Delone & McLean IS Success Model (2003), metingen gebaseerd op enquêtes en theoretische kaders	Experimentele studies met manipulatie van privacybewustzijn, zoals privacy scores en heuristische besluitvorming

2.3. Verantwoording van theoriekeuze

Er zijn verschillende theorieën die mogelijk relevant zouden zijn voor het verklaren van de bereidheid om data te delen van studenten met betrekking tot digitale overheidsdiensten. Toch is er gekozen voor PCT en institutioneel vertrouwen. Deze keuze is gebaseerd op de centrale rol die beide theorieën spelen in de verklaring van datadeelbereidheid en de relatie daarvan met vertrouwen in overheidsdiensten. Alternatieve theorieën zoals het Technology Acceptance Model (TAM) of Innovation Resistance Model (IRT) richten zich voornamelijk op de technologische adoptie en gebruikersgemak, maar besteden relatief weinig aandacht aan privacy en vertrouwen, wat de kern is van dit onderzoek (Alarabiat et al., 2017; Talwar et al., 2020). Communication

Privacy Management Theory (CPM) biedt ook inzichten in vertrouwen en toepasbaar aan digitalisering, maar de theorie is vooral ontwikkeld voor interpersoonlijke contexten en niet voor institutionele verhoudingen tussen burger en staat (Petronio & Child, 2020).

2.4. Studenten en digitale overheidsdiensten

Zoals eerder besproken heeft de digitalisering van overheidsdiensten de interactie en verhouding tussen burger en staat aanzienlijk veranderd. Voor studenten die vaak worden bestempeld als ‘digital natives’ (Prensky, 2001) (omdat deze generatie geboren is in het informatietijdperk) betekent dit dat ze in hoge mate afhankelijk zijn van digitale platforms en portalen voor zaken zoals studiefinanciering (MijnDUO), belastingaangifte (MijnBelastingdienst), en gemeentelijke registratie (Portalen via DigiD). Ondanks hun digitale vaardigheid blijkt uit onderzoek dat studenten weinig aandacht geven aan online privacy en gegevensdeling met private partijen (Smaling, 2017). Hoewel uit de enquête bleek dat studenten privacy belangrijk vonden, gaf de meerderheid toe niet veel te doen om hun data te beschermen. Daarnaast bevinden studenten zich vaak in een overgangsfase tussen institutionele afhankelijkheid (zoals bij DUO) en toenemende autonomie. Deze levensfase kan leiden tot een ambivalente houding ten opzichte van vertrouwen in digitale overheidssystemen.

Bovendien wordt veel overheidsdata opgeslagen op de cloud, waarvan een groot deel in de handen van Amerikaanse bedrijven (Merien, 2025). Dit roept zorgen op over privacy en gegevensbescherming, aangezien buitenlandse overheden mogelijk toegang kunnen eisen tot deze data, of onveilig om kunnen gaan met de datahuishouding daarvan. Hoewel de Tweede Kamer dit gepauzeerd heeft, staan aanzienlijke hoeveelheden data nog op deze servers (van Harreveld, 2025).

Deze factoren benadrukken het belang van transparantie en verantwoord datagebruik door overheidsinstanties om het vertrouwen van studenten in digitale diensten te waarborgen. Het is essentieel dat studenten niet alleen bewust worden gemaakt van de implicaties van datadeling, maar ook dat zij controle krijgen over hun data. Door studenten als een aparte gebruikersgroep te beschouwen wordt duidelijk dat hun specifieke behoeften en zorgen rondom digitale overheidsdiensten aandacht behoeven. Het adresseren van deze kwesties is cruciaal voor het bevorderen van vertrouwen en het stimuleren van actieve participatie van studenten in de digitale samenleving.

2.5. Conceptueel model en verwachtingen

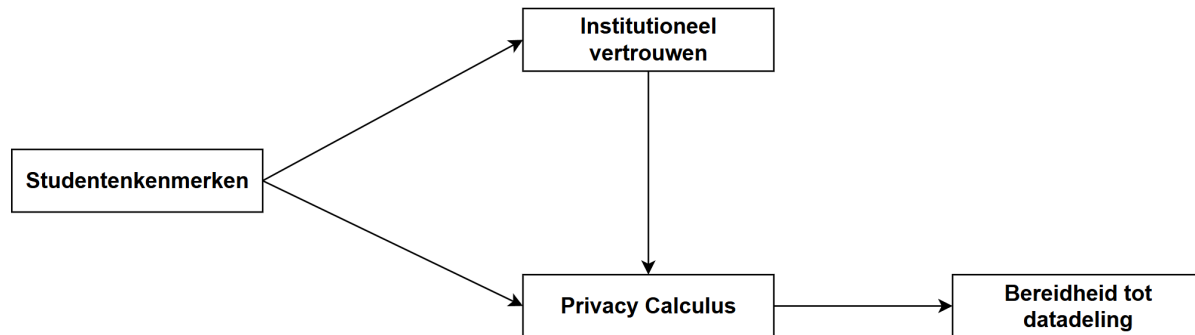
Op basis van de besproken literatuur wordt in dit deel van het theoretisch kader een conceptueel model opgesteld dat de verwachte samenhang tussen de kernvariabelen in dit onderzoek inzichtelijk maakt. Dit model zal de theoretische basis vormen voor het verklaren van de bereidheid van studenten om persoonlijke data te delen met de overheid in het kader van gepersonaliseerde digitale dienstverlening.

De twee stromingen uit het literatuuronderzoek vormen de kern voor het conceptueel model. Ten eerste biedt de Privacy Calculus theorie inzicht in hoe studenten de voordelen en risico's van datadeling afwegen. Hierbij spelen rationele, contextuele en psychologische factoren een grote rol. Ten tweede benadrukt het perspectief van institutioneel vertrouwen het belang van vertrouwen in de overheid en haar digitale systemen als voorwaarde voor vrijwillige datadeling. Daarnaast wordt erkend dat studenten als doelgroep bepaalde kenmerken vertonen, zoals hoge digitale vaardigheid, institutionele afhankelijkheid, en privacybewustzijn. Deze kenmerken kunnen de privacy-afweging en indirect het institutioneel vertrouwen beïnvloeden.

De relaties tussen de variabelen voor het model volgen logisch uit de besproken literatuur. Studentenkenmerken beïnvloeden zowel het vertrouwen in de overheid als de manier waarop studenten hun privacyafweging maken. Digitale vaardigheden, privacyattitudes en institutionele afhankelijkheid als jongvolwassen spelen hierbij als grote invloeden op de bereidheid van studenten. Institutioneel vertrouwen beïnvloedt vervolgens de rationele afwegingen in de privacy calculus. Wanneer studenten de overheid bijvoorbeeld als integer ervaren, zullen zij de risico's van datadeling lager inschatten en de voordelen eerder accepteren (Mayer et al., 1995; Alzahrani et al., 2017). De privacy calculus is de laatste stap, waar de student hun keuze maken of ze bereid zijn om hun data te delen met overheidsinstanties of niet. De afweging tussen waargenomen risico's en voordelen wordt mede gevormd door vertrouwen in de overheid en de kenmerken van de student. (Acquisti et al., 2016; Meier & Krämer, 2024). Het model kent dus een 'flowchart' structuur waarin studentenkenmerken beide verklaringroutes aflopen, en waarin institutioneel vertrouwen doorwerkt via de privacy calculus op de bereidheid van studenten. In figuur 2 is het model visueel te zien.

Figuur 2

Schematische weergave conceptueel model



Op basis van de literatuur en het conceptueel model formuleer ik een aantal hypothesen die de verwachte relaties tussen de variabelen uitwerken.

H1: Hoe hoger het institutioneel vertrouwen, hoe groter de bereidheid van studenten om persoonlijke gegevens te delen met de overheid.

H2: Hoe positiever de uitkomst van de privacy calculus, hoe groter de bereidheid van studenten om persoonlijke gegevens te delen met de overheid.

H3: Studenten met hogere digitale vaardigheden ervaren een positievere privacy calculus dan studenten met lagere digitale vaardigheden.

H4: Studenten met een sterk privacybewustzijn ervaren een negatievere privacy calculus dan studenten met een laag bewustzijn.

H5: Studenten die afhankelijker zijn van overheidsdiensten ervaren een positievere privacy calculus dan studenten met minder afhankelijkheid.

3. Methodologie

In dit hoofdstuk wordt de methodologische aanpak uiteengezet. Het doel van het onderzoek is om te begrijpen wat de bereidheid van studenten beïnvloedt met betrekking tot datadeelgedrag met de overheid voor gepersonaliseerde diensten. Vanwege het verkennende karakter is gekozen voor kwalitatief onderzoek met semi-gestructureerde interviews, die thematisch zijn opgebouwd op basis van het theoretisch kader, maar ruimte laten voor persoonlijke verdieping. De volgende paragrafen behandelen de casusselectie, dataverzameling, operationalisatie en validiteit van het onderzoek.

3.1. Casusselectie

Voor dit onderzoek is gekozen om semi-gestructureerde interviews af te nemen onder studenten in Nederland. Om een representatief beeld te verkrijgen van hoe studenten omgaan met datadeling in het kader van digitale overheidsdiensten, is ervoor gekozen om studenten te benaderen vanuit drie onderwijsniveaus: wo-, hbo- en mbo-studenten. Deze differentiatie is van belang, aangezien digitale vaardigheden, afhankelijkheid van overheidsdiensten en privacybewustzijn aanzienlijk kunnen verschillen per opleidingsniveau (Smaling, 2017).

Om de diversiteit binnen de studentenpopulatie te waarborgen, is gekozen voor een meervoudige locatiekeuze. Per onderwijsniveau zouden twee studenten worden geïnterviewd op elk van de drie locaties, wat had moeten leiden tot een totaal van 18 interviews ($3 \text{ locaties} \times 3 \text{ niveaus} \times 2 \text{ studenten}$). Deze opzet was bedoeld om te voorkomen dat studenten met dezelfde studieachtergrond geïnterviewd werden, omdat het zou kunnen leiden tot vergelijkbare antwoorden. Door de meivakantie is het echter niet gelukt om voldoende mbo-studenten te werven; in plaats van zes zijn slechts twee mbo-studenten geïnterviewd. Hierdoor komt het totale aantal respondenten op 14.

De drie geselecteerde steden zijn Den Haag, Leiden en Delft. Deze steden zijn gekozen op basis van pragmatische overwegingen zoals bereikbaarheid en beschikbare netwerken van de onderzoeker, maar bieden tegelijkertijd een breed scala aan onderwijsinstellingen. Per stad wordt geprobeerd om studenten van een universiteit (wo), hogeschool (hbo) en mbo-instelling te includeren. De locatieverdeling is als volgt:

- Den Haag: Universiteit Leiden (Campus Wijnhaven), Haagse Hogeschool.

- Leiden: Universiteit Leiden (Faculteit Pieter de la Court), Hogeschool Leiden, MBO Rijnland
- Delft: Technische Universiteit Delft, Hogeschool Inholland.

Deze locatiekeuze volgt een doelgerichte steekproefstrategie waarbij studenten worden geselecteerd op basis van hun verwachte informatierijkheid en relevantie voor het onderzoeksdoel (Yang & Miller, 2008). Door te werken met verschillende onderwijsniveaus en geografische locaties binnen de Randstad wordt getracht een zo rijk mogelijk inzicht te verkrijgen in de variatie binnen de doelgroep.

3.2. Methode van dataverzameling

Voor de dataverzameling is gekozen voor het afnemen van semi-gestructureerde interviews. Deze methode is geschikt om diepgaand inzicht te verkrijgen in de percepties, ervaringen en overwegingen van studenten met betrekking tot het onderzoek. Semi-gestructureerde interviews bieden enerzijds houvast via vooraf vastgestelde thema's met betrekking tot de literatuur, maar laten anderzijds ook ruimte voor doorvragen en het verkennen van onverwachte inzichten, passend bij dit exploratief onderzoek. De interviews zijn opgebouwd aan de hand van een interviewgids (zie figuur 3 in appendix), die thematisch gestructureerd is op basis van het conceptueel model uit het theoretisch kader.

3.3. Operationalisatie

Om de variabelen te operationaliseren wordt gebruikgemaakt van een codeerschema. Dit schema is gebaseerd op de wetenschappelijke literatuur uit het theoretisch kader en vormt een brug tussen de conceptuele theorievorming en de empirische dataverzameling. Elk concept uit het model is vertaald naar een set indicatoren die tijdens de interviews worden bevraagd. De keuze voor deze operationalisatie komt voort uit de theorie; de begrippen zijn ontleend aan bestaande modellen over privacybeslissingen, vertrouwen en digitale overheidsdiensten. Door deze modellen te koppelen aan interviewvragen wordt het mogelijk om de complexiteit van individuele overwegingen systematisch te analyseren. Daarnaast is het schema zodanig opgezet

dat het kan dienen als analytisch raamwerk tijdens de coderingsfase van de data-analyse. Het biedt structuur bij het ordenen van de transcripties, maar laat tegelijkertijd ruimte voor inductieve verfijning van codes tijdens het analyseren. In figuur 4 (zie appendix) wordt het codeerschema gepresenteerd, waarin per concept de definitie, bijbehorende interviewvragen en relevante theoretische bronnen worden weergegeven.

3.4. Validiteit en betrouwbaarheid

Bij kwalitatief onderzoek zoals dit is het waarborgen van validiteit en betrouwbaarheid essentieel voor de geloofwaardigheid van de bevindingen. In deze paragraaf worden de maatregelen besproken die zijn genomen om zowel de interne als externe validiteit, evenals de betrouwbaarheid, van het onderzoek te versterken.

De interne validiteit is relatief hoog vanwege de grote diversiteit van studenten en scholen, hoewel het hoger zou kunnen zijn door het op landelijk niveau te doen in alle provincies. Ook door gebruik te maken van een enkele interview procedure voor alle interviews kunnen de observaties met elkaar vergeleken worden.

Hoewel generaliseerbaarheid in kwalitatief onderzoek beperkt is, is er wel gestreefd naar theoretische en contextuele overdraagbaarheid. Door doelgericht studenten van verschillende onderwijsniveaus (mbo, hbo, wo) te selecteren op meerdere locaties (Den Haag, Leiden, Delft), wordt de kans vergroot dat diverse perspectieven binnen de bredere studentenpopulatie worden meegenomen. Deze ‘maximum variatie’ in de steekproef draagt bij aan het identificeren van patronen die mogelijk ook buiten deze specifieke context herkenbaar zijn. Hoewel het onderzoek geen statistische representativiteit nastreeft, biedt het wél aanknopingspunten voor vergelijkbare situaties binnen de Nederlandse context van digitaliserende overheidsdiensten.

Om de betrouwbaarheid van het onderzoek te vergroten, is de dataverzameling zo systematisch mogelijk uitgevoerd. Alle interviews worden opgenomen (na toestemming), en vervolgens getranscribeerd met behulp van Amberscript, gevolgd door handmatige controle. Voor de data-analyse wordt gebruikgemaakt van een vooraf opgesteld codeerschema, dat tijdens de analyse iteratief wordt verfijnd. Deze combinatie van deductieve en inductieve codering zorgt voor transparantie en herhaalbaarheid in de interpretatie van de data.

Tot slot wordt gebruikgemaakt van methodologische transparantie: keuzes rondom selectie, vraagstelling en analyse zijn expliciet verantwoord, zodat de lezer inzicht heeft in hoe tot bepaalde inzichten is gekomen. Daarmee wordt de geloofwaardigheid van de onderzoeksbevindingen versterkt.

4. Bevindingen

In dit hoofdstuk worden de empirische bevindingen gepresenteerd en geanalyseerd aan de hand van het in hoofdstuk 2 uitgewerkte theoretische kader. De analyse volgt de structuur van het conceptueel model: eerst wordt ingegaan op de invloed van digitale vaardigheden, privacybewustzijn en institutionele afhankelijkheid, waarna de rol van institutioneel vertrouwen wordt besproken. Tot slot worden de afwegingen binnen de privacy calculus behandeld, in samenhang met de voorgaande factoren. Op deze manier wordt inzicht verkregen in de mechanismen achter datadeelgedrag onder studenten.

4.1. Digitale vaardigheden

WO-studenten beoordelen hun digitale vaardigheden als hoog (7–9), met motieven als een technische achtergrond, werkervaring of interesse in digitalisering. Twee studenten maken gebruik van geavanceerde digitale middelen zoals VPN's, wachtwoordmanagers of privacyplug-ins (WO 4 en 6), wat wijst op bovengemiddelde digitale competentie. Andere studenten beperken zich tot basale voorzorgsmaatregelen, zoals het vermijden van bepaalde websites of het bewust omgaan met cookies (WO 6).

Opvallend is dat studenten erkennen dat digitale vaardigheid niet betekent dat ze alles begrijpen: ondanks hun ervaring weten ze soms niet precies wat overheidsapps met hun data doen (WO 2), of zijn ze kritisch op automatische systemen die zonder uitleg besluiten nemen (WO 4). Studenten lijken zich goed digitaal te kunnen redden, maar blijven alert op risico's van datagebruik, zonder dat dit altijd leidt tot consequent privacybeschermend gedrag.

De HBO-studenten in dit onderzoek schatten hun digitale vaardigheden gemiddeld in tussen een 6 en een 7,5. Deze zelfinschatting wordt onderbouwd met uiteenlopende motieven, zoals vertrouwdheid met digitale formulieren en het lezen van voorwaarden (HBO 2), of het opgroeien met technologie. De lagere kant werd onderbouwd met terugkerende zoekproblemen of afhankelijkheid van ouders (HBO 1).

Wat betreft digitale veiligheid is de toepassing van vaardigheden wisselend. Sommige studenten nemen meerdere maatregelen, zoals HBO 5, die zowel een VPN gebruikt als sterke wachtwoorden. Anderen noemen enkel basale voorzorgsmaatregelen, zoals het gebruik van

sterke wachtwoorden (HBO 1 en HBO 6), of antivirussoftware (HBO 3). Bij deze groep lijkt de digitale vaardigheid vooral functioneel en beperkt tot wat direct noodzakelijk is, zonder verdere verdieping of eigen initiatief.

Hoewel studenten zichzelf relatief bovengemiddeld inschatten, blijkt uit hun toelichtingen dat hun kennis vaak beperkt blijft tot alledaags gebruik. Zo stelt een student: *“Ik heb nog niet echt veel doorgelezen op de site van DUO... ik zou daar wel meer op kunnen kijken”* (HBO 5). Een ander zegt: *“Ik weet niet eens wat ze met mijn data doen”* (HBO 4). Deze uitspraken laten zien dat digitale zelfredzaamheid bij veel studenten weliswaar voldoende is voor praktisch gebruik, maar tekortschiet in kritisch en technisch inzicht, waardoor er ruimte blijft voor versterking van databewustzijn en controle.

Beide mbo-studenten beoordelen hun digitale vaardigheden als laag tot gemiddeld. MBO 1 geeft zichzelf een 6 en voelt zich redelijk zelfredzaam met DigiD, terwijl MBO 2 zichzelf een 3 geeft en weinig interesse toont in digitale technologie. Hun gebruik van digitale overheidsdiensten is beperkt en vooral functioneel van aard. In de toepassing blijken vaardigheden vooral gericht op noodzakelijke handelingen, zoals het aanvragen van een ID of het invullen van formulieren. Verdere verdieping of proactief gebruik van digitale beveiliging blijft achterwege.

4.2. Privacybewustzijn en attitude

WO-studenten tonen een relatief hoog bewustzijn van online privacy; alle zes beschouwen hun persoonsgegevens als waardevol en kwetsbaar. Dit komt voort uit zowel bezorgdheid als uit eigen ervaring. Zoals één student aangeeft: *“Data online is heel makkelijk te delen en te hacken... het is heel belangrijk om dat goed te bewaren”* (WO 2). Tegelijkertijd leeft het besef dat volledige bescherming lastig is: *“Ik weet niet wat er met die data gebeurt... dus daar zitten wel gaten in, ja”* (WO 5).

Toch is er een duidelijke kloof tussen houding en gedrag. Vier van de zes studenten geven aan dat zij ondanks hun privacybewustzijn beperkte of inconsistente maatregelen nemen. Een student noemt het gebruik van notities op de telefoon als wachtwoordopslag (WO 1), terwijl een ander stelt: *“Je bent soms gewoon laks bij sommige delen”* (WO 2). Ook zijn maatregelen vaak

basaal of incidenteel, zoals het vermijden van TikTok (WO 6) of het gebruik van adblockers zonder structurele bescherming (WO 3).

Wat betreft dataverzameling door de overheid zijn studenten verdeeld. Drie studenten uiten expliciet vertrouwen zolang de doeleinden duidelijk zijn (WO 3, 4 en 6). De resterende drie studenten hebben andere opinies, zoals het niet vertrouwen van de datahuishouding (WO 1), zelfgerapporteerde onmachtigheid (WO 2), en brede afkeuring van dataverzameling door de overheid (WO 5).

Onder HBO-studenten varieert het privacybewustzijn sterk. Vier van de zes respondenten geven aan privacy belangrijk te vinden, maar de diepgang van hun motieven en de mate waarin zij ernaar handelen verschilt. Eén student zegt: *“Privacy is wel belangrijk... het is fijn dat niet iedereen weet waar je woont, wat je doet, wie je bent”* (HBO 5). Tegelijk tonen twee studenten weinig betrokkenheid bij het onderwerp. Eén van hen zegt: *“Nee, het maakt me niet zoveel uit wat ze met mijn gegevens doen eigenlijk”* (HBO 1).

Hier is ook een (kleinere) kloof tussen houding en gedrag. Slechts drie van de zes studenten nemen actieve maatregelen, zoals het weigeren van cookies (HBO 2, HBO 6) of het gebruik van VPN (HBO 5). Anderen vertrouwen vooral op standaardinstellingen of laten maatregelen achterwege: *“Niet echt. Ja, normale dingen, maar die zitten al ingebouwd”* (HBO 4). Eén student merkte zelfs op: *“Ik ben er twee maanden geleden pas achtergekomen dat je cookies kunt weigeren”* (HBO 6).

Wat betreft overheidsdataverzameling zijn HBO-studenten verdeeld. Drie studenten geven aan dat ze de overheid in principe vertrouwen met hun data (HBO 1, 4 en 5), terwijl twee anderen expliciet wantrouwen uiten over overmatig gebruik of onduidelijke doelen (HBO 2 en 6). Eén student geeft aan dat algoritmische fouten zijn vertrouwen aantasten: *“...sommige data hebben ze echt wel nodig om hun diensten aan jou te kunnen bewijzen ... Ik weet dat niet zeker, maar dat is een aanname dat ze eigenlijk best nog wel wat data gebruiken die ze eigenlijk misschien niet nodig hebben, maar puur voor andere doeleinden. Ja daar ben ik niet zo'n fan van.”* (HBO 2).

Beide mbo-studenten geven aan privacy belangrijk te vinden, maar uiten dit op verschillende manieren. MBO 1 maakt zich vooral zorgen in situaties waarin anonimiteit gewenst is, bijvoorbeeld bij het uiten van meningen. Voor overige situaties *“maakt het niet veel uit”*. Maatregelen blijven beperkt tot het vermijden van het gebruik van de eigen naam op online

platforms. MBO 2 toont meer bewustzijn en verwijst naar berichten over grootschalige dataverzameling. Er worden actief cookies geweigerd en er worden niet overal accounts aangemaakt. Tegelijkertijd wordt benadrukt “*niets te verbergen*” te hebben, wat de zorgen relativeert. Beide studenten geven aan zelden bewust na te denken over hun datagedrag.

4.3. Institutionele afhankelijkheid

Vier van de zes WO-studenten (WO 1, 2, 3, 5) geven in de interviews aan dat zij zich afhankelijk voelen van digitale overheidsdiensten, met name voor essentiële zaken zoals studiefinanciering en belastingaangifte. Deze afhankelijkheid wordt meestal als vanzelfsprekend ervaren. “*Ik voel mij heel afhankelijk van [DUO], want ik ben student dus ik heb het wel echt nodig... ik moet mijn geldzaken delen, anders krijg ik geen lening*” (WO 1). Ook anderen benoemen het structurele karakter van deze afhankelijkheid: “*Jawel, flink. Je weet zelf ook wel dat wanneer er een storing is in DUO ... dat alles digitaal is, dat is natuurlijk wel gevaarlijk*” (WO 2).

Tegelijk ervaren studenten het gebruik van digitale diensten zelden als problematisch. Alle WO-studenten beschouwen digitalisering als iets wat het leven vergemakkelijkt. “*Bij alles wat ik digitaal kan doen, doe ik digitaal met de overheid*” (WO 3), en “*Het bespaart tijd, is efficiënter... je hoeft niet te zoeken naar een bepaald loket*” (WO 4). Niemand geeft de voorkeur aan analoge methoden, al zou één student die gebruiken als digitaal niet beschikbaar is (WO 3). Tegelijk uiten sommigen zorgen over machtsongelijkheid: “*Als de overheid nou zegt van: geef mij die data, anders krijg je geen geld meer, ja dan moet ik wel*” (WO 6). Anderen herkennen het gemak van digitale interactie als factor die hun bereidheid tot datadeling beïnvloedt. “*Ik denk dat ik daardoor wel makkelijker data deel, omdat ik weet dat daardoor diensten toegankelijker worden. Dus ik sta dan wel meer open om data te delen*” (WO 4).

Vijf van de zes HBO-studenten (HBO 1, 2, 3, 5, 6) geven aan zich in meerdere of mindere mate afhankelijk te voelen van digitale overheidsdiensten, vooral voor studiefinanciering, DigiD, visumaanvragen en rijbewijzen. Die afhankelijkheid wordt meestal als vanzelfsprekend ervaren: “*Ik moet bijvoorbeeld voor mijn rijbewijs een gezondheidsverklaring invullen... je betaalt geld, maar je levert ook je gegevens aan. Je hebt het gewoon nodig*” (HBO 2) en “*Ik heb er nooit echt bij stilgestaan dat je dat ook analoog kunt doen... ik denk wel dat ik*

afhankelijk ben” (HBO 5).

Vijf studenten (HBO 1, 3, 4, 5, 6) geven de voorkeur aan digitale interactie met de overheid, die als gemakkelijk en efficiënt wordt ervaren. *“Ik doe het liever vanuit thuis”* (HBO 3), aldus één student. Niemand spreekt een voorkeur uit voor analoge alternatieven, al worden die wel herkend.

Drie studenten (HBO 2, 5, 6) geven aan dat hun gevoel van afhankelijkheid of het ervaren gemak hun bereidheid om data te delen verhoogt. *“Ik ben er afhankelijk van, dus dan ben je meer bereid om die data te delen”* (HBO 2), en *“Als alles online moet, dan deel ik sneller mijn data... ook al is dat misschien kwetsbaar”* (HBO 5). Eén student benadrukt de structurele druk in deze relatie: *“Je hebt geen andere keus... als je je woonplaats niet opgeeft, krijg je gewoon die uitwonende beurs niet”* (HBO 5).

4.4. Institutioneel vertrouwen

Vier van de zes WO-studenten (WO 2, 3, 4 en 6) vertrouwen de overheid met hun gegevens. WO 2 vreest vooral externe hacks. WO 4 toont lichte twijfel, WO 6 maakt zich weinig zorgen over datalekken. WO 3 koppelt zijn vertrouwen aan de relatief goede digitale infrastructuur in Nederland vergeleken met België: *“Wij doen het in Nederland gewoon goed met digitalisering. Mijn vriendin woont in België, het is een grote chaos daar... Wij zijn denk ik veel verder dan wij denken met digitalisering.”*

Twee studenten (WO 5 en WO 6) bespreken expliciet de impact van schandalen. WO 5 werd sceptischer door de Toeslagenaffaire vanwege de rol van vooringenomen algoritmes. WO 6 zegt dat het zijn vertrouwen niet beïnvloedde omdat hij toen nog in België woonde. Ook WO 3 voelde zich niet geraakt: *“Nee, persoonlijk niet. Misschien omdat het ook ver weg van mij gebeurt – heel egoïstisch gezegd, maar ja. Het raakt mij gewoon niet en alles wat ik digitaal met de overheid moet doen gaat goed.”*

Vier van de zes HBO-studenten (HBO 1, 3, 4 en 5) geven aan dat zij de overheid in algemene zin vertrouwen met hun persoonlijke gegevens. Dit vertrouwen wordt meestal niet expliciet onderbouwd, maar eerder verondersteld op basis van eerdere ervaringen of het

ontbreken van incidenten. *“Ik vind het allemaal prima... ik heb nog nooit meegemaakt dat ik ergens door m'n vertrouwen verloren ben”* (HBO 1). HBO 4 zegt: *“Ik heb nooit problemen gehad, dus het is niet alsof ze mijn vertrouwen hebben geschonden.”*

Twee studenten (HBO 2 en 6) uiten expliciet wantrouwen, vooral uit zorgen over datamisbruik en verborgen doeleinden. HBO 2 vermoedt dat onnodige gegevens worden opgevraagd voor andere doelen. HBO 6 denkt dat de overheid profielen opstelt die mogelijk verkocht worden aan bedrijven, bijvoorbeeld voor reclamedoelstellingen.

Bij drie studenten (HBO 2, 3 en 6) beïnvloeden schandalen als de Toeslagenaffaire hun houding. HBO 2 noemt het *“echt schandalig... pas laat is het opgelost”*, HBO 6 concludeert na uitleg: *“Dat is best wel heftig... dan wordt er eigenlijk etnisch geprofileerd.”* Anderen geven aan niet geraakt te zijn: *“Voor mij is het niet heel erg belangrijk”* (HBO 4).

Beide mbo-studenten ervaren weinig institutionele afhankelijkheid van digitale overheidsdiensten. MBO 1 zegt zich *“niet echt afhankelijk”* te voelen en gebruikt digitale diensten alleen wanneer het strikt noodzakelijk is, zoals bij het aanvragen van een ID. Ook MBO 2 geeft aan weinig gebruik te maken van digitale overheidsplatformen sinds de start van de opleiding. Hoewel beide studenten digitale diensten functioneel waarderen, beschouwen zij hun relatie met de digitale overheid niet als structureel of dwingend.

4.5. Privacy calculus

WO-studenten maken doorgaans een pragmatische afweging tussen voordelen en risico's van datadeling met de overheid. Vijf van de zes noemen dat ze bewust gegevens delen wanneer dit nodig is voor toegang tot diensten. WO 1 zegt: *“Als ik iets nodig heb van de overheid zoals belasting aangeven dan moet ik wel mijn data delen... anders niet zo snel.”* WO 4 deelt sneller omdat het diensten toegankelijker maakt. WO 3 wijst op efficiëntie, zolang het geen *“hele privé dingen”* betreft zoals relaties of inkomen. Tegelijkertijd is er ook een terughoudende stem. WO 5 wil *“liever zo weinig mogelijk [data] delen”* vanwege gebrek aan inzicht in datagebruik en stelt: *“Ik ben wel van mening voor zoveel mogelijk privacy, dat ieder persoon voor zichzelf kan beslissen. En dat wordt moeilijk als alles van iedereen geweten is.”*

HBO-studenten beschrijven hun datadelingsgedrag overwegend in functionele termen,

waarbij toegang tot diensten centraal staat. Vier van de zes studenten (HBO 1, 2, 3 en 5) geven aan dat ze hun gegevens delen wanneer dit nodig is om toegang te krijgen tot een dienst of voorziening. Zoals HBO 1 zegt: *“Als ik zelf iets nodig heb van de overheid zoals belasting aangeven dan moet ik wel mijn data delen”*. HBO 2 benadrukt de wederkerigheid van de relatie: *“Je geeft ze dan maar je data, want ja, ik heb dat geld ook nodig”*.

Voor sommige studenten speelt gemak een grote rol. HBO 3 zegt: *“Ik doe het liever vanuit thuis... het verloopt soepel”*, HBO 5 deelt sneller data *“ook al is dat misschien kwetsbaar”*, en HBO 6 denkt er *“niet altijd bij na”*. Studenten delen meestal alleen strikt noodzakelijke informatie: *“Als ze m'n telefoonnummer niet nodig hebben, geef ik dat ook niet”* (HBO 5).

Beide mbo-studenten maken een pragmatische afweging bij het delen van persoonlijke gegevens met de overheid. MBO 1 zegt alleen het minimale te willen delen en noemt het verplicht aanleveren van data in ruil voor overheidsdiensten een *“lichte vorm van omkoperij”*. Daarbij wordt nauwelijks nagedacht over de gevolgen van datadeling. MBO 2 is bereid om gegevens te verstrekken wanneer dit nodig is voor het ontvangen van diensten, zoals toeslagen, en begrijpt dat extra informatie soms nodig is om misbruik te voorkomen. In beide gevallen blijft de privacy calculus impliciet en wordt deze voornamelijk gestuurd door noodzakelijkheid en gemak.

5. Analyse

In dit hoofdstuk worden de vijf hypothesen uit het conceptueel model getoetst aan de hand van de kwalitatieve interviewdata. Het model stelt dat de bereidheid van studenten om persoonlijke gegevens te delen met de overheid wordt beïnvloed door individuele kenmerken, structurele afhankelijkheid van overheidsdiensten en het institutioneel vertrouwen in de overheid. Deze factoren beïnvloeden hoe studenten de privacy calculus afwegen.

De analyse is gestructureerd per hypothese. Telkens wordt besproken in hoeverre de empirische bevindingen de verwachting ondersteunen, nuanceren of tegenspreken. Daarbij wordt ook gekeken naar verschillen tussen HBO- en WO-studenten en naar onderlinge samenhangen tussen de variabelen. De hypothesetoetsing dient zowel om het model te onderbouwen als om inzicht te bieden in de drijfveren achter datagedrag binnen een context van toenemende digitalisering van overheidsdiensten.

H1: Hoe hoger het institutioneel vertrouwen, hoe groter de bereidheid van studenten om persoonlijke gegevens te delen met de overheid.

De interviews ondersteunen deze hypothese grotendeels. Studenten die vertrouwen uitspreken in de overheid – zoals WO 2, 4 en 6, HBO 1, 3, 4 en 5, en MBO 1 en 2 – geven aan zonder veel terughoudendheid data te delen. Ze gaan ervan uit dat de overheid zorgvuldig en integer met gegevens omgaat, wat hun bereidheid versterkt. Het verband is echter niet in alle gevallen consistent. Sommige studenten met weinig vertrouwen – zoals HBO 2 en 6 of WO 5 – blijken alsnog gegevens te delen, vaak uit noodzaak. In zulke gevallen is er sprake van structurele afhankelijkheid: toegang tot diensten zoals DUO vereist datadeling, ongeacht het vertrouwen. Meerdere studenten benadrukken dat er in de praktijk weinig keuzevrijheid bestaat. Ook komt naar voren dat schandalen zoals de Toeslagenaffaire niet altijd invloed hebben op het gedrag, tenzij studenten zich er persoonlijk door geraakt voelen (bijv. WO 3, HBO 1). Dit wijst op het belang van nabijheid en betrokkenheid in de perceptie van risico's. De bevindingen sluiten aan bij het model van Mayer et al. (2007), waarin vertrouwen rust op bekwaamheid, integriteit en welwillendheid. Tegelijk bevestigen ze het belang van contextuele factoren zoals

afhankelijkheid, zoals beschreven door Alzahrani et al. (2017).

De hypothese wordt grotendeels bevestigd. Een hoger institutioneel vertrouwen gaat samen met een grotere bereidheid tot datadeling, al kan deze relatie in specifieke situaties worden overstemd door structurele afhankelijkheid of lage persoonlijke betrokkenheid bij vertrouwensschendingen.

H2: Hoe positiever de uitkomst van de privacy calculus, hoe groter de bereidheid van studenten om persoonlijke gegevens te delen met de overheid.

De bevindingen ondersteunen deze hypothese in brede zin. Zowel WO- als HBO-studenten geven aan dat zij bereid zijn data te delen wanneer daar concrete voordelen tegenover staan, zoals toegang tot studiefinanciering of administratief gemak (bijv. WO 1, 3; HBO 2, 5; MBO 2). In deze gevallen overheersen functionele overwegingen, waarbij risico's veelal als secundair worden beschouwd.

Er zijn aanwijzingen dat deze afweging niet altijd bewust of rationeel plaatsvindt. Verschillende respondenten (bijv. HBO 6, WO 6) geven aan nauwelijks stil te staan bij de implicaties van hun datagedrag, wat suggereert dat de privacy calculus vaak impliciet blijft. Dit komt overeen met inzichten van Acquisti et al. (2016), die benadrukken dat context en intuïtie een belangrijke rol spelen in privacybeslissingen. Tegelijkertijd zijn er studenten die expliciet negatief oordelen over datadeling en terughoudend handelen (bijv. WO 5, HBO 2). In deze gevallen blijken privacyzorgen en wantrouwen de calculus te domineren, wat leidt tot minder bereidheid tot informatieverstrekking.

De analyse bevestigt daarmee de centrale veronderstelling van de privacy calculus-theorie: studenten maken, al dan niet altijd expliciet, een afweging tussen baten en risico's. De data wijzen echter ook op de beperkte rationaliteit van dit proces, en de invloed van afhankelijkheid en gewoonte op het uiteindelijke gedrag.

H3: Studenten met hogere digitale vaardigheden ervaren een positievere privacy calculus dan studenten met lagere digitale vaardigheden.

De resultaten wijzen op gedeeltelijke ondersteuning van deze hypothese. WO-studenten beoordelen hun digitale vaardigheden doorgaans hoger dan HBO-studenten en tonen meer bewustzijn van dataprocessen. Sommige WO-studenten gebruiken geavanceerde tools zoals VPN's of wachtwoordmanagers en geven blijk van kritisch bewustzijn over wat digitale overheidssystemen met hun gegevens doen. Dit wijst op een verband tussen hogere vaardigheden en meer doordachte afwegingen.

Tegelijkertijd blijkt dat digitale vaardigheid niet automatisch leidt tot een positievere privacy calculus. Ook WO-studenten geven aan regelmatig te handelen uit gemak of routine, zonder altijd stil te staan bij de risico's. Bovendien geldt dat een hoger vaardigheidsniveau niet noodzakelijk leidt tot minder zorgen over privacy: sommige vaardige studenten zijn juist kritischer en terughoudender. Lagere ingeschatte vaardigheid lijkt ook niet te correleren met een negatieve privacy calculus. MBO 2 schatte zichzelf in als een 3 maar heeft toch veel vertrouwen in de overheid en ervaart een positieve privacy calculus. Deze conclusie is echter getrokken uit een enkele respondent, en is dus niet generaliseerbaar naar de bredere (MBO-)populatie zonder aanvullend onderzoek.

Bij HBO-studenten zijn de digitale vaardigheden gemiddeld lager. Zij tonen vaker functionele benadering van digitale diensten: voldoende voor basale interactie, maar met beperkte kennis over gegevensverwerking. Toch zijn ook binnen deze groep studenten te vinden die weinig risico ervaren en zonder veel bezwaren data delen. Dit duidt erop dat digitale vaardigheid weliswaar invloed heeft op bewustzijn, maar slechts in beperkte mate op de uiteindelijke afweging. De hypothese wordt maar beperkt ondersteund. Digitale vaardigheden lijken samen te hangen met groter bewustzijn, maar hebben geen eenduidige invloed op hoe studenten de baten en risico's van datadeling waarderen.

H4: Studenten met een sterk privacybewustzijn ervaren een negatievere privacy calculus dan studenten met een laag bewustzijn.

De data geven gedeeltelijke ondersteuning aan deze hypothese. Studenten die aangeven privacy belangrijk te vinden (zoals WO 2, 4 en 5 en HBO 2 en 5) benoemen regelmatig zorgen over datamisbruik, onduidelijke doeleinden of gebrekkige controle over hun gegevens. In sommige gevallen vertaalt dit zich in terughoudendheid om data te delen, wat duidt op een negatievere privacy calculus. Vooral WO 5 en HBO 2 geven expliciet aan dat zij liever zo min mogelijk delen, mede vanuit principiële of veiligheidsgerelateerde motieven.

Toch blijkt in de praktijk dat er vaak een kloof bestaat tussen houding en gedrag. Veel studenten met een hoog privacybewustzijn nemen nauwelijks structurele maatregelen, of geven toe uit gemak alsnog gegevens te verstrekken. Daarnaast zijn er studenten met een relatief laag bewustzijn (zoals HBO 1 en 4; MBO 2) die wel data delen, maar zelden over nadenken. Voor hen lijkt er eerder sprake van afwezigheid van een duidelijke afweging dan van een positieve calculus.

Bovendien is het bewustzijn vaak oppervlakkig of fragmentarisch. Studenten erkennen privacy als belangrijk, maar missen inzicht in hoe dataverwerking precies werkt. Dit sluit aan bij eerder onderzoek waarin gesteld wordt dat privacyattitudes niet automatisch leiden tot privacybeschermend gedrag. De hypothese wordt dus deels bevestigd. Sterker privacybewustzijn gaat soms gepaard met terughoudendheid, maar leidt lang niet altijd tot een negatievere privacy calculus vanwege inconsistente gedragsvertaling.

H5: Studenten die afhankelijker zijn van overheidsdiensten ervaren een positievere privacy calculus dan studenten met minder afhankelijkheid.

De bevindingen ondersteunen deze hypothese in duidelijke mate. Vrijwel alle studenten geven aan afhankelijk te zijn van digitale overheidsdiensten, met name voor zaken als studiefinanciering, belastingaangifte en identiteitsverificatie via DigiD. Zowel WO- als HBO-studenten erkennen dat zij zonder deze diensten belangrijke voorzieningen zouden mislopen, wat hun bereidheid om persoonlijke gegevens te delen vergroot.

Respondenten koppelen hun afhankelijkheidsgevoel regelmatig aan hun houding ten opzichte van datadeling. Studenten zoals WO 4 en HBO 2 en 5 geven expliciet aan dat hun bereidheid om data te delen toeneemt vanwege het gemak en de noodzaak van digitale diensten. De voordelen wegen in deze gevallen zwaarder dan eventuele zorgen over privacy. Voor deze studenten leidt afhankelijkheid tot een pragmatische, en dus positievere, privacy calculus.

Tegelijkertijd wordt de afhankelijkheidsrelatie soms als problematisch ervaren. Enkele studenten benoemen dat zij weinig keus hebben: het niet delen van gegevens betekent uitsluiting van noodzakelijke voorzieningen. Hoewel dit hun privacy calculus positiever maakt in termen van uitkomst (namelijk: delen), roept het wel vragen op over de vrijwilligheid van hun keuze. Dit wijst op een spanningsveld tussen geïnformeerde toestemming en structurele noodzaak. Bij de mbo-studenten wordt hypothese 5 echter niet ondersteund: ondanks lage afhankelijkheid varieert de privacy calculus van kritisch (MBO 1) tot positief (MBO 2). Deze resultaten worden mogelijk beïnvloed door de lage hoeveelheid MBO-respondenten.

6. Conclusie en discussie

In dit hoofdstuk wordt de onderzoeksvraag beantwoord, gevolgd door een reflectie op de keuzes die gemaakt zijn om dit onderzoek uit te voeren en aanbevelingen voor vervolgonderzoek.

6.1. Beantwoording van de onderzoeksvraag

Deze scriptie onderzocht de vraag: *Wat beïnvloedt de bereidheid van studenten om hun persoonlijke gegevens te delen met de overheid voor gepersonaliseerde diensten?* Uit de kwalitatieve interviews blijkt dat deze bereidheid wordt gevormd door een complex samenspel van vertrouwen in de overheid, ervaren afhankelijkheid van digitale diensten en de persoonlijke afweging van baten en risico's.

Hoewel veel studenten zeggen bereid te zijn hun gegevens te delen, blijkt dat deze beslissing zelden voortkomt uit een expliciete of rationele afweging. De privacy calculus is vaak impliciet en pragmatisch: gemak, gewoonte en het ontbreken van alternatieven spelen een dominante rol. Studenten delen gegevens voornamelijk wanneer dit functioneel noodzakelijk is, zoals voor studiefinanciering of belastingzaken. Dit wijst op een conditionele bereidheid die eerder gestuurd wordt door context dan door overtuiging.

Institutioneel vertrouwen blijkt in veel gevallen een versterkende factor: studenten die de overheid als integer en competent beschouwen, delen hun gegevens met meer vertrouwen. Toch is dit vertrouwen geen noodzakelijke voorwaarde: ook studenten met wantrouwen geven aan toch data te delen, uit gevoel van verplichting of afhankelijkheid. Dit laat zien dat het delen van gegevens in de context van digitale overheidsdiensten zelden een autonome keuze is, maar vaak plaatsvindt binnen asymmetrische machtsverhoudingen.

Daarnaast blijkt dat digitale vaardigheden en privacybewustzijn niet eenduidig samenhangen met datagedrag. Studenten die zichzelf als digitaal vaardig of privacybewust beschouwen, handelen lang niet altijd consequent naar deze overtuigingen. Hierin wordt zichtbaar dat attitudes zich niet altijd vertalen naar gedrag.

Kortom, de bereidheid tot datadeling onder studenten wordt slechts ten dele verklaard door klassieke theorieën zoals de Privacy Calculus of modellen van vertrouwen. In de praktijk

overheersen pragmatiek, afhankelijkheid en routinematig gedrag, waarmee de vermeende autonomie van studenten voor digitale overheidsdiensten ter discussie komt te staan.

6.2. Discussie

De bevindingen van dit onderzoek bevestigen en nuanceren bestaande theoretische inzichten over datadeling, vertrouwen en privacy in het digitale domein. De Privacy Calculus Theory (Laufer & Wolfe, 1977) blijkt slechts gedeeltelijk toepasbaar. Studenten geven weliswaar voordelen en risico's aan, maar maken zelden een expliciete kosten-batenanalyse. Veel keuzes zijn pragmatisch, routinematig of contextgedreven, wat aansluit bij de kritiek van Acquisti et al. (2016) op het rationele model van privacybeslissingen.

Het model van institutioneel vertrouwen (Mayer et al., 2007) biedt daarentegen meer directe verklaringskracht. Studenten die de overheid als bekwaam en welwillend ervaren, delen hun gegevens sneller. Tegelijk laat dit onderzoek zien dat ook studenten met weinig vertrouwen bereid zijn tot datadeling, vooral uit structurele afhankelijkheid. Deze bevinding bevestigt de zienswijze van Six en Latusek (2023), die wantrouwen omschrijven als een actief proces dat niet altijd tot weigering leidt, maar ook tot berusting of strategisch gedrag.

De resultaten tonen verder dat digitale vaardigheden en privacybewustzijn niet eenduidig doorwerken in gedrag. Studenten die zichzelf vaardig of bewust noemen, blijken vaak alsnog nonchalant met data om te gaan. Dit nuanceert eerdere bevindingen van Srivastava en Teo (2009), en Carter en Bélanger (2005), en sluit aan bij Smaling (2017) en ECDL (2015), die waarschuwen voor een overschatting van digitale geletterdheid bij jongeren.

Een kracht van dit onderzoek is de diepgang die ontstaat door kwalitatieve interviews, waardoor betekenisgeving, motieven en context zichtbaar worden. Door thematische analyse zijn onderliggende patronen geïdentificeerd, ook wanneer respondenten zich niet expliciet bewust waren van hun gedrag. Ook heeft de uiteenzetting tussen privacy calculus en institutioneel vertrouwen een waardevolle theoretische meerwaarde geleverd aan het onderzoek. Hoewel de combinatie van privacy calculus en institutioneel vertrouwen uiteindelijk onvoldoende bleek om alle patronen te verklaren, bood deze benadering wel inzicht in de gelaagdheid van studentenmotieven en -afhankelijkheden.

Een beperking is echter de beperkte generaliseerbaarheid: het onderzoek is kleinschalig, beperkt tot WO-, HBO-, en een paar MBO studenten, en mogelijk beïnvloed door sociale wenselijkheid. Daarnaast maakt het gebruik van zelfrapportage het moeilijk om te bepalen in hoeverre attitude en gedrag daadwerkelijk overeenkomen. Tot slot vormt de beperking tot de Randstad een obstakel voor de brede verklarende kracht van het onderzoek.

Deze studie levert een inhoudelijke bijdrage aan de literatuur over digitale overheidsdiensten door te laten zien dat de bereidheid van studenten om persoonlijke gegevens te delen met de overheid niet louter het resultaat is van een rationele kosten-batenanalyse, maar het product van een complex samenspel van vertrouwen, afhankelijkheid, gemak en gewoonte. Waar veel bestaand onderzoek focust op technologische acceptatie of privacyzorgen in abstracte termen, laat dit onderzoek juist zien hoe jongeren in de praktijk omgaan met digitale overheidsrelaties: vaak pragmatisch, soms kritisch, maar zelden volledig geïnformeerd. Door privacy calculus en institutioneel vertrouwen te combineren in één analytisch kader, en deze te toetsen aan kwalitatieve data, biedt de studie niet alleen een theoretische verdieping, maar ook een realistischer (zij het gelimiteerd) beeld van hoe datagedrag tot stand komt in het dagelijks leven van studenten. Hiermee geeft het onderzoek handen en voeten aan abstracte theorievorming binnen de e-governance literatuur.

6.3. Aanbevelingen voor toekomstig onderzoek en beleid

De uitkomsten van dit onderzoek wijzen op verschillende richtingen voor toekomstig onderzoek naar datadeling in het publieke domein. Allereerst verdient de relatie tussen structurele afhankelijkheid en datagedrag meer systematische aandacht. Hoewel in de literatuur vaak wordt uitgegaan van autonome, rationele burgers (Laufer & Wolfe, 1977; Mayer et al., 2007), suggereren deze bevindingen dat ervaren afhankelijkheid van digitale diensten een bepalende – en mogelijk dwingende – factor is. Vervolgonderzoek kan dit verder uitdiepen door institutionele context en machtsverhoudingen explicieter mee te nemen.

Daarnaast zou kwantitatief of experimenteel onderzoek kunnen bijdragen aan meer generaliseerbare uitspraken over verbanden tussen vertrouwen, afhankelijkheid en gedrag. Denk daarbij aan surveys onder grotere en meer diverse populaties (inclusief grotere hoeveelheden

MBO-studenten en mogelijk ook werkenden), of een ‘vignettenonderzoek’ waarin verschillende scenario’s van dataverzameling worden voorgelegd en reacties worden gemeten.

Ook verdient de attitude-gedragskloof nadere verkenning. Verschillende studenten zeggen privacy belangrijk te vinden, maar handelen daar niet naar. Toekomstig onderzoek zou gebruik kunnen maken van gedragsdata of logbestanden, om het verschil tussen zelfrapportage en daadwerkelijk digitaal gedrag inzichtelijk te maken.

Ten slotte is meer inzicht nodig in de rol van intuïtieve besluitvorming in digitale interacties met de overheid. Beslissingen worden zelden rationeel genomen; veel studenten handelen op basis van gewoonte, tijdsdruk of gemak. Het betrekken van gedragswetenschappelijke inzichten, zoals uit de nudge- of heuristiek-literatuur, kan bestaande bestuurskundige modellen verrijken.

Naast richtingen voor vervolgonderzoek volgen ook enkele aanbevelingen voor beleid. Gezien de impliciete aard van de privacy calculus en de ervaren afhankelijkheid van digitale overheidsdiensten, is het wenselijk dat overheidsinstanties zoals DUO en gemeenten meer transparantie bieden over datagebruik. Een concreet instrument hiervoor is het ontwikkelen van een gepersonaliseerd datadashboard waarin zichtbaar is welke gegevens verzameld worden, met welk doel en op welke momenten.

Daarnaast dienen overheidsportalen explicieter te communiceren welke gegevensverzameling verplicht is en welke optioneel. Hiermee wordt de vrijwilligheid van datadeling versterkt. Ten slotte zou digitale geletterdheid integraal onderdeel moeten worden van voorlichtingsmomenten rondom studiefinanciering of DigiD, gericht op het vergroten van inzicht in rechten en risico’s. Deze aanbevelingen beogen niet alleen het vertrouwen van studenten te versterken, maar ook hun handelingsbekwaamheid te vergroten in een steeds complexer digitaal overheidslandschap. Een digitale overheid die studenten echt serieus neemt, begint niet bij technologie, maar bij vertrouwen, keuzevrijheid en transparantie over data.

7. Literatuurlijst

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54(2), 442-492. <https://doi.org/10.1257/jel.54.2.442>
- Alarabiat, A., Soares, D., & Estevez, E. (2017). *Predicting Citizens Acceptance of Government-led e-Participation Initiatives through Social Media: A Theoretical Model*. <https://doi.org/10.24251/HICSS.2017.345>
- Al-Omairi, L., Al-Samarraie, H., Alzahrani, A. I., & Alalwan, N. (2020). Students' intention to adopt e-government learning services: A developing country perspective. *Library Hi Tech*, 39(1), 308-334. <https://doi.org/10.1108/LHT-02-2020-0034>
- Alzahrani, L., Al-Karaghoul, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review*, 26(1), 164-175. <https://doi.org/10.1016/j.ibusrev.2016.06.004>
- Bannister, F., & Connolly, R. (2011). The Trouble with Transparency: A Critical Review of Openness in e-Government. *Policy & Internet*, 3(1), 1-30. <https://doi.org/10.2202/1944-2866.1076>
- Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), 165-176. <https://doi.org/10.1016/j.jsis.2007.12.002>
- Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, 15(1), 5-25. <https://doi.org/10.1111/j.1365-2575.2005.00183.x>

- Colesca, S. E. (2009). Increasing E-trust: A Solution To Minimize Risk In E-Government Adoption. *Journal of Applied Quantitative Methods*, 4(1), 31-44.
- Dedding, C., & Goedhart, N. (2021). Uit beeld geraakt—Digitale ongelijkheid als maatschappelijke opgave. *Rijksoverheid*.
<https://www.rijksoverheid.nl/documenten/rapporten/2021/12/21/uit-beeld-geraakt---digitale-ongelijkheid-als-maatschappelijke-opgave>
- DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*, 19(4), 9-30.
- Digitale gelijkheid begint op school*. (2020, december 17). Kennisnet.
<https://www.kennisnet.nl/opinie/digitale-gelijkheid-begint-op-school/>
- Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2005). New Public Management Is Dead—Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*, 16(3), 467-494. <https://doi.org/10.1093/jopart/mui057>
- Fraudeaanpak DUO discriminerend en illegaal*. (2024, november 11). Autoriteit Persoonsgegevens.
<https://www.autoriteitpersoonsgegevens.nl/actueel/fraudeaanpak-duo-discriminerend-en-illegaal>
- Fraudebestrijding door DUO*. (2024, maart 21). [Text]. Tweede Kamer.
https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/fraudebestrijding-door-duo
- Kanne, P., & Driessen, M. (2021a, maart 5). *Vooraf Toeslagenaffaire schaadt vertrouwen in overheid*. Ipsos I&O Publiek.

<https://www.ipsos-publiek.nl/actueel/vooral-toeslagenaffaire-schaadt-vertrouwen-in-overheid/>

Kanne, P., & Driessen, M. (2021b, maart 5). Vooral Toeslagenaffaire schaadt vertrouwen in overheid. *Ipsos I&O Publiek*.

<https://www.ipsos-publiek.nl/actueel/vooral-toeslagenaffaire-schaadt-vertrouwen-in-overheid/>

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, 33(3), 22-42.

<https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>

Li, Y., & Shang, H. (2023). How does e-government use affect citizens' trust in government? Empirical evidence from China. *Information & Management*, 60(7), 103844. <https://doi.org/10.1016/j.im.2023.103844>

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, 371(1987), 1-17.

Mayer, R. C., Schoorman, F. D., & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *The Academy of Management Review*, 32(2), 344-354.

Meier, Y., & Krämer, N. C. (2024). The Privacy Calculus Revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels. *Communication Research*, 51(2), 178-202. <https://doi.org/10.1177/00936502221102101>

Meijer, A., & Bekkers, V. (2015). A metatheory of e-government: Creating some order in a fragmented research field. *Government Information Quarterly*, 32(3), 237-245.

<https://doi.org/10.1016/j.giq.2015.04.006>

Méndez-Rivera, C. A., Patiño-Toro, O. N., Valencia-Arias, A., & Arango-Botero, D. M.

(2023). Factors Influencing the Adoption of E-Government Services: A Study among University Students. *Economies*, 11(9), Article 9.

<https://doi.org/10.3390/economies11090225>

Mensah, I. K. (2019). Factors Influencing the Intention of University Students to Adopt and Use E-Government Services: An Empirical Evidence in China. *SAGE Open*, 9(2),

2158244019855823. <https://doi.org/10.1177/2158244019855823>

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385.

<https://doi.org/10.1016/j.giq.2019.06.002>

Merien. (2025, februari 13). *Trump heeft vrij spel over Nederlandse overheidsdata*. IO+.

<https://iopius.nl/nl/posts/trump-heeft-vrij-spel-over-nederlandse-overheidsdata>

Nederland te afhankelijk van Amerikaanse clouddiensten. (2025, maart 15). BNNVARA.

<https://www.bnnvara.nl/kassa/artikelen/nederland-te-afhankelijk-van-amerikaanse-clouddiensten>

Nederlandse digitale overheid wederom van Europees topniveau. (2023, november 7).

Consultancy.

<https://www.consultancy.nl/nieuws/49360/nederlandse-digitale-overheid-wederom-van-europees-topniveau>

- Nikiforova, A., Clarinval, A., Zuiderwijk, A., Rudmark, D., Milic, P., & Rajamäe-Soosaar, K. (2024). *Innovation Resistance Theory in Action: Unveiling Barriers to Open Government Data Adoption by Public Organizations to Unlock Open Data Innovation* (No. arXiv:2407.10883). arXiv. <https://doi.org/10.48550/arXiv.2407.10883>
- OECD. (2007). *OECD e-Government Studies: Netherlands 2007*. OECD. <https://doi.org/10.1787/9789264030299-en>
- OECD. (2016). *Digital Government Strategies for Transforming Public Services in the Welfare Areas*. OECD. <https://doi.org/10.1787/0d2eff45-en>
- Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, 31, 76-82. <https://doi.org/10.1016/j.copsyc.2019.08.009>
- Prensky, M. (2001). Digital Natives, Digital Immigrants. *MCB University Press*, 9(5), 1-6. <https://doi.org/10.1108/10748120110424816>
- Safeguarding Individuals' Digital Rights*. (2023). European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2023_en
- Sigmund, T., & Korčák, J. (2021). *Altruism Extension of the Privacy Calculus* (J. Maci, P. Maresova, K. Firlej, & I. Soukal, Red.; pp. 680-686). <https://doi.org/10.36689/uhk/hed/2021-01-067>
- Six, F. E., & Latusek, D. (2023). Distrust: A critical review exploring a universal distrust sequence. *Journal of Trust Research*, 13(1), 1-23. <https://doi.org/10.1080/21515581.2023.2184376>

Smaling, E. (2017, februari 16). *Studenten hechten aan hun privacy, tot het onhandig wordt*. Erasmus Magazine.

<https://www.erasmusmagazine.nl/2017/02/16/studenten-online-privacy-enquete/>

Srivastava, S. C., & Teo, T. S. H. (2009). Citizen Trust Development for E-Government Adoption and Usage: Insights from Young Adults in Singapore. *Communications of the Association for Information Systems*, 25. <https://doi.org/10.17705/1CAIS.02531>

Talwar, S., Talwar, M., Kaur, P., & Dhir, A. (2020). Consumers' Resistance to Digital Innovations: A Systematic Review and Framework Development. *Australasian Marketing Journal*, 28(4), 286-299. <https://doi.org/10.1016/j.ausmj.2020.06.014>

Teo, T. S. H., Srivastava, S. C., & Jiang, L. (2008). Trust and Electronic Government Success: An Empirical Study. *Journal of Management Information Systems*, 25(3), 99-131.

The Fallacy of the 'Digital Native': Why Young People Need to Develop Their Digital Skills. (2015). European Computer Driving License Foundation.

<https://ec.europa.eu/futurium/en/content/ecdl-foundation-fallacy-digital-native-why-young-people-need-develop-their-digital-skills.html>

van Harreveld, M. (2025, maart 13). *Kamer pauzeert dataopslag Nederlandse overheid in Amerikaanse cloud*. bnr.nl.

<https://www.bnr.nl/nieuws/tech-innovatie/10569204/kamer-pauzeert-dataopslag-nederlandse-overheid-in-amerikaanse-cloud>

van Helden, W. J., Govers, E. J. E., Maltzahn, G. L. B., Vegter, B. J., & Beer, S. (2013). *De burger gaat digitaal*. De Nationale Ombudsman.

<https://www.kennisopenbaarbestuur.nl/documenten/2013/12/09/de-burger-gaat-digitaal>

- Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 33(3), 472-480. <https://doi.org/10.1016/j.giq.2016.06.004>
- Wang, H., & Lo, J. (2013). Determinants of citizens' intent to use government websites in Taiwan. *Information Development*, 29(2), 123-137.
<https://doi.org/10.1177/0266666912453835>
- Wang, T., & Lu, Y. (2010). Determinants of Trust in E-Government. *Institute of Electrical and Electronics Engineers, 2010 International Conference on Computational Intelligence and Software Engineering, Wuhan, China, 2010*, 1-4.
<https://doi.org/10.1109/CISE.2010.5676832>
- Warkentin, M., Gefen, D., Pavlou, P., & Rose, G. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets*, 12, 157-162.
<https://doi.org/10.1080/101967802320245929>
- Welch, E. W., Hinnant, C. C., & Moon, M. J. (2004). Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory*, 15(3), 371-391. <https://doi.org/10.1093/jopart/mui021>
- Yang, K., & Miller, G. (Red.). (2008). *Handbook of research methods in public administration* (2nd ed). CRC Press.

8. Appendix

Figuur 3

Brede procedure voor de semi-gestructureerde interviews

Algemene achtergrond

- Wat studeert u momenteel?
- Hoe vaak maakt u gebruik van digitale overheidsplatformen (zoals MijnDUO, DigiD, Studielink)?
- Hoe digitaal vaardig voelt u zichzelf? Geef uzelf een cijfer tussen 1-10.

Privacybewustzijn en attitude

- Vindt u het belangrijk om uw online privacy te beschermen? Waarom wel/niet?
- Welke maatregelen neemt u zelf om uw gegevens te beschermen?
- Hoe kijkt u aan tegen dataverzameling door de overheid in het algemeen?

Institutioneel vertrouwen

- In hoeverre vertrouwt u de overheid met uw persoonlijke gegevens?
- Zijn er specifieke overheidsdiensten die u wel of juist niet vertrouwt?
- Heeft u ervaringen gehad met overheidsdiensten die uw vertrouwen versterkten of verzwakten?
- (Indien niet benoemd in antwoord): Heeft de toeslagenaffaire of het DUO-schandaal dan geen impact gehad op uw vertrouwen?

Privacy calculus (afweging kosten en baten)

- Denkt u na over de gevolgen van het delen van uw persoonlijke data met de overheid?
- Kunt u beschrijven wanneer u bereid bent wél gegevens te delen? En wanneer niet?
- Welke voordelen ziet u in gepersonaliseerde overheidsdiensten? En welke risico's?

Afhankelijkheid en gebruik van diensten

- In hoeverre voelt u zich afhankelijk van digitale overheidsdiensten (zoals DUO)?
- Zou u die diensten blijven gebruiken als u er minder op aangewezen was?
- Is dat afhankelijkheidsgevoel van invloed op uw bereidheid om data te delen?

Afsluiting

- Heeft u suggesties voor hoe de overheid beter om zou kunnen gaan met uw persoonlijke data?
- Is er iets wat u verder kwijt wilt over dit onderwerp?

Figuur 4*Codeerschema met concepten, definities, indicatoren en bronnen*

Concept	Definitie	Interviewvragen	Bron(nen)
Institutioneel vertrouwen	Verwachting dat de overheid bekwaam, integer en welwillend handelt	Vertrouwen in overheid; ervaringen met DUO/DigiD	Mayer et al. (2007); Alzahrani et al. (2017)
Privacy Calculus	Afweging tussen waargenomen voordelen en risico's van datadeling	Wanneer data delen? Voordelen? Risico's?	Laufer & Wolfe (1977); Acquisti et al. (2016); Meier & Krämer (2024)
Privacybewustzijn	Mate van bewustzijn en zorg over online gegevens	Belang privacy; zelfbescherming t.o.v. dataverzameling	Van Zoonen (2016); Sigmund & Korčák (2021)
Afhankelijkheid	Gevoel van noodzakelijkheid bij gebruik van digitale overheidsdiensten	Afhankelijkheid van DUO/DigiD; alternatieven; invloed op bereidheid tot datadelen	Smaling (2017); Merien (2025); van Harreveld (2025)
Digitale vaardigheden	Zelfinschatting van competentie in omgaan met digitale overheidsdiensten	Gebruik overheidsplatforms; digitale zelfredzaamheid	Srivastava & Teo (2009); Carter & Belanger (2005)