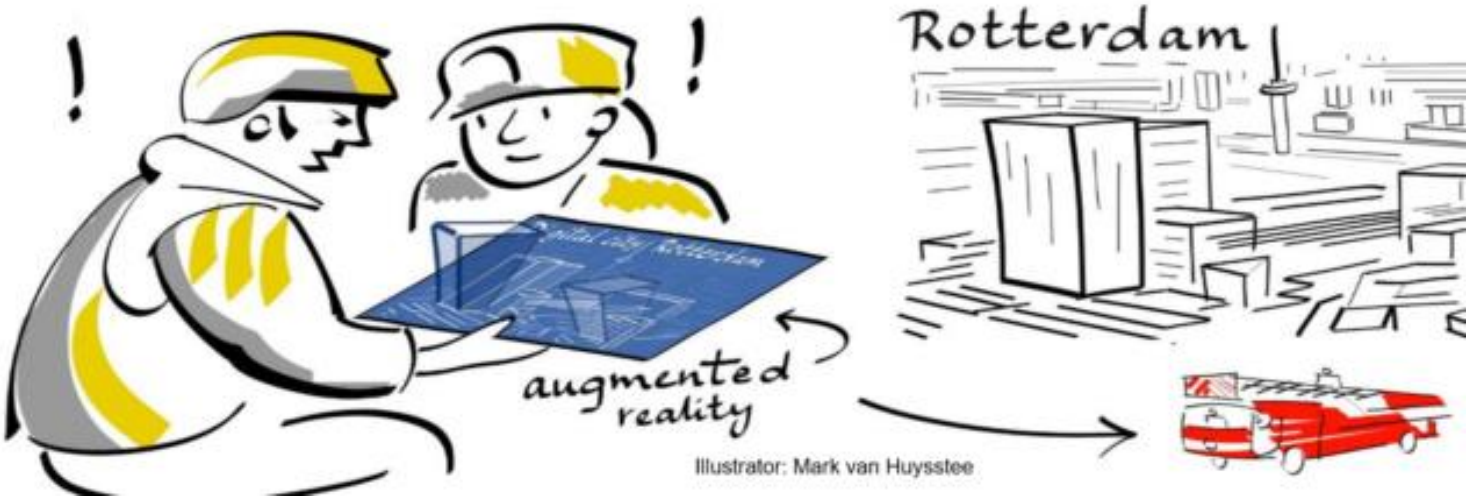
Data delen in noodsituaties: wat vinden we daarvan?

Een kwantitatief onderzoek naar de houding van burgers tegenover het delen van data in verschillende noodsituaties



Master Thesis

Sabien Dekkers (584628)
Erasmus Universiteit Rotterdam (ESSB)
Master Bestuurskunde: Beleid en Politiek

Onder supervisie van: dr. Rebecca Moody (EUR) & dr. Peter Scholten (IHS)
Tweede beoordelaar: prof. dr. Menno Fenger
Datum: 18 juli 2022

ERASMUS UNIVERSITEIT ROTTERDAM

Voorwoord

Vijf maanden lang heb ik met plezier aan mijn scriptie gewerkt en het resultaat ligt voor u. Het scriptiestress-verhaal is gelukkig aan mij voorbijgegaan. Het uitvoeren van wetenschappelijk onderzoek heeft mij altijd geboeid en het was een belangrijke drijfveer achter mijn stagekeuze. Hoewel dit een nieuw onderzoeksgebied voor mij was, en de weg vinden in de grote stapel wetenschappelijke artikelen niet altijd even gemakkelijk was, kan ik zeggen dat ik terugkijk op een leuk, interessant scriptieproces.

Tijdens mijn stage binnen het DE-RISC project heb ik kennis kunnen maken met hoe het is om academisch onderzoek te doen wat tegelijkertijd praktisch toepasbaar is. Door de interdisciplinaire insteek, de verschillende werkpakketten en de samenwerking met verschillende partners van buiten de universiteit, heb ik een heel mooi beeld gekregen van hoe zoiets in de praktijk eraan toegaat. Ik wil Peter Scholten enorm bedanken voor de begeleiding gedurende mijn stage. Hij was altijd bereid om mee te denken of helpen en de constructieve feedback die ik heb mogen ontvangen, heb ik zeker niet ervaren als ‘gezeur’ maar heeft het scriptieproces voor mij alleen maar waardevoller gemaakt!

Daarnaast wil ik graag de collega’s van het Erasmus MC, in het bijzonder Jan Jaap Zijl, bedanken. Het uitzetten van een survey bleek meer voeten in de aarde te hebben dan van tevoren werd gedacht, maar de vasthoudendheid en betrokkenheid van hem, Peter en andere collega’s hebben ervoor gezorgd dat uiteindelijk de juiste balletjes gingen rollen. De betrokken en open houding van Peter en Jan Jaap maakte dat ik altijd met een fijn gevoel onze donderdagmeetings in ging, ook al waren deze om 9 uur ’s ochtends en had ik soms nog geen koffie op.

Ook wil ik mijn begeleider Rebecca bedanken voor haar input, tips, enthousiasme en energie. Meerdere malen ben ik verbaasd geweest over de snelheid waarmee ze dingen aan kon pakken. Wanneer ik vragen had, werden deze vrijwel altijd meteen opgelost. Dank voor het geven van sturing, voor alle feedback en de interessante verhalen of weetjes tijdens onze meetings.

Daar waar het gaat om data, privacy en ethiek is naar mijn mening de inspraak van de burger essentieel. Ik hoop dat deze scriptie ervoor zorgt dat ik de mening van de burger heb weten over te brengen en dit in het achterhoofd gehouden zal worden. In dat geval is mijn doel geslaagd!

Rotterdam, 18 juli

Sabien Dekkers

Samenvatting

Met de nieuwe digital twin technologie kan informatie over de werkelijkheid binnen een gebouw verzameld worden. Zo'n digital twin kan ingezet worden wanneer er sprake is van een calamiteit (digitaal calamiteiten systeem) en kan helpen ter verbetering van de calamiteitenrespons van nooddiensten. Hiervoor is het van belang om te weten wat de mening is van burgers als data hiervoor verzameld en gekoppeld zou worden. Deze studie hoopt hieraan bij te dragen door te onderzoeken welke factoren van invloed zijn op de houding van burgers om in noodsituaties hun datagegevens te delen met een digitaal calamiteiten systeem. Dit zal middels een survey (N=236) met verschillende denkbeeldige situaties (vignetten) en aan de hand van lineaire regressieanalyse onderzocht worden. Gekeken is welke factoren van invloed zijn voor vier soorten noodsituaties: individuele nood, collectieve nood, een dreiging van een noodsituatie en een directe noodsituatie.

Uit de resultaten blijkt dat burgers in alle situaties enigszins rationeel de voor- en nadelen van het delen van hun data, afwegen. Wel verschilt per noodsituatie de mate waarin factoren samenhangen met de houding van burgers. Factoren die te maken hebben met het systeem en het data-deelverzoek, zoals het doel waarvoor data wordt gebruikt en de organisatie die een beroep doet op de data, beïnvloeden de manier waarop de voor- en nadelen afgewogen worden en daarmee de houding van burgers. In zijn algemeenheid zien we dat aan de voordeelkant van de vergelijking het verwachte nut en het vertrouwen in de brandweer een grote rol speelt. Hiertegenover staan de risico's die mensen verwachten wanneer zij hun data delen met het systeem en de algemene privacy zorgen die zij hebben. Per noodsituatie is voor burgers belangrijk met wie data wordt gedeeld: (meer) vertrouwen in de stakeholder waarmee data wordt gedeeld kan tot op zekere hoogte risico's en zorgen verminderen, maar is niet geheel in staat om deze risico's en zorgen weg te nemen.

Het advies is om de communicatie en plannen naar buiten goed vorm te geven. Dit door het vaststellen van een sociaal contract. Hiervoor dient goed nagedacht te worden hoe over het systeem gecommuniceerd wordt, waarbij duidelijk het verwachte nut en de overkoepelende waarden achter een dergelijk systeem naar voren gebracht worden. Daarbij dienen ook duidelijke regels en kaders vastgesteld te worden over het gebruik van een digitaal calamiteiten systeem. Over deze kaders, de risico's die wel of niet bestaan en bepaalde wet- en regelgeving, zouden burgers vervolgens geïnformeerd kunnen worden. Dit alles kan meer vertrouwen creëren en risico's en zorgen wegnemen. Door daarnaast een toezichthoudende instantie op te richten (met professionals en burgers), kan toegezien worden op de uitvoer van deze regels en kan gaandeweg het publieke belang in de gaten gehouden worden.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

In de westerse maatschappij neemt big data een steeds prominentere rol in. Onder andere door maatschappelijke uitdagingen op het gebied van milieu, mobiliteit, duurzaamheid en veiligheid zetten steeds meer gemeenten in op het ontwikkelen van een slimme stad (ook wel Smart City*).* In slimme steden worden data en technologieën ingezet om complexe maatschappelijke vraagstukken het hoofd te bieden (Ristvej et al., 2020). Ze worden gezien als een nieuw middel voor stadsmanagement (de Haan & Butot, 2021), vanuit het idee dat verstedelijking een toenemende druk zal uitoefenen op de infrastructuur, middelen en openbare veiligheid van een stad (Caragliu et al., 2011).

Binnen de ontwikkelingen rondom big data en slimme steden is er toenemende aandacht voor de digital twin technologie. Deze technologie maakt het mogelijk om een virtuele representatie te maken van bijvoorbeeld een product of gebouw. Door het verzamelen van data kan real-time informatie gebundeld worden of gedrag in de 'echte' wereld nagebootst worden. Een digital twin van een gebouw kan daarmee beschouwd worden als informatiebron die de werkelijkheid weergeeft (Vereniging van Nederlandse Gemeenten (VNG), 2022) en tegelijkertijd verschillende activiteiten in datzelfde gebouw en de infrastructuur daarvan kan ondersteunen (Volk, Stengel & Schultmann, 2014), denk aan onderhouds- of verduurzamingsprocessen.

In het geval van een noodsituatie (e.g. een ongeval of brand) kan een digital twin gebruikt worden als hulpmiddel door hulpdiensten ter verbetering van de calamiteitenrespons. Dit is interessant omdat de mogelijkheid van een eventuele noodsituatie en de impact hiervan groter wordt in meer dichtbevolkte gebieden. Hulpdiensten werken op dit moment nog met ontruiming- en aanvalsplattegronden. Dit terwijl in publieke gebouwen data wordt verzameld die, wanneer gekoppeld, het gebouw en haar gebruikers in kaart kan brengen zodat dit ingezet kan worden voor het aanpakken van veiligheids- en crisisvraagstukken (Ramesh et al., 2020). Om die reden wordt gekeken naar het opzetten van een *digitaal calamiteiten systeem*: een digitale applicatie die hulpdiensten kan voorzien van de meest accurate informatie over het gebouw en de aanwezige mensen daarin.

De maatschappelijke en individuele voordelen van een digitaal calamiteiten systeem zijn groot. Het tijdig en effectief delen van data kan de risico- en crisisbeheersing ten goede komen en mogelijke schade verminderen, maar voor een effectieve werking van het systeem is data en instemming van de samenleving nodig. Daarom is het belangrijk om te onderzoeken of

burgers hun data met een dergelijk systeem willen delen, als ook eventuele zorgen van burgers en factoren die bepalend zijn voor de houding tegenover het delen van data met een calamiteiten systeem, beter te begrijpen.

1.2 Doel- en vraagstelling

De doelstelling van deze studie is toetsen welke factoren een invloed hebben op de acceptatie van een digitaal calamiteiten systeem door middel van het uitzetten van een survey onder medewerkers, studenten en bezoekers van een ziekenhuis. Op deze manier hopen we tegelijkertijd een kader te kunnen schetsen voor een transparante, doelbewuste en legitieme implementatie van het systeem. De hoofdvraag van dit onderzoek is als volgt: *Welke factoren zijn van invloed op de houding van burgers om in noodsituaties datagegevens te delen met een digitaal calamiteiten systeem?*

Voor het goed beantwoorden van deze hoofdvraag, dient een antwoord geformuleerd te worden op de volgende deelvragen:

1. Welke factoren met betrekking tot de houding van burgers tegenover data delen, kunnen uit de literatuur worden afgeleid?
2. Hoe kunnen de theorieën afkomstig uit deze literatuur gecombineerd worden en welke hypothesen vloeien daaruit voort?
3. Welke factoren hebben, na het toetsen van de hypothesen, een invloed op de houding tegenover data delen in het geval van een digitaal calamiteiten systeem?
4. Welke aanbevelingen kunnen hierbij geformuleerd worden?

De hoofdvraag zal beantwoord worden aan de hand van data uit een survey onder studenten en medewerkers van het Erasmus MC in Rotterdam en bezoekers van ieder willekeurig ziekenhuis. In de survey worden realistische noodsituaties geschetst, waarna we de houding tegenover het verstrekken van data aan een digitaal calamiteiten systeem voor de verschillende noodsituaties kunnen meten, als ook de factoren die hierop van invloed zijn.

1.3 Maatschappelijke relevantie

Het delen en koppelen van data voor een digitaal calamiteiten systeem vraagt om een zorgvuldige aanpak. Juist op het gebied van veiligheid en het behoud hiervan komen urgente ethische vraagstukken omtrent datagedreven technologieën om de hoek kijken, zoals privacy

en sociale rechtvaardigheid (de Haan & Butot, 2021). Data moeten gebruikt worden voor het algemeen belang terwijl tegelijkertijd de individuele wensen en privacy van mensen beschermd moet worden.

Dit betekent dat het van belang is om te weten wat de burger vindt en welke zorgen zij hebben. Immers, het uitsluiten van het perspectief van de burger kan ertoe leiden dat te weinig aandacht is voor de prioriteiten van de burger zelf en is daarmee problematisch voor de legitimiteit (Shelton & Lodato, 2019). De Vereniging van Nederlandse Gemeenten (VNG) stipte al het belang aan van transparantie en verantwoording over de inzet van digital twins en het behouden van het vertrouwen van de burgers op dit gebied. Onder ander andere door het verminderde vertrouwen in de politiek en algemene wantrouwen ten opzichte van technologieën, is het van groot belang om burgers te betrekken bij de inzet van digital twins (VNG, 2022) zoals een digitaal calamiteiten systeem. Middels dit onderzoek zal hieraan tegemoetgekomen worden door aan de voorkant om de mening van burgers te vragen.

1.4 Wetenschappelijke relevantie

Veel onderzoek is uitgevoerd naar de bereidheid of houding van burgers om data te delen op het gebied van e-commercie (McKnight et al., 2002; Gefen et al., 2003; Pavlou 2003; Dinev & Hart, 2006; Li et al., 2011; Robinson, 2017; Ackermann et al., 2021; Urbonavicius et al., 2021), onderzoek (Chen et al., 2016; Bearth & Siegrist, 2020; Waind, 2020) of de gezondheidszorg (Anderson & Agarwal, 2011). Met betrekking tot de acceptatie en het gebruik van e-governmentdiensten is er veel algemeen onderzoek (Warkentin et al., 2002; Carter & Bélanger; 2005; Carter & Schaupp; 2008; Welch et al., 2005), hoewel er ook onderzoeken zijn waarin gekeken wordt naar specifiekere e-governmentdiensten zoals het elektronisch aangifte doen van inkomstenbelasting (Carter & Schaupp, 2008). Een aantal onderzoeken zijn uitgevoerd naar technologieën binnen een slimme stad op bijvoorbeeld het gebied van mobiliteit (Thomas et al., 2016) en stedelijke veiligheid (Butot et al., 2020; Jameson et al., 2019), maar over het algemeen is weinig bekend over de houding van burgers als het gaat om toepassingen van slimme steden.

Volgens de Haan en Butot (2021) zou stedelijk veiligheidsbeheer zelfs sterk ondervertegenwoordigd blijven als toepassingsgebied van de slimme stad en is er dan ook weinig bekend over de houding van burgers tegenover veiligheidssystemen binnen dit soort steden (de Haan & Butot, 2021). Stedelijke veiligheid verwijst hier naar bescherming tegen schade die direct wordt veroorzaakt door het gedrag van (andere) mensen in de stedelijke ruimte

(de Haan & Butot, 2021). In dit onderzoek zal een breder begrip van veiligheid gehanteerd worden, namelijk publieke veiligheid, omdat een digitaal calamiteiten systeem zowel ingezet kan worden voor stedelijke veiligheid (in de vorm van een bedreiging of gijzeling) als voor de veiligheid van gebouwen of voor schade die niet direct het gevolg is van het gedrag van anderen, zoals brand in een gebouw. Ook op dit gebied is onderzoek schaars en blijft het vaak beperkt tot natuurrampen (Hartama et al., 2016; Tonmoy et al., 2020).

Studies naar de acceptatie van een digitaal calamiteiten systeem of soortgelijke systemen zijn, naar ons beste weten, nog niet uitgevoerd. Het is algemeen erkend dat privacygerelateerde beslissingen situationeel zijn en afhankelijk van het doel en de context waarbinnen de data gevraagd wordt (Urbonavicius et al., 2021). Naar verwachting geldt dit ook voor de houding ten opzichte van data delen met een digitaal calamiteiten systeem. De veiligheidsdoeleinden van een dergelijk systeem en de (uitzonderlijke) noodsituaties waar mensen mee geconfronteerd kunnen worden, maken dat het interessant is om te onderzoeken wat voor de burger van belang is bij het delen van hun data wanneer dit binnen een andere context en met een ander doel gebeurt. Noodsituaties kunnen namelijk bepaalde gevoelens of situaties creëren waardoor eerder gevonden factoren die een effect zouden hebben op de houding van burgers, anders kunnen werken.

Daarbij keken voorgaande onderzoeken over de adoptie van e-governmentdiensten naar een klein aantal factoren of naar de invloed van bepaalde contextuele of individuele factoren afzonderlijk. Dit terwijl deze factoren gelijktijdig een invloed uitoefenen op de bereidheid om data te delen en vaak ook met elkaar interacteren (Ackermann, Burkhalter, Mildenberger, Frey, & Bearth, 2021). Voor dit onderzoek naar een digitaal calamiteiten systeem willen we deze complexiteit erkennen en een brede, meer holistische visie toepassen. Dit onderzoek hoopt een bijdrage te leveren aan de uitbreiding van de literatuur op het gebied van e-governmentdiensten in slimme steden door, naast in te gaan op publieke veiligheid als relatief nieuw toepassingsgebied, een grote verscheidenheid aan individuele- en contextuele factoren mee te nemen en te kijken naar welke van deze factoren de meeste invloed hebben. Deze factoren komen voort uit een integratie van de *Unified Theory of Acceptence and Use of Technology* (UTAUT) en de privacy calculus met verschillende theorieën uit de gedragsbestuurskunde, om het belang te onderschrijven van de rol die emoties en gevoelens kunnen spelen, en contextuele theorieën. Op deze manier kan getoetst worden hoe het UTAUT-model en de andere theorieën werken met betrekking tot een digitaal calamiteiten systeem. Daarnaast hopen we, door ook de context in beschouwing te nemen, mogelijke verschillen in acceptatie van de technologie te begrijpen (Whetten, 2009).

1.5 Leeswijzer

Hoofdstuk 2 geeft een beschrijving van de theorieën en hoe deze samengevoegd kunnen worden. In hoofdstuk 3 wordt de onderzoeksopzet, de data en methoden besproken. De resultaten van de analyse worden besproken in hoofdstuk 4, waarna in de conclusie de deelvragen en bijbehorende hoofdvraag beantwoord zullen worden (hoofdstuk 5) gevolgd door een methodologische en theoretische reflectie op het onderzoek (hoofdstuk 6).

2. Theorie

De mate waarin burgers bereid zijn data te delen kan beïnvloed worden door meerdere factoren. In dit hoofdstuk zullen een aantal belangrijke theorieën uiteengezet worden waar deze factoren logischerwijs uit volgen. Hierbij zal gestart worden vanuit de *Unified Theory of Acceptence and Use of Technology* (UTAUT). Dit model is ontworpen door Venkatesh et al. (2003; 2012) en wordt veel gebruikt wanneer het gaat om de adoptie van informatie- en communicatietechnologie (ICT). Het is onder andere gebruikt voor onderzoek naar nieuwe bedrijfstechnologieën, internetgebruik voor consumenten, e-government voor burgers en nieuwe technologieën in de gezondheidszorg (Venkatesh et al., 2016). Dit model is echter nog nooit toegepast op de acceptatie van een ICT-systeem wat ingezet kan worden in het geval van noodsituaties.

In navolging van Weber (2012) en Venkatesh et al. (2016), die stellen dat uitbreidingen van het UTAUT-model vooral gaan over veranderingen binnen de al bestaande factoren, zullen in dit onderzoek meerdere potentiële nieuwe factoren meegenomen worden ter uitbreiding van het model. Hiervoor zullen we het basismodel van UTAUT integreren met andere theorieën. Hierin zal allereerst het privacy calculus model besproken worden. Daarna worden andere theorieën aangehaald die ons in staat stellen om meerdere factoren mee te nemen met betrekking tot de context en het irrationele gedrag van mensen.

Binnen het uiteindelijke conceptuele model (figuur 1, pagina 29) onderscheiden we contextuele en individuele factoren, waarbij de laatste onderverdeeld wordt in individuele overtuigingen en individuele attributen. Deze twee verschillen van elkaar in de zin dat overtuigingen betrekking hebben op hoe iemand ergens over *denkt*. Attributen daarentegen gaan over persoonskenmerken en hoe iemand *is*. Individuele overtuigingen hebben daarmee altijd betrekking op de context of technologie (Homburg et al., 2020), terwijl individuele attributen hier los van staan. Studies tonen ook aan dat sommige persoonlijk attributen geen effect hebben op de uiteindelijke data die iemand deelt (Keith et al., 2013), mogelijk doordat situatiespecifieke individuele overtuigingen deze attributen kunnen overstemmen (Keith et al., 2012; Kehr et al., 2015). Daarom dient een onderscheidt gemaakt te worden tussen al bestaande, persoonlijke attitudes en individuele overtuigingen die situatiespecifiek zijn.

De factoren die afkomstig zijn uit het UTAUT-model kunnen onder individuele overtuigingen geschaard worden (Venkatesh et al., 2016). Omdat dit het startpunt van de theorie is, zullen we op het microniveau beginnen met het bespreken van de individuele overtuigingen. Na het bespreken van deze theorie en bijbehorende hypothesen zullen de individuele overtuigingen behandelt worden die voortkomen uit de privacy calculus benadering.

Vervolgens zullen we verdergaan met het bespreken van de individuele attributen, waarna we toe zullen werken naar het macroniveau en de contextuele factoren.

2.1 Individuele overtuigingen: UTAUT

In het UTAUT-model wordt gesteld dat de intentie van burgers om een technologie te gebruiken, bepaald wordt door 1) het verwachte nut van de technologie, 2) het gebruiksgemak, 3) de mate van sociale invloed uit iemands omgeving en 4) faciliterende omstandigheden. Het verwachte nut en de mate van sociale invloed worden hieronder besproken. Het gebruiksgemak heeft betrekking op de mate van inspanning die gepaard gaat met het gebruik van de technologie (Venkatesh et al., 2003). Met faciliterende omstandigheden wordt verwezen naar de mate waarin gebruikers toegang hebben tot een organisatorische en technische infrastructuur die hen kan ondersteunen in het gebruik van een systeem (Venkatesh et al., 2003).

In dit onderzoek zullen deze twee factoren uit het UTAUT-model echter niet meegenomen worden. Deze keuze is gemaakt omdat de uitkomstmaat in het originele UTAUT-model is gericht op een actie die mensen moeten ondernemen (of zouden willen nemen), namelijk het wel of niet gebruiken van een systeem. Bij de technologie die in dit onderzoek getoetst wordt, i.e. een digitaal calamiteiten systeem, is dit niet het geval. Het gaat in dit onderzoek erom of men het een *goed idee* zou vinden als hun data gedeeld zou worden met een dergelijk systeem. Doordat het geen actie van het subject vergt, zijn de factoren die gaan over het gebruiksgemak en de faciliterende omstandigheden irrelevant. Daarom zal alleen 1) het verwachte nut van de technologie en 2) de mate van sociale invloed meegenomen worden.

2.1.1 Verwachte nut

In de huidige context gaat het verwachte nut over de overtuiging van burgers dat een digitaal calamiteiten systeem hen wat op zal leveren en of het zal helpen bij het oplossen van mogelijke problemen die zich voor kunnen doen in noodsituaties. Deze factor is toegevoegd vanuit het idee dat verwachtingen over de uitkomst en extrinsieke motivatie van belang zijn voor het gebruiken van een technologie. Het effect van het verwachte nut weerspiegelt daarmee de mate waarin houdingen beïnvloed worden door een extrinsieke uitkomst (Dinev & Hart, 2006; Venkatesh et al., 2003).

Voorgaande onderzoeken vonden dat het verwachte nut het sterkste effect had op de intentie om data te delen (Venkatesh et al., 2003). Vanuit de gedachte dat degene met een hogere intentie om data te delen, ook een meer positieve houding zal hebben tegenover het

delen van data, stellen we de volgende hypothese (1) op: *Hoe hoger het verwachte nut van een digitaal calamiteiten systeem, hoe positiever de houding tegenover het delen van data met het systeem.*

2.1.2 Sociale invloed

Venkatesh et al. (2003) definiëren sociale invloed als de mate waarin individuen het gevoel hebben dat mensen binnen hun sociale kring vinden dat zij een ICT-systeem moeten gebruiken. Het gaat hierbij om anderen die belangrijk voor iemand zijn of mensen die een invloed hebben op het gedrag van diegene. De achterliggende gedachte is dat het gedrag van mensen beïnvloed wordt door de manier waarop men denkt dat anderen naar hen en het adopteren van een bepaalde technologie zullen kijken (Venkatesh et al., 2003). Sociale invloed heeft een impact op de houding om data te delen via drie mechanismen: conformisme, internalisering en identificatie. Hierbij gaan de laatste twee voornamelijk over wat iemand zelf gelooft of waarmee iemand zich identificeert, terwijl conformisme ingaat op een gedragsverandering als gevolg van sociale druk over hoe iemand zou moeten handelen (Venkatesh et al., 2003).

Sociale invloed zou afnemen naarmate men een technologie langer kent of gebruikt, omdat ervaring met een systeem in dat geval meer leidend is bij het gebruik ervan (Venkatesh et al., 2003). Verwacht kan worden dat sociale invloed nog een groot effect zal hebben op de houding tegenover een digitaal calamiteiten systeem, omdat dit een vrij nieuwe, nog onbekende technologie is. We stellen de volgende hypothese (2) op: *Hoe meer positieve sociale invloed mensen ervaren met betrekking tot het delen van data met een digitaal calamiteiten systeem, hoe positiever de houding tegenover het delen van data met het systeem.*

2.2 Individuele overtuigingen: privacy calculus

Een ander, veelgebruikt theoretisch raamwerk dat toegepast wordt op vraagstukken rondom data delen is de privacy calculus. Deze theorie lijkt op de economische nutsbenadering, in de zin dat gekeken wordt naar factoren in de vorm van kosten en baten, of voor- en nadelen, waartussen een afweging gemaakt zou worden alvorens mensen beslissen hun data te delen (Anderson & Agarwal, 2011). Hierbij gaat het veelal om privacyoverwegingen en wordt het principe van nutsmaximalisatie nagestreefd (Keith et al., 2012). De batenkant kan een weerspiegeling geven van de bereidheid die men heeft om de risico's die gepaard gaan met data delen, te accepteren (Anderson & Agarwal, 2011). Ander onderzoek (Kehr et al., 2015) laat

juist zien dat een bepaalde mate van bereidheid omtrent het delen van data voortvloeit uit de kosten- en batenkant en de manier waarop deze twee elkaar onderling beïnvloeden.

Aan de kostenkant van de vergelijking gaat het vaak over de privacy risico's (Keith et al., 2012) terwijl de batenkant meer ingaat op vertrouwen (Culnan & Bies, 2003; Mayer et al. 1995; Malhotra et al., 2004) of het nut dat iemand eruit haalt (Keith et al., 2012). In dit onderzoek zullen we ingaan op zowel de kosten- als de batenkant door enerzijds te kijken naar (factoren van) risicopercepties en anderzijds naar voordeelpercepties. Door naar beide kanten van de calculus te kijken, en niet alleen naar de privacy risico's en zorgen die mensen hebben, kan onderzocht worden of mensen de voordelen van het delen van hun data genoeg vinden om op te wegen tegen de eventuele risico's en bijbehorende gevolgen (Ackermann et al., 2021).

Tot de voordeelkant van de vergelijking behoort, wanneer het gaat over individuele overtuigingen, het verwachte nut. Dit komt voort uit het UTAUT-model en is hierboven besproken. Aan de risicokant zal het gaan over de verwachte risico's die iemand heeft met betrekking tot het gebruiken van een digitaal calamiteiten systeem. Dit wordt verder uiteengezet in onderstaande paragraaf 2.2.1. Daarnaast zal in de daaropvolgende paragraaf gekeken worden naar het vertrouwen dat men heeft. Dit is een factor die zowel aan de kant van de risicopercepties als de voordeelpercepties geplaatst kan worden (Bearth & Siegrist, 2020). Wanneer vertrouwen aanwezig is, zullen enerzijds de verwachte risico's verminderen (Jarvenpaa & Tractinsky, 1999; Pavlou, 2003) of zorgen en onzekerheden gecompenseerd worden (Malhotra et al., 2004; Schaupp et al., 2010). Anderzijds zou het een positief effect kunnen hebben op de voordeelpercepties, onder andere doordat het verwachte nut toeneemt (Pavlou, 2003).

2.2.1 Verwachte risico's

In eerder onderzoek (Schaupp et al., 2010; Dinev & Hart, 2006; Li et al., 2011) is aangetoond dat de risico's die mensen voorzien een effect hebben op de intentie om een technologisch systeem te gebruiken. Aangezien het lastig is om risico's objectief vast te stellen, richten onderzoeken over het delen van data zich op de subjectieve risicoverwachting (Warkentin et al., 2002). Het verwachte risico heeft betrekking op de overtuiging van een burger om met een negatief resultaat geconfronteerd te worden (Robinson, 2017), of verlies te lijden, wanneer hij of zij bepaalde handelingen uit moet voeren om een uitkomst na te streven (Warkentin et al., 2002).

Schaupp et al. (2010) stellen dat de verwachte risico's voortkomen uit a) onzekerheden over de omgeving (*omgevingsonzekerheid*) en b) onzekerheden over het gedrag van stakeholders en de angsten die hieruit voort kunnen komen (*gedragsonzekerheid*). Omgevingsonzekerheid heeft te maken met het internet, de technologie en het onvoorspelbare karakter hiervan (Pavlou, 2003) en komt voort uit de onderliggende infrastructuur van een technologie of systeem (Ring & van de Ven, 1994). Dit alles ligt veelal buiten de controle van de burger (Pavlou, 2003). Gedragsonzekerheden zijn relationeel van aard en komen voort uit (verwachtingen over) het gedrag van de organisaties die gemoeid zijn met het systeem (Pavlou, 2003; Ring & van de Ven, 1994). Hierbij kan gedacht worden aan de angst dat derde partijen het proces van data delen in gevaar brengen of onvoldoende maatregelen zijn genomen om risico's gerelateerd aan de onderliggende infrastructuur, te verminderen (Pavlou, 2003). Zowel omgevingsonzekerheden als gedragsonzekerheden kunnen gepaard gaan met risico's die kunnen leiden tot een verlies van privacy.

De houding van iemand omtrent data delen zal afhankelijk zijn van deze onzekerheden. Meer onzekerheden leidt tot meer angsten en verwachte risico's. Onderzoek op het gebied van e-commercie toont aan dat risico's de intentie om data te delen verminderen (Pavlou, 2003; Kehr et al., 2015). Verwacht kan worden dat de e-commercie context met meer onzekerheid gepaard gaat dan een publieke context, waar het digitaal calamiteiten systeem toegepast wordt. Toch is op het gebied van ICT-adoptie van e-governmentdiensten dezelfde tendens te zien (Warkentin et al., 2002; Carter & Bélanger, 2005; Schaupp et al., 2010). In navolging hiervan stellen we de volgende hypothese (3) op: *Hoe meer verwachte risico's, hoe negatiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.2.2 Vertrouwen

In alle economische en sociale interacties waar onzekerheden en risico's een rol spelen is vertrouwen een belangrijk, bepalend kenmerk (Pavlou, 2003). Dit geldt ook voor de acceptatie van internettechnologieën (Gefen, 2000). In e-commercie onderzoek is gebrek aan vertrouwen een van de belangrijkste redenen om geen data te delen of niet te interacteren met een systeem (Keen, 1999). Op het gebied van e-governmentdiensten is de belangrijke rol van vertrouwen meermaals onderzocht (Bélanger & Carter, 2008; Schaupp et al., 2010; Warkentin et al., 2002; Welch et al., 2005). In navolging van meerdere definities van vertrouwen (McKnight et al., 1998; Rotter, 1967; Gefen, 2000), definiëren we vertrouwen als de verwachting van een burger dat een ander individu, organisatie of institutie geen misbruik zal maken van de kwetsbaarheden

van de ander ook al heeft het individu, de organisatie of institutie wel de macht om dit te doen (Pavlou & Gefen, 2004). Hierbij zijn verwachtingen dat de andere partij tegemoet zal komen aan de verwachtingen van de burger.

Vertrouwen heeft twee facetten, welke lijken op de hierboven benoemde onzekerheden waarin angst een rol speelt en wat veelal hand in hand gaat met vertrouwen. Aan de ene kant heb je de traditionele kijk op vertrouwen in een specifieke organisatie (Pavlou, 2003). Aan de andere kant het vertrouwen in de ICT-dienst of infrastructuur (Pavlou, 2003). Wanneer burgers besluiten zich kwetsbaar op te stellen tegenover een andere organisatie, en daarmee de organisatie vertrouwen, nemen ze de kenmerken van de organisatie (i.e. gedragsonzekerheid) en kenmerken van de dienst en technologische infrastructuur (i.e. omgevingsonzekerheid) in overweging (Pavlou, 2003). In dit onderzoek zal ook op vertrouwen ingegaan worden door allereerst te kijken naar vertrouwen in de organisaties. Daarna wordt gekeken naar vertrouwen in een digitaal calamiteiten systeem als dienst en de achterliggende infrastructuren.

Vertrouwen in de organisaties

Met betrekking tot vertrouwen in organisaties zal gekeken worden naar a) het vertrouwen in de overheid als organisatie en b) het vertrouwen in de organisaties die toegang hebben tot de data van een digitaal calamiteiten systeem, namelijk het ziekenhuis, de brandweer en de politie. Algemeen vertrouwen in de overheid is van belang, omdat het gezien kan worden als een organisatie die publieke diensten verleend en publieke waarde creëert (Carter & Bélanger, 2005; McKnight et al., 2002; Welch et al., 2005). In het geval van een digitaal calamiteiten systeem gaat het ook over een publieke dienst waar overheidsinstanties mee gemoeid zijn, waardoor vertrouwen in de overheid een uitwerking zou kunnen hebben op de houding tegenover (het delen van data met) het systeem.

Zeker wanneer sprake is van informatieassymetrie, door bijvoorbeeld gebrek aan expertise of kennis waardoor men niet na kan gaan of correct wordt gehandeld, is vertrouwen cruciaal (Culnan & Armstrong, 1999). In het geval van een digitaal calamiteiten systeem is dit het geval. Als gevolg van informatieassymetrie en het niet (goed) kunnen controleren of anticiperen op het gedrag van mensen en organisaties, ontstaat sociale complexiteit (Moody, 2010). Door vertrouwen gaan mensen ervanuit dat de ander zich zal gedragen zoals verwacht, waardoor de complexiteit van de interactie met een organisatie af zal nemen (Pavlou, 2003; Gefen, 2000; Luhmann, 1979).

Zo zou vertrouwen een bepalende factor zijn achter het verwachte nut van een technologie, omdat de garantie dat je daadwerkelijk het nut haalt uit het gebruik van een

systeem deels afhangt van de organisatie(s) achter dat systeem (Gefen, 1997) en de verwachting dat de organisatie zich zal gedragen in overeenstemming met de overtuigingen van diezelfde burger (Pavlou, 2003; Bearth & Siegrist, 2020). Daarbij zou het de burger een stukje gevoel van controle teruggeven over hoe persoonlijke data gebruikt wordt, wat waarschijnlijk aanmoedigend werkt voor het delen van data (Warkentin et al., 2002).

Ervan uitgaande dat vertrouwen betekent dat degene ook meer vertrouwen heeft in het handelen van de organisatie (Warkentin et al., 2002), zou dit onzekerheden over het handelen en angsten over de te vertrouwen organisatie (i.e. gedragsonzekerheid) moeten verminderen (Pavlou, 2003; Bearth & Siegrist, 2020). Dit maakt dat vertrouwen ook een uitwerking kan hebben op de risicopercepties van burgers: het niet aanwezig zijn van vertrouwen, vergroot de zorgen of angsten waardoor men meer risico's voorziet. In overeenstemming met de literatuur stellen we de volgende hypothesen op:

H4: *Hoe hoger het vertrouwen in de overheid, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

H5: *Hoe hoger het vertrouwen in het ziekenhuis, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

H6: *Hoe hoger het vertrouwen in de brandweer, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

H7: *Hoe hoger het vertrouwen in de politie, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

Vertrouwen in de technologie

Vertrouwen in de organisatie omvat ook voor een groot deel vertrouwen in de technologie en achterliggende infrastructuur, zelfs als de organisatie geen absolute controle heeft hierover (Pavlou, 2003). Vertrouwen in ICT-diensten is zowel online en binnen de e-commercie (Urbonavicius et al., 2021; Bansal et al., 2016) als e-government (Carter & Bélanger, 2005; Schaupp et al., 2010) uitgebreid onderzocht. Met betrekking tot vertrouwen in elektronische diensten, onderscheiden Tan & Theon (2011) twee vormen: 1) vertrouwen in de entiteit die de service levert en 2) vertrouwen in het mechanisme achter de service. In overeenkomst met eerder onderzoek (Pavlou, 2003; Carter & Bélanger, 2005; Schaupp et al., 2010) zal vertrouwen

in elektronische diensten op dezelfde tweeledige manier bekeken worden. Hierbij gaat het vertrouwen in de entiteit over het digitaal calamiteiten systeem. Vertrouwen in het mechanisme achter een digitaal calamiteiten systeem heeft betrekking op algemeen vertrouwen in de technologische infrastructuur.

Het wegblijven van vertrouwen in (de infrastructuur achter) elektronische diensten kan meer onzekerheid en zorgen tot gevolg hebben doordat data makkelijk verzameld, gemanipuleerd en gebruikt kan worden door meerdere partijen die niet direct met het gebruik te maken hoeven hebben (Warkentin et al., 2002). De omgevingsonzekerheid die bestaat over de technologische infrastructuur en de onvoorspelbaarheid hiervan, kan gedempt worden door vertrouwen (Pavlou, 2003). Vertrouwen geeft, zoals hierboven ook kort benoemd, een stuk controle terug die de burger lijkt kwijt te raken met het gebruik van een systeem (Pavlou, 2003). Dit alles zou een positief effect moeten hebben op de houding tegenover het delen van data en leidt daarmee tot de volgende hypothesen:

H8: *Hoe hoger het vertrouwen in een digitaal calamiteiten systeem, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

H9: *Hoe hoger het algemene technologische vertrouwen, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.3 Individuele attributen

In de voorgaande paragrafen zijn de individuele overtuigingen besproken. Nu zullen de individuele attributen nader beschouwd worden. Attributen van gebruikers kunnen gaan over demografische kenmerken (Venkatesh et al., 2016) zoals leeftijd, geslacht en opleidingsniveau, maar ook over andere persoonskenmerken of factoren die iets zeggen over hoe iemand *is* en losstaan van de context en de te implementeren technologie. Het toevoegen van individuele attributen biedt de mogelijkheid om andere factoren uit de meer emotionele en irrationele hoek van het menselijk gedrag toe te voegen. Dit ter aanvulling op de privacy calculus benadering, van waaruit de kwestie omtrent het delen van data vooral benaderd wordt vanuit de rationele hoek.

Dat individuen namelijk niet altijd rationeel handelen, is terug te zien in de privacy paradox. De privacy paradox refereert naar de discrepantie die bestaat tussen de risicopercepties die mensen hebben bij het delen van data en het daadwerkelijke deelgedrag dat mensen tonen,

in de zin dat mensen met meer risicopercepties alsnog relatief vaak bereid zijn om hun data te delen (Acquisti & Grossklags, 2004; Norberg et al., 2007). Dit staat haaks op de veronderstelling van de privacy calculus dat mensen rationeel handelen en waarbij ervan uitgegaan wordt dat een lineaire relatie bestaat tussen de voordeel- en risicokant (Dinev & Hart, 2006).

Onder andere door psychologische beperkingen zoals *bounded rationality*, i.e. beperkte beschikbare informatie en tijd om tot een besluit te komen (Acquisti & Grossklags, 2005), zitten er grenzen aan het toepassen van de privacy calculus (Kehr et al., 2015). Als gevolg worden besluitvormingsprocessen ook vormgegeven door vuistregels, of heuristieken (Gigerenzer & Gaissmaier, 2011). Het *risk-as-feelings* perspectief (Loewenstein et al., 2001) biedt een alternatief voor de privacy calculus doordat rekening gehouden wordt met deze emoties, gevoelens en factoren die deze emoties en gevoelens kunnen beïnvloeden. Zo kan een persoon meer bezorgd zijn door eerdere ervaringen met datalekken of beslissingen maken om meer emotionele redenen, waarbij gekeken wordt naar de waarschijnlijkheid dat iets voorkomt (Loewenstein et al., 2001).

In navolging van die redenering is het aannemelijk dat zeker wanneer een individu gevraagd wordt om zijn/haar data te delen in het geval van een noodsituatie, zij over zullen gaan tot het delen hiervan vanuit een emotionele toestand, welke wordt beïnvloed door persoonlijke factoren. Om deze reden worden in dit onderzoek meerdere individuele attributen meegenomen. In tegenstelling tot persoonlijke overtuigingen staan deze los van de te implementeren technologie. Attributen variëren van persoonlijke ervaringen, competenties van mensen of andere karaktereigenschappen zoals risicoaversie en de mate waarin iemand zich zorgen maakt over privacygerelateerde zaken.

2.3.1 ICT-vaardigheden

Een kenmerk dat de houding tegenover het delen van data met een digitaal calamiteiten systeem kan beïnvloeden, is de mate waarin iemand technologisch vaardig is. Onderzoekers vonden dat ervaring met smartphone technologieën, kwantiteit van gebruik hierin (Wenz et al., 2017, Keusch et al., 2019; Struminskaya et al., 2020) en zelfeffectiviteit in computergebruik (Carter & Schaupp, 2008; Chiu & Wang, 2008) relateerden aan een hogere bereidheid om een bepaalde technologie te gebruiken. Het hebben van meer ervaring in het gebruik van internet zou ertoe leiden dat burgers zich in mindere mate zorgen maken over risico's, terwijl het een positieve uitwerking heeft op vertrouwen (Dutton & Shepherd, 2006). Ervan uitgaande dat de houding

tegenover het delen van data positief beïnvloed wordt door een afname in risico's en een toename in vertrouwen, en ICT-vaardigheden hier een effect op hebben, stellen we de volgende hypothese (10) op: *Hoe beter de ICT-vaardigheden, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.3.2 Privacy zorgen

Eerder onderzoek (Dinev & Hart, 2006; Li et al., 2011; Dinev et al., 2012) laat zien dat de algemene privacy zorgen die iemand heeft van invloed zijn op opvattingen over data delen en het daadwerkelijke deelgedrag. Het gaat hier om de algemene neiging van burgers om zich zorgen te maken over hun privacy met betrekking tot hun data (Malhotra et al., 2004) en staat daarmee los van de context (Li et al., 2011). Wel kunnen contextuele factoren de impact van algemene privacy zorgen op de houding tegenover het delen van data beïnvloeden. In de interactie met een digitaal calamiteiten systeem kan het echter ontbreken aan concrete informatie over de context, zoals met wie de data wordt gedeeld. Algemene privacy zorgen kunnen daardoor een belangrijke rol spelen in het vormgeven van de houding tegenover data delen (Li et al., 2011).

Ook de mate waarin iemand waarde hecht aan het behouden van autonomie over zijn/haar data is hier van belang. Zoals eerder benoemd gaat het proces van data delen gepaard met onzekerheden, onder andere vanwege de perceptie van de burger dat zij de controle over hun data verliezen (Smith et al., 2011; Wang et al., 2016). Voor iemand die minder waarde hecht aan het behouden van autonomie hoeft een verlies van controle niet per se tot een minder positieve houding tegenover data delen te leiden. Immers, wanneer je het behouden van autonomie over je data minder belangrijk vindt, of in mindere mate bang bent om dit te verliezen, dan heb je mogelijk een positievere houding omdat je het an sich al minder erg vindt om de controle over je data te verliezen.

Dinev en Hart (2006) lieten zien dat factoren als vertrouwen niet compleet de privacy zorgen weg kunnen nemen: zelfs wanneer mensen beslissen om over te gaan op het delen van hun data, blijven hun privacy zorgen bestaan. Onderzoekers hebben aangetoond dat de algemene privacy zorgen een positief effect hebben op de verwachte risico's (Li et al., 2011; Kehr et al., 2015) en negatief op de intentie om data te delen (Stewart & Segers, 2002; Son & Kim, 2008; Li et al., 2011). Met betrekking tot smartphone sensor data zijn privacy zorgen een van de belangrijke redenen voor het niet willen delen van data (Revilla et al., 2019 &

Struminskaya et al., 2020). Verwacht wordt dat (hypothese 11): *Hoe meer privacy zorgen, hoe negatiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.3.3 Conformisme

Conformisme gaat in op de mate waarin burgers zich (willen) gedragen volgens de sociale norm. Sociale normen zijn het resultaat van een min of meer gedeeld begrip in de samenleving over welk gedrag is toegestaan, verboden of juist verplicht (Crawford & Ostrom 1995). Door socialisatie, blootstelling aan en observaties van andermans gedrag krijgen we de normen en waarden aangeleerd (Melnyk et al., 2021). Vanuit de overtuiging dat bepaalde gedrag populair is (Stibe & Cugelman, 2019) of iets verstandig is om te doen als iedereen het doet, volgen mensen de acties of meningen van anderen (Cialdini et al., 1990).

Binnen de samenleving zijn er meerdere groepen die verschillende normen en waarden aanhangen (Ultee, Arts & Flap, 2011). De integratietheorie stelt dat iemand die sterker in een groep is geïntegreerd ook sterker de normen en waarden van de desbetreffende groep zal overnemen (Ultee, Arts & Flap, 2011). Zeker mensen die de neiging hebben om meer te conformeren aan de sociale norm en zich willen gedragen zoals anderen, zullen naar de sociale normen en waarden van de groep willen handelen.

De vraag is welke normen en waarden binnen de verschillende groepen leven. Berkowitz & Daniels (1964) stellen in een reeks experimenten dat mensen gemotiveerd zijn om anderen te helpen die van hen afhankelijk zijn, omdat het geven van hulp iets is wat voortkomt uit de ‘social responsibility norm’. Mensen leren hierdoor snel dat het helpen van anderen een belangrijke waarde is (Szuster, 2016). Zij die deze norm aanhangen zullen mogelijk positiever tegenover data delen staan, maar de mate waarin mensen geneigd zijn om anderen te helpen die buiten hun groep vallen varieert per cultuur. Het is tegelijkertijd denkbaar dat iemand bij een groep hoort waarvan mensen heel veel waarde hechten aan privacy, en hij of zij daardoor negatiever tegenover data delen zal staan. De mate waarin conformisme leidt tot een meer positieve of negatieve houding tegenover een digitaal calamiteiten systeem, zal daarom afhangen van de sociale normen en waarden die iemand aanhangt als gevolg van de groep waartoe iemand behoort. Daarom stellen we de volgende twee tegengestelde hypothesen op: (12) *Hoe meer iemand de neiging heeft te conformeren aan de sociale norm, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem;* en (13) *Hoe meer iemand de neiging heeft te conformeren aan de sociale norm, hoe negatiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.3.4 Altruïsme

In het geval van noodsituaties is het aannemelijk dat altruïsme een rol zal spelen in het beïnvloeden van de houding tegenover data delen. Met altruïsme doelen we op de onbaatzuchtigheid en mate waarin iemand gericht is op het welzijn van anderen. In het geval van gezondheidsdata vonden Anderson & Agarwal (2011) dat altruïsme een effect had op het delen van data voor onderzoeksdoeleinden. In een onderzoek naar het koppelen van surveydata (Sala et al., 2014) wordt de mate waarin iemand behulpzaam wil zijn geassocieerd met een hogere mate van bereidheid.

Een digitaal calamiteiten systeem levert niet alleen persoonlijke voordelen, en soms zelfs geen persoonlijke voordelen, maar zit veelal op het bredere, maatschappelijke nut. Het afwegen van je recht op privacy tegenover de rechten van anderen, of de maatschappij als geheel, zal er voor een altruïst anders uitzien dan voor iemand die minder altruïstisch is. Een altruïst zal zich eerder behulpzaam opstellen. Als iets positief is voor de maatschappij, dan zal een altruïst eerder geneigd zijn om zijn/haar eigen privacy op te geven of risico's te accepteren door data te delen met een digitaal calamiteiten systeem. We stellen dat (H14): *Hoe altruïstischer iemand is, hoe positiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.3.5 Risicoaversie

Burgers verschillen in hun neiging om risico's te vermijden in plaats van deze op te zoeken (Ye et al., 2008). De houding die iemand heeft ten opzichte van het nemen van risico's speelt ook een rol in de kosten-batenafweging (Moloney & Poti, 2013). Risicoaversie zou leiden tot grotere privacy zorgen (Korzaan et al., 2009; Harborth & Pape, 2020). Uit onderzoek (Trepte et al., 2017) blijkt dat in culturen die hoog scoren op risicoaversie, privacy risico's belangrijker blijken bij het nemen van beslissingen over het delen van data, terwijl minder waarde gehecht wordt aan het verwachte nut. Vanuit het idee dat de verwachte risico's voor de risicoaverse mensen groter zijn en de voordelen minder, zal naar verwachting de risicokant zwaarder wegen dan de voordeelkant bij het maken van een beslissing. Dat leidt tot de volgende hypothese (15): *Hoe meer risicoavers iemand is, hoe negatiever de houding tegenover het delen van data met een digitaal calamiteiten systeem.*

2.4 Contextuele factoren

De privacy calculus theorie zou, naast te veel de focus te leggen op het rationele aspect, ook niet altijd de omgeving meenemen terwijl dit wel een factor is die van invloed kan zijn op iemands houding over data delen. Overwegingen die binnen een specifieke context gemaakt worden, zouden algemene attitudes en houdingen immers kunnen overstemmen (Li et al., 2011; Keith et al., 2013). Zo zou de mate waarin burgers waarde hechten aan bescherming en geheimhouding van hun data voortkomen uit een bepaalde indruk van hun verwachte privacy op dat moment, welke gemaakt wordt door het afwegen van de voor- en nadelen binnen de context waar zij in zitten (Dinev et al., 2012; Kehr et al., 2015).

De rol van de context in het beïnvloeden van theorieën en bevindingen op het individuele niveau heeft steeds meer aandacht gekregen (Venkatesh et al., 2016). Als het gaat om ICT spreken Hong et al. (2014) over de kenmerken en gebruikscontext van de technologie. In dit onderzoek zal ingegaan worden op de gebruikscontext door te kijken naar de verschillende soorten noodsituaties waarin mensen keuzes moeten maken en de verschillende stakeholders die, afhankelijk van de situatie, te maken hebben met het proces van data delen. Met betrekking tot kenmerken van de technologie zal ingegaan worden op het type data dat gevraagd wordt te delen. Op deze manier komen we tegemoet aan de aanbeveling van Venkatesh et al. (2016) om het UTAUT-model als basis te gebruiken, waarna contextfactoren kunnen worden toegevoegd om nieuwe effecten te identificeren of bestaande effecten te verfijnen.

Communicatie privacy management theorie is een benadering die voortbouwt op de privacy calculus benadering, maar een contextueel element toevoegt. Deze benadering voegt expliciet toe dat mensen beslissen hun data te delen op basis van criteria of regels die zij belangrijk vinden op het moment dat de beslissing moet worden genomen (Petronio & Durham, 2008). Zo zouden mensen beslissingen maken op basis van de risico-voordeel verhoudingscriteria (Anderson & Agarwal, 2011). Binnen deze criteria stellen ze dat mensen in hun beslissing om data te delen, rekening houden met de verschillende soorten en niveaus van risico's (Anderson & Agarwal, 2011). Situationele factoren die aanwezig zijn in het verzoek, zoals het soort data, het doel waarvoor de data zal worden gebruikt en de organisatie die het deel-verzoek uitdraagt, beïnvloeden het type en niveau van risico en de bijbehorende risico-voordeel calculatie (Anderson & Agarwal, 2011).

Hiernaast voegt de theorie nog een ander criterium toe, namelijk de relevante contextuele factoren. Het online disclosure consciousness model van Robinson (2017) sluit hierop aan. Volgens dit model verplaatsen mensen zich over het continuüm van data delen op

basis van een van de volgende drie factoren: 1) acties van de stakeholder die erop gericht zijn om iemand wel of niet zijn/haar data te laten delen (i.e. voordelen geven, vertrouwen verbeteren), 2) persoonlijke ervaringen (i.e. eerdere ervaringen met data delen of van iemand in je nabije omgeving, sociale druk) en 3) externe gebeurtenissen (i.e. media aandacht voor datalekken, bedreigingen voor de volksgezondheid) (Robinson, 2017).

De eerste twee factoren zijn in de voorgaande paragrafen besproken. We zullen in de komende paragrafen allereerst ingaan op de contextuele factoren in de vorm van externe gebeurtenissen, een factor die door beide theorieën aangehaald wordt. Daarna gaan we in op de verschillende type data en stakeholders. Voor deze contextuele factoren zullen geen hypothesen geformuleerd worden, omdat de data het niet toelaat dat dezen expliciet getoetst worden in de analyse. De theorieën hierover zullen wel uiteengezet worden, zodat de context waarbinnen een digitaal calamiteiten systeem opereert meer duiding krijgt. Overwegingen om data te delen worden immers gemaakt binnen een bepaalde context. Verschillen in de effecten van individuele factoren kunnen daardoor eventueel verklaard worden door de context waarin keuzes gemaakt worden. Interessant is daarom te bekijken hoe de houding omtrent data delen verschilt naar bepaalde contextuele factoren. Om dit toelichting te kunnen geven, zullen hierover beschrijvende analyses uitgevoerd worden.

2.4.1 Noodsituaties

Contextuele factoren kunnen betrekking hebben op bepaalde leefomstandigheden of traumatische gebeurtenissen (Anderson & Agarwal, 2011). Traumatische gebeurtenissen delen vaak een aantal gemeenschappelijke eigenschappen: ze zijn ongewenst, onverwacht en oncontroleerbaar (Norris, 1990). Hierbij kan gedacht worden aan een onverwacht sterfgeval, beroving, verwonding door brand of een ramp, evacuatie of andere direct dreigende gevaren die zich voor kunnen doen (Norris, 1990). Goodman et al. (1998) zeggen dat iets een traumatische gebeurtenis is als een persoon of iemand in diens directe omgeving een gebeurtenis heeft meegemaakt die levensbedreigend was, waarbij sprake is van geweld en/of aantasting van de lichamelijke integriteit. In dit onderzoek zal gekeken worden naar de bereidheid om data te delen in het geval van verschillende noodsituaties, welke volgens bovenstaande definities aangeduid kunnen worden als traumatische gebeurtenis.

De *prospect theory* (Kahneman & Tversky, 1979) biedt een uitleg voor hoe mensen beslissingen maken wanneer zij met risico's te maken hebben. Hierbij wordt gekeken naar de relatie tussen de contingente omgeving, in de vorm van winst-verlies, en de risicobereidheid

van individuen (McDermott et al., 2008). De theorie behandelt hoe mensen keuzes maken op basis van individuele heuristieken en biedt daarmee een andere kijk op het proces van data delen dan de privacy calculusbenadering.

In het kort zijn degenen die met winst worden geconfronteerd risicomijdend, terwijl degenen die met verliezen worden geconfronteerd juist meer risicozoekend zijn (McDermott et al., 2008; Keith et al., 2012). Dit biedt een interessante kijk op de beslissingen die mensen maken over het delen van data in noodsituaties, omdat in dit geval ook sprake is van winst (bepaalde voordelen) en verliezen (bepaalde risico's). Nu hoeft lang niet iedere calamiteit even grote, directe gevolgen te hebben voor een individu. In dit onderzoek maken we onderscheid tussen 1) omvang en 2) urgentie van de noodsituatie. Omvang is onderverdeeld in individuele nood en collectieve nood. Urgentie heeft betrekking op een dreiging dan wel een directe noodsituatie.

In dit licht presenteren McDermott et al. (2008) een model waarin ze laten zien dat factoren buiten de controle van het individu, zoals omgevingsfactoren, beslissingen kunnen beïnvloeden. Meer specifiek stellen zij dat keuzes over leven en dood, voortplanting en ons voortbestaan in meerdere mate bepaald worden door de manier zoals de *prospect theory* dit voorschrijft in vergelijking met het maken van andere keuzes (McDermott et al., 2008; Kühberger et al., 1999; Wang, 1996). Dit betekent dat, wanneer beslissingen genomen moeten worden die in meerdere mate te maken hebben met overleven, mensen zich meer risicozoekend gaan gedragen naarmate de dreiging groter is (McDermott et al., 2008).

Noodsituaties kunnen de percepties van risico's door het individu ook beïnvloeden. Factoren die mogelijk een invloed hebben op de risicopercepties, zoals vertrouwen in de technologische infrastructuur, kunnen in het geval van een noodsituatie minder belangrijk worden bij het nemen van een beslissing om data te delen (Anderson & Agarwall, 2011). De voordeelperceptie is dan, door een toename in het verwachte nut, meer prominent: een meer risicovolle keuze vergroot de overlevingskans (McDermott et al., 2008) in het geval van een noodsituatie. Aan de andere kant kunnen ook, wanneer in mindere mate sprake is van een noodsituatie, de voordelen minder zichtbaar zijn en zal de risicoperceptie juist groter zijn, wat de rol van vertrouwen belangrijker maakt in de houding om data te delen.

Dinev en Hart (2006) keken naar persoonlijk belang en het effect op de bereidheid om persoonlijke data te delen op internet. Zij vonden dat het hebben van een persoonlijk belang kon overheersen over eventuele privacy zorgen die mensen hadden (Dinev & Hart, 2006). De noodsituatie waarin iemand zich bevindt, kan een belangrijke indicator zijn voor het persoonlijke belang dat iemand kan hebben bij het delen van zijn of haar data. Verwacht kan

worden dat burgers meer persoonlijk belang hebben bij het oplossen van een collectieve nood, zoals een brand, dan de individuele nood van een ander persoon. Daarbij zullen de verliezen waarmee burgers worden geconfronteerd groter zijn in het geval van een collectieve nood, waardoor zij zich eerder risicozoekend zullen gedragen of de risico's die gepaard gaan met het delen van data zullen accepteren.

Intertemporele keuzetheorie stelt dat korte termijn uitkomsten zwaarder wegen dan lange termijn uitkomsten bij het maken van beslissingen (Keith et al., 2012). *Delay discounting* is hier een voorbeeld van en verwijst naar de neiging van mensen om bij het maken van keuzes grotere waarde toe te kennen aan directe risico's en voordelen tegenover latere (Acquisti & Grossklags, 2004). In het geval van een eventuele noodsituatie betekent dit dat eerder oog zal zijn voor de directe risico's en eventuele voordelen die gepaard gaan met de situatie die zich voordoet, terwijl men de risico's over het delen van hun data zal onderschatten omdat deze verder in te toekomst liggen. Dit zal nog groter zijn in het geval van een directe noodsituatie versus een dreiging van een noodsituatie, omdat de risico's en voordelen bij een dreiging onduidelijker zijn en verder in de toekomst liggen.

Het onderzoek van Brandimarte et al. (2012) sluit hierop aan. Zij toonden aan dat besluitvorming over het delen van data beïnvloed wordt door de merkbaarheid en directheid van eventuele gevolgen die vastzitten aan het besluit. Onderbuikgevoelens zouden beslissingen van mensen kunnen vormgeven als de merkbaarheid laag is en risico's verderweg liggen qua tijd en afstand (Kehr et al., 2015). Volgens onderzoek blijken mensen tevens meer angst te ervaren wanneer de uitkomst van een situatie sneller plaats zal vinden en kan gedrag daardoor veranderen (Loewenstein et al. 2001). Daarbij gedragen mensen zich zoals eerder vermeld doorgaans emotioneler en meer risicozoekend wanneer het gaat om een keuze tussen leven en dood (Druckman & McDermott, 2008). Verwacht kan worden dat mensen minder beïnvloed worden door emotie wanneer minder sprake is van (directe) nood, waardoor mensen in het geval van een dreiging minder zullen handelen zoals de *prospect theory* voorschrijft en meer rationeel de voordelen en risico's in overweging zullen nemen.

2.4.2 Stakeholder

In eerder onderzoek naar het verzamelen van mobiele data werd al aangetoond dat uitmaakt welke stakeholder de data verzameld (Keusch et al., 2019; Struminskaya et al., 2020). De theorie van Nissenbaum (2009) over contextuele integriteit stelt dat het delen van data afhangt van contextspecifieke verwachtingen. Deze verwachtingen zijn afhankelijk van het type data,

wat later besproken wordt, het doel waarvoor deze data verzameld wordt en *met wie* de data wordt gedeeld. Burgers kunnen verschillende verwachtingen hebben over het beoogde gebruik van verschillende type data, afhankelijk van wie om de data vraagt (Struminskaya et al., 2020) of wie het zal gebruiken. Zo zou het delen van locatiegegevens met de politie opgevat kunnen worden als surveillance, terwijl het delen van deze gegevens met een ziekenhuis of brandweer niet dergelijke verwachtingen teweeg zal brengen.

Vertrouwen speelt hierin weer een belangrijke rol. Het is van belang dat burgers vertrouwen hebben in de organisatie die de dienst levert (Schaupp et al., 2010). Het gaat hierbij om de overtuiging dat organisaties in staat zijn om (elektronische) diensten effectief te leveren (Schaupp et al., 2010). In e-government gaat het met betrekking tot dit concept om de reputatie van de organisatie (Schaupp et al., 2010) en heeft het betrekking op de mate waarin men vindt dat een organisatie eerlijk en betrokken is. Burgers zullen eerder gebruik maken van diensten waarvan de organisaties die ermee gemoeid zijn een goede reputatie hebben (Schaupp et al., 2010).

Vanuit psychologisch en sociologisch standpunt komt vertrouwen voort uit socialisatieprocessen. Hierdoor hebben burgers in meer of mindere mate de neiging om anderen te vertrouwen (McKnight et al., 1998). Hierbij wordt een onderscheid gemaakt tussen het oorspronkelijke vertrouwen enerzijds en het aanhoudende vertrouwen anderzijds (McKnight et al., 1998). Oorspronkelijk vertrouwen komt voort uit psychologische disposities (zoals de neiging om anderen te vertrouwen), sociale normen, persoonskenmerken of andere cognitieve processen (Warkentin et al., 2002). Aanhoudend vertrouwen put meer uit vertrouwen in het proces, wat gebaseerd is op eerdere ervaringen (Warkentin et al., 2002).

Het is echter de vraag of het vertrouwen in de stakeholders binnen dit onderzoek daadwerkelijk voortkomt uit het proces, omdat mensen hoogstwaarschijnlijk niet veel directe ervaringen hebben met de politie, brandweer of ziekenhuis. Vertrouwen in hulpverleners en de politie zou daarmee niet zozeer betrekking hebben op het functioneren, maar eerder op de functie die zij in de samenleving bekleden: om er voor je te zijn indien een noodsituatie zich voordoet (Smeets & Baars, 2016).

Onderzoek naar vertrouwen van burgers in bepaalde beroepen, laat zien dat Nederlanders veel vertrouwen hebben in de brandweer (GfK Verein, 2018). Ook medisch personeel komt hoog uit de bus (GfK Verein, 2018). Politiemannen en -vrouwen krijgen nog steeds veel vertrouwen, maar minder dan de brandweer of het medisch personeel (GfK Verein, 2018). De *Global Trustworthiness Index* van IPSOS (2021), waarin de

brandweer niet meegenomen wordt, laat voor Nederland met betrekking tot medisch personeel en politie dezelfde tendens zien.

2.4.3 Type data

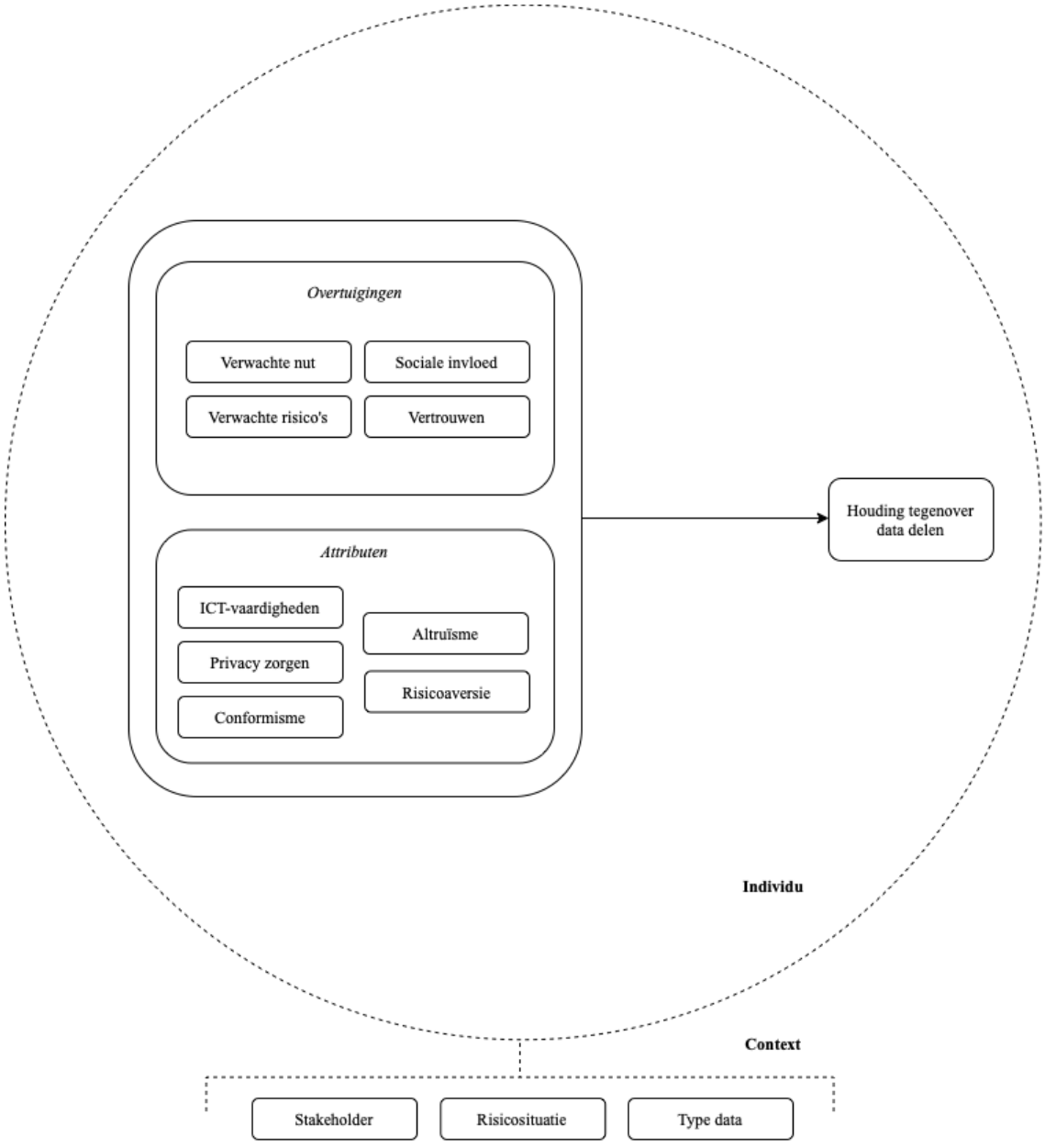
In navolging van de contextuele integriteitstheorie van Nissenbaum (2009) kunnen verwachtingen over het beoogde gebruik van data, afhankelijk van wie het vraagt, ook verschillen per type data (Struminskaya et al., 2020). Deze verschillende verwachtingen kunnen een effect hebben op de houding van iemand tegenover het delen van data. Eerder onderzoek toonde al aan dat het nodig is om een onderscheid te maken tussen de verschillende type data op basis van de gevoeligheid ervan (Malhotra et al., 2004; Li et al., 2011; Rohm & Milne, 2002). Volgens communicatie privacy management theorie zullen individuen verschillende grenzen en regels toepassen in hun besluiten om data te delen afhankelijk van het type data dat gevraagd wordt (Petronio & Durham, 2008). Regels omtrent het delen van data zouden veranderen op een manier dat naarmate het risico in verband met de te delen data toeneemt, de kans groter wordt dat deze niet gedeeld wordt (Metzger, 2007).

Malhotra et al. (2004) toonde al aan dat gevoelige data zorgt voor een verhoogde risicoperceptie. Dit doordat de mogelijke negatieve gevolgen van het delen van gevoeligere data groter kunnen zijn (Anderson & Agarwal, 2011). Bereidheid om data te delen lijkt over het algemeen hoger te zijn wanneer het gaat om anonieme data (Ackermann et al., 2021, Revilla, 2019), mogelijk doordat anonieme data als minder gevoelig worden beschouwd.

2.5 Conceptueel model

Nu zijn de verschillende theoretische invalshoeken besproken. Deze leiden tot het conceptuele model zoals te vinden op de volgende pagina. In dit model worden twee dingen meegenomen die voortkomen uit de rationele en meer irrationele theorieën, namelijk de individuele overtuigingen (paragraaf 2.2) en attributen (paragraaf 2.3). De contextuele factoren die in voorgaande paragraaf 2.4 zijn besproken, hangen mogelijk wel samen met de houding omtrent data delen. Doordat we deze niet kunnen toetsen, zullen deze in het model niet meegenomen worden als factoren die een directe invloed hebben op de houding. In plaats daarvan worden ze hierin opgenomen als factoren die kunnen samenhangen met het besluitvormingsproces op het individuele niveau.

Figuur 1. Conceptueel model



3. Data en methoden

In dit hoofdstuk zal allereerst de gekozen onderzoeksopzet besproken worden. Vervolgens zal de dataverzamelingsmethode uiteengezet worden, als ook de operationalisering van de gebruikte variabelen en de validiteit en betrouwbaarheid van deze variabelen en de steekproef. Tot slot zal een beschrijving gegeven worden van de analysetechniek.

3.1 Onderzoeksopzet

Het onderzoek is deductief van aard. Hiervoor is gekozen omdat al veel theorieën bestaan over het delen van data. Met deductief onderzoek kunnen de hypothesen die hieruit voortvloeien getoetst worden. De theorieën die zijn gebruikt voor het ontwikkelen van de hypothesen gingen doorgaans over andere situaties en systemen. Beslissingen omtrent het delen van data zijn situationeel en afhankelijk van het doel en de context (Urbonavicius et al., 2021). Doordat nog relatief weinig bekend is over de factoren die mogelijk van invloed zouden zijn op het delen van data met een digitaal calamiteitensysteem, proberen we middels deze studie te onderzoeken of voor een calamiteitensysteem dezelfde patronen ontdekt kunnen worden.

Aan de hand van de bestaande theorie en eerder onderzoek, is door middel van literatuurreview een survey opgesteld (zie bijlage 1 voor alle items). Surveyonderzoek is bij uitstek geschikt voor deductief, toetsend onderzoek doordat het een efficiënte manier is om een grotere hoeveelheid respondenten te bereiken. De onafhankelijke variabelen bestaan uit directe vragen, veelal meerdere items waaruit schalen geconstrueerd kunnen worden. Om houdingen omtrent het delen van data inzichtelijk te krijgen, zijn in totaal vier vignetten opgesteld. Er is gekozen voor het gebruik van vignetten in plaats van directe vragen vanwege drietal redenen. Allereerst wordt op deze manier de kans op sociaal wenselijke antwoorden verminderd. Ten tweede kunnen vragen in een bepaalde context en voor een bepaalde situatie gesteld worden, wat ertoe leidt dat de omstandigheden waarbinnen data gedeeld kan worden, beter gecontroleerd kunnen worden. Daarbij vergroot het de interne validiteit van de uitkomstmaat (houding tegenover het delen van data), doordat respondenten zich een betere voorstelling kunnen maken van een concrete situatie die voor hen geschetst wordt (Wallander, 2009). De vignetten en operationaliseringen zullen later in dit hoofdstuk uitgebreider besproken worden.

3.2 Steekproef

Het digitaal calamiteiten systeem wordt ontwikkeld voor het Erasmus MC, een ziekenhuis in Rotterdam wat onderdeel is van een pilot. Om die reden zijn data voor dit onderzoek verzameld

onder studenten en medewerkers van het Erasmus MC. Vanuit ethische overwegingen zijn bezoekers van het Erasmus MC niet meegenomen. In plaats daarvan is besloten bezoekers fictief te bevragen. Dit betekent dat data zijn verzameld onder mogelijke bezoekers van een willekeurig ziekenhuis.

Alle respondenten dienden 18 jaar of ouder te zijn. De data zijn verzameld tussen 5 mei en 20 juni door middel van *convenience sampling*. Allereerst zijn vanaf 5 mei mogelijke bezoekers benaderd. Daarna zijn bachelor- en masterstudenten Geneeskunde op 30 mei via mail benaderd om de online enquête in te vullen. Op 8 juni is naar hen een herinnering verstuurd. Op dezelfde data is de survey onder medewerkers verspreid via de online communicatiekanalen van het Erasmus MC.

In totaal zijn 529 mensen aan de survey begonnen. Hiervan hebben 236 respondenten (44,61%) de totale survey ingevuld. De steekproef is gecheckt op missende waarden en outliers, Eén respondent had bij leeftijd een range (40-45) ingevuld. Hiervoor is de middelste waarde (43) gepakt. Verder had één respondent een missende waarde op leeftijd en een andere respondent had een leeftijd van 101 jaar, wat onwaarschijnlijk is. Voor beide respondenten is de gemiddelde leeftijd ingevuld die hoort bij de rol die zij vervulden (i.e. medewerker, student, bezoeker).

3.2.1 Externe validiteit en betrouwbaarheid steekproef

Doordat gebruik is gemaakt van convenience sampling, is de representativiteit van de data en daarmee de externe validiteit lager. Zo is de sample relatief hoogopgeleid. Sommige onderzoeken laten zien dat lager opgeleiden minder bereid zijn om hun data te delen (Wenz et al., 2017; Robinson, 2017). De gehele sample is daarnaast relatief jong, wat te wijten is aan de gemiddelde leeftijd van de bezoekersgroep. Deze ligt op 31 jaar. Eerder onderzoek laat geen eenduidig beeld zien over een effect van leeftijd op het delen van data.

In tabel 1 op de volgende pagina zijn de percentages per rol weergegeven in de populatie en binnen de steekproef. Hieruit is op te maken dat de gemiddelde leeftijd voor de niet-medische medewerkers wat hoger ligt in de steekproef (45 jaar tegenover 39 in de populatie). Deze groep is tevens ondergerepresenteerd. Bachelorstudenten hebben ruimschoots meer de survey ingevuld en zijn daarmee overgerepresenteerd. Hetzelfde geldt voor medische medewerkers en masterstudenten, hoewel het verschil hiervoor wat kleiner is. Voor de niet-medische medewerkers en de masterstudenten zijn de mannen overgerepresenteerd in de steekproef.

Daarbij konden mensen zelf kiezen of ze meededen aan het onderzoek. Hierdoor en door de manier waarop de vragenlijst is verspreid, kan sprake zijn van zelfselectie. Degenen die meer vertrouwen hebben in de organisatie die het deel-verzoek uitdraagt (in dit geval het ziekenhuis), zullen eerder geneigd zijn de enquête in te vullen. Dit kan ervoor zorgen dat de houding tegenover het delen van data positiever is dan normaliter het geval zou zijn. Door de zelfselectie en convenience sampling kunnen bepaalde (sub)groepen onder- of overgerepresenteerd zijn, zoals hierboven is aangestipt. Vanwege de mogelijke bias die hiermee gepaard gaat, kunnen de resultaten niet gegeneraliseerd worden naar de grotere populatie.

Hoewel de mate waarin men bereid is om zijn/haar data te delen niet generaliseerbaar is naar de volledige Nederlandse populatie, kan wel gekeken worden naar de relatieve effecten van de verschillende noodsituaties in de vignetten ten opzichte van elkaar, wat ook een belangrijk aandachtspunt is binnen deze studie.

Tabel 1. Representativiteit steekproef

	% in populatie	**% in steekproef**	**± leeftijd in populatie**	**± leeftijd in steekproef**
Medisch	11,43	17,89	39	40
Niet-medisch	74,13	46,32	39	45
Bachelor	7,27	22,63	21	20
Master	7,17	13,16	25	24

3.3 Operationalisering

Hieronder wordt besproken hoe de variabelen zijn geoperationaliseerd. Alle items, inclusief degenen die uiteindelijk niet meegenomen worden in de analyses, zijn te vinden in bijlage 1.

3.3.1 Vignetten afhankelijke variabelen

De vier vignetten verschilden in a) het type noodsituatie en b) de nooddienst die opgeroepen werd voor de betreffende noodsituatie. Aangezien het nog onduidelijk was om welke type data het precies zou gaan, is niet gedifferentieerd naar het type data maar gaan alle vignetten over anonieme data. Bovendien zou het toevoegen van verschillende type data in de vignetten leiden tot een te grote differentiatie tussen de vignetten en kan het toevoegen van verschillende type data zorgen voor een minder heldere meting. De vignetten zijn te vinden in tabel 2 op de volgende pagina.

Respondenten werd gevraagd om, mocht dezelfde situatie zich voordoen, aan te geven in welke mate (0: helemaal mee oneens – 4: helemaal mee eens) hij of zij net zoals de persoon

in het vignet zou handelen. Hierbij ging de persoon in het vignet altijd over tot het delen van zijn of haar anonieme data. Om toch te kunnen bekijken of er verschil zou zijn in de houding ten opzichte van data delen tussen anonieme en persoonlijke data, werd daarna nog aan de respondenten gevraagd of men ook zijn/haar data zou delen als het persoonlijke data betrof.

Zodat bekeken kan worden in hoeverre de vignetten ook realistisch geacht werden door respondenten, is aan hen per situatie gevraagd of zij het realistisch vonden. Dit is middels twee vijfpunt Likertschaal items bevraagd. Per vignet is gekeken naar het gemiddelde van deze twee items, om zo de mate van realisme te beoordelen. De betrouwbaarheid van de vignetten zijn, met een Cronbach's Alpha van tenminste 0,859, goed. Tevens waren de scores voldoende hoog (bijlage 2), waardoor is besloten om alle vignetten mee te nemen in de analyses.

Tabel 2. Vignetten gebruikt in studie

Vignet	**Tekst**
Directe noodsituatie	Emma staat in de apotheek van het Erasmus MC om medicatie op te halen. Voordat ze aan de beurt is vindt er een overval plaats en wordt de apotheker door de overvaller onder schot gehouden. De politie en de ME worden ingezet. Naast Emma zijn er nog 11 andere bezoekers in de apotheek. Emma vindt het een goed idee om haar data te delen met het 'calamiteiten management systeem' omdat ze denkt dat het zal helpen met het oplossen van de situatie.
Dreiging van noodsituatie	Volgens een woordvoerder van de gemeente Rotterdam, die spreekt namens de burgemeester, politie en Openbaar Ministerie, is er informatie binnengekomen over een dreiging tegen een of meerdere personen binnen het Erasmus MC. Bob merkt dat rondom het ziekenhuis veel politie aanwezig is. Het lijkt Bob een goed idee om uit voorzorg zijn data te delen met het 'calamiteiten management systeem'.

Collectieve nood	Laila is als verpleegkundige aan het werk in het Erasmus MC wanneer ze hoort dat op de kinderafdeling brand is uitgebroken. Ze ziet de brandweer arriveren, welke meteen begint met het ontruimen van de afdeling. Hoe groot de brand is en hoe veel kinderen op de afdeling liggen, is nog onduidelijk. Wel is er rookontwikkeling ontstaan die zich inmiddels via de schachten verspreid naar andere afdelingen van het ziekenhuis. Laila is bezorgd over de situatie en vindt het een goed idee om haar data te delen met het 'calamiteiten management systeem'.
Individuele nood	Kevin is op het toilet van het Erasmus MC als een patiënt onwel wordt. Kevin ziet dit gebeuren en bedenkt zich dat er zo snel mogelijk iemand moet komen om de man te hulp te schieten. In de hoop dat de situatie sneller opgelost kan worden, lijkt Kevin het een goed idee om zijn data te delen met het 'calamiteiten management systeem'.

3.3.2 Schaalconstructie te gebruiken variabelen

Factoranalyse

Op basis van factoranalyse (bijlage 3) is eventuele overlap tussen items zo veel mogelijk uitgesloten en is bekeken of de items daadwerkelijk onder het construct vallen wat ze horen te meten. De Kaiser-Meyer-Olkin[1] maat was 0,836 en ligt daarmee boven het minimum van 0,6. Om ervoor te zorgen dat een hogere score staat voor een hogere mate van het te meten construct, zijn voor conformisme twee en voor risicoaversie één item gehercodeerd.

Respondenten konden per vignet een indicatie geven van hun houding tegenover data delen voor zowel niet herleidbare, anonieme data als herleidbare, persoonlijke data. Doordat de items over herleidbare, persoonlijke data de factoranalyse verstoorde, is besloten om deze items weg te laten. Alle communaliteiten zijn hoog genoeg, maar drie items (autonomie5, conformisme5 en zelfredzaamheid1) zijn niet meegenomen in de uiteindelijke factoranalyse doordat de variabelen op het verkeerde construct laadde. Hierna laat de factoranalyse met varimax rotatie een simpele structuur zien.

[1] Een statistische maat die bepaald hoe geschikt de data is voor het uitvoeren van een factoranalyse.

Op basis van de overige items en factorladingen worden schalen geconstrueerd. De items die aanvankelijk apart onder autonomie en privacy vielen, laadde in de factoranalyse onder hetzelfde construct. Besloten is om deze samen te nemen in een variabele die de privacy zorgen van respondenten meet. Hetzelfde geldt voor vertrouwen in de technologie van een digitaal calamiteiten systeem en vertrouwen in het internet; deze vragen worden samengevoegd tot een schaal die algemeen technologisch vertrouwen meet.

Het vertrouwen in de politie en de brandweer laadde ook op hetzelfde construct. Toch is ervoor gekozen om deze als aparte schalen in de analyse op te nemen, omdat volgens eerder onderzoek een verschil is in het vertrouwen dat men heeft in de politie en in de brandweer (GfK Verein, 2018; IPSOS, 2021). Tevens zou het vertrouwen in nooddiensten gebaseerd zijn op de functie die zij in de samenleving bekleden (Smeets & Baars, 2016). Hoewel beiden als hulpverleners aangeduid kunnen worden, is de taak die zij hebben en de functie die ze bekleden binnen de samenleving anders van aard.

Tot slot zijn de verwachte risico's van data delen apart bevraagd voor anonieme en persoonlijke data. Omdat bij het samenstellen van de afhankelijke variabele besloten is om alleen in te gaan op de houding omtrent data delen in het geval van niet herleidbare, anonieme data, is besloten om de items die ingaan op de verwachte risico's van het delen van persoonlijke data (item 4 tot en met 6) weg te laten.

Betrouwbaarheid

Voor alle te construeren schalen is gekeken naar de betrouwbaarheid. Voor de variabele die het verwachte nut dient te meten, stijgt de Cronbach's Alpha van 0,831 naar 0,873 als het eerste item niet meegenomen wordt in de uiteindelijke schaal. Ondanks dat het UTAUT-model bestaat uit veelvuldig gevalideerde schalen, wordt besloten om dit item te verwijderen. Hiervoor is gekozen omdat dit item ingaat op het verwachte nut van een digitaal calamiteit systeem in iemand zijn of haar dagelijks leven. Aangezien de situaties waarbij een digitaal calamiteiten systeem ingezet moet worden relatief zelden voorkomen, is deze vraag mogelijk minder gepast gezien het doel van een digitaal calamiteiten systeem. Voor sociale invloed zou de Cronbach's Alpha stijgen van 0,795 naar 0,805 als het eerste item niet meegenomen zou worden. Dit is niet gedaan omdat deze minimale stijging niet opweegt tegen het mogelijke verlies van inhoudsvaliditeit.

Verder wordt op basis van de betrouwbaarheidsanalyse bij altruïsme het derde en vierde item uit de schaal weggelaten. De Cronbach's Alpha stijgt in dit geval van 0,697 naar 0,774. Voor zelfredzaamheid en conformisme gaat er ook een item uit (respectievelijk item 2 en 4).

Voor de overige schalen is, indien sprake was van een stijging van de Cronbach's Alpha, een afweging gemaakt tussen een verhoging van de betrouwbaarheid versus de inhoudsvaliditeit van het construct. Zo zou voor het algemene technologische vertrouwen verwijdering van het vierde item leiden tot een lichte toename van de betrouwbaarheid (0,915 naar 0,920). Deze kleine stijging woog in dit geval niet op tegen het verlies aan inhoudsvaliditeit. Uiteindelijk zijn restrictieve somschalen geconstrueerd voor 17 variabelen (n items): vier variabelen voor de houding tegenover het delen van anonieme data (3 items per vignet), het verwachte nut (3), sociale invloed (3), verwachte risico's (3), vertrouwen in een digitaal calamiteiten systeem (4), algemeen technologisch vertrouwen (8), vertrouwen ziekenhuis (4); vertrouwen brandweer (4); vertrouwen politie (4); vertrouwen overheid (4); privacy zorgen (6); altruïsme (2); conformisme (4); risicoaversie (6); zelfredzaamheid (2). ICT-vaardigheid wordt ook meegenomen als afhankelijke variabele in de analyses. Deze moesten respondenten zelf beoordelen op een schaal van beginner (0) tot expert (4). De Cronbach's Alpha van alle geconstrueerde variabelen zijn te vinden in tabel 3 (pagina 37).

3.3.3 Controlevariabelen

Om voor geslacht, opleidingsniveau en de rol die men in een ziekenhuis vervult te kunnen controleren in de analyses, zijn dummyvariabelen aangemaakt. In de analyses zijn mannen, de opleidingscategorie midden en niet-medisch medewerker de referentiecategorie. Tevens wordt gecontroleerd voor leeftijd en eerdere negatieve privacy ervaringen. Voor deze laatste variabele konden respondenten op een vijf-puntsschaal item aangeven hoe vaak zij slachtoffer waren geweest van een ongepaste inbreuk op hun privacy. Respondenten hadden niet vaak een dergelijke ervaring meegemaakt. Om deze reden zijn de laatste drie categorieën samengevoegd tot de categorie regelmatig t/m vaak (3). In tabel 3 op de volgende pagina zijn de beschrijvende statistieken van alle variabelen te vinden.

Tabel 3. Beschrijvende statistieken en betrouwbaarheid schalen

	Frequentie of gemiddelde (SD)	**Cronbach's Alpha (*n* items)**
Afhankelijke variabele		
Directe noodsituatie (0 – 4)	2,20 (1,13)	0,981 (3)
Dreiging van noodsituatie (0 – 4)	2,70 (1,12)	0,980 (3)
Collectieve nood (0 – 4)	2,79 (1,03)	0,965 (3)
Individuele nood (0 – 4)	2,75 (0,98)	0,927 (3)
Onafhankelijke variabelen		
Verwachte nut (0 – 4)	3,11 (0,73)	0,873 (3)
Sociale invloed (0 – 4)	2,53 (0,78)	0,795 (3)
Verwachte risico's (0 – 4)	1,89 (0,80)	0,829 (3)
Vertrouwen DCS (0 – 4)	3,01 (0,81)	0,910 (4)
Vertrouwen technologie (0 – 4)	2,06 (0,80)	0,918 (8)
Vertrouwen ziekenhuis (1 – 4)	2,81 (0,64)	0,864 (4)
Vertrouwen brandweer (1,50 – 4)	3,07 (0,57)	0,865 (4)
Vertrouwen politie (0 – 4)	2,71 (0,75)	0,898 (4)
Vertrouwen overheid (0 – 4)	1,92 (0,83)	0,896 (4)
Privacy zorgen (0,14 – 4)	2,36 (0,77)	0,891 (6)
Altruïsme (1 – 4)	3,00 (0,62)	0,774 (2)
Conformisme (0,50 – 4)	2,23 (0,73)	0,847 (4)
Risicoaversie (0,67 – 3,67)	2,25 (0,66)	0,826 (6)
ICT-vaardigheden (0 – 4)	2,08 (1,08)	
Controlevariabelen		
Zelfredzaamheid (0 – 4)	2,55 (0,73)	0,723 (2)
Negatieve ervaringen (0 – 2)	0,70 (0,58)	
Leeftijd (18 – 88)	34,69 (14,90)	
Geslacht		
Man	44,5%	
Vrouw	52,5%	
x	3,0%	
Opleidingsniveau		
Midden	33,9%	
Hoog	66,1%	
Rol		
Medisch medewerker	14,4%	
Niet-medisch medewerker	37,3%	
Bachelorstudent	18,2%	
Masterstudent	10,6%	
Bezoeker	19,5%	

Bron: DE-RISC enquête 2022, N=236

3.4 Analysetechniek

De hypothesen zullen getoetst worden door middel van multivariate regressieanalyse. Aan de hand van deze analyse kan nagegaan worden of en in welke mate factoren een effect hebben op het delen van data in een bepaalde noodsituatie. Doordat de andere variabelen die in regressieanalyse meegenomen worden constant blijven, kan nagegaan worden of een effect ook daadwerkelijk toegeschreven kan worden aan een bepaalde variabele. Op deze manier kan gecontroleerd worden voor relevante kenmerken en kunnen mogelijke effecten beter ingeschat worden.

Om uit te sluiten dat de variabelen in de regressieanalyse niet te veel met elkaar correleren, zijn de VIF-waarden opgevraagd. Deze en bijbehorende correlaties zijn te vinden in bijlage 4. De VIF-waarden behoren tenminste onder de 4 te liggen. Alle variabelen voldoen hieraan. Met behulp van onder andere een Q-Q plot is bekeken of de standaardfout normaal verdeeld is. Dit is het geval. Tevens mag er voor regressieanalyse geen sprake zijn van homoscedasticiteit (i.e. wanneer de variantie van een of meerdere onafhankelijke variabelen gelijk is voor meerdere categorieën van die variabele). Ook aan deze assumptie wordt voldaan, waardoor verdergegaan kan worden met de multivariate regressieanalyses.

4. Resultaten

In dit hoofdstuk zullen beknopt de resultaten besproken worden. Allereerst wordt gekeken naar de samenhang tussen de context en data delen. Hierbij zal ook ingegaan worden op hoe positief de houding is om data te delen voor de verschillende vignetten. Daarna zal ingegaan worden op de resultaten van de regressieanalyse. Model 0 bevat telkens alleen de afhankelijke- en controlevariabelen. In model 1 worden de onafhankelijke variabelen meegenomen. In totaal zullen deze modellen vijf keer gedraaid worden: een keer voor elke noodsituatie en een keer voor alle noodsituaties samen. De tabel met resultaten hiervan zijn te vinden in tabel 4 op pagina 42. Een samenvatting van alle hypothesen en de resultaten hiervan wordt gegeven aan het einde van dit hoofdstuk, in tabel 5.

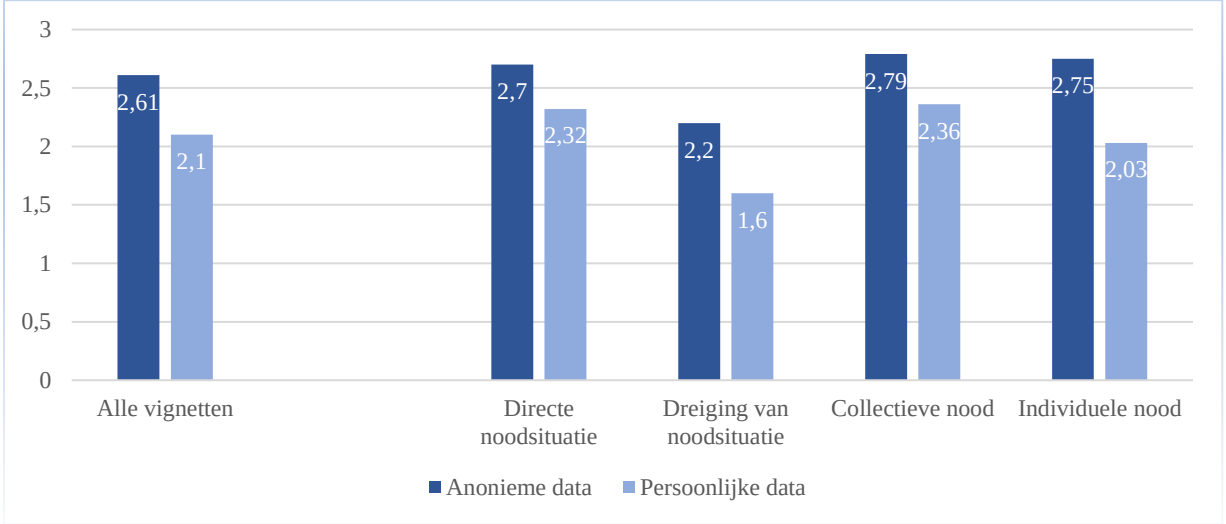
4.1 Samenhang contextuele factoren en de houding tegenover data delen

Om meer duiding aan de context te geven waarbinnen de data gedeeld wordt en hoe deze een samen kunnen hangen met de houding omtrent data delen, worden eerst de beschrijvende resultaten met betrekking tot de contextuele factoren getoond. Daarna zullen de resultaten van de regressieanalyse met de effecten van de individuele factoren besproken worden.

Houding tegenover data delen per noodsituatie

In figuur 2 (volgende pagina) zijn de verschillen in houding tegenover het delen van data voor de verschillende noodsituaties weergegeven. Hierbij geldt dat hoe hoger de score, hoe positiever de houding. In de figuur is te zien dat de gemiddelde houding in het geval van een dreiging van een noodsituatie, collectieve- en individuele nood redelijk dicht bij elkaar liggen. Respondenten staan het meest positief tegenover het delen van data bij een collectieve nood (2,79) en individuele nood (2,74). De houding is het minst positief bij een dreiging van een noodsituatie (2,20). De correlaties tussen de verschillende noodsituaties zijn te vinden in bijlage 5.

Figuur 2. Gemiddelde houding tegenover data delen naar noodsituatie en type data



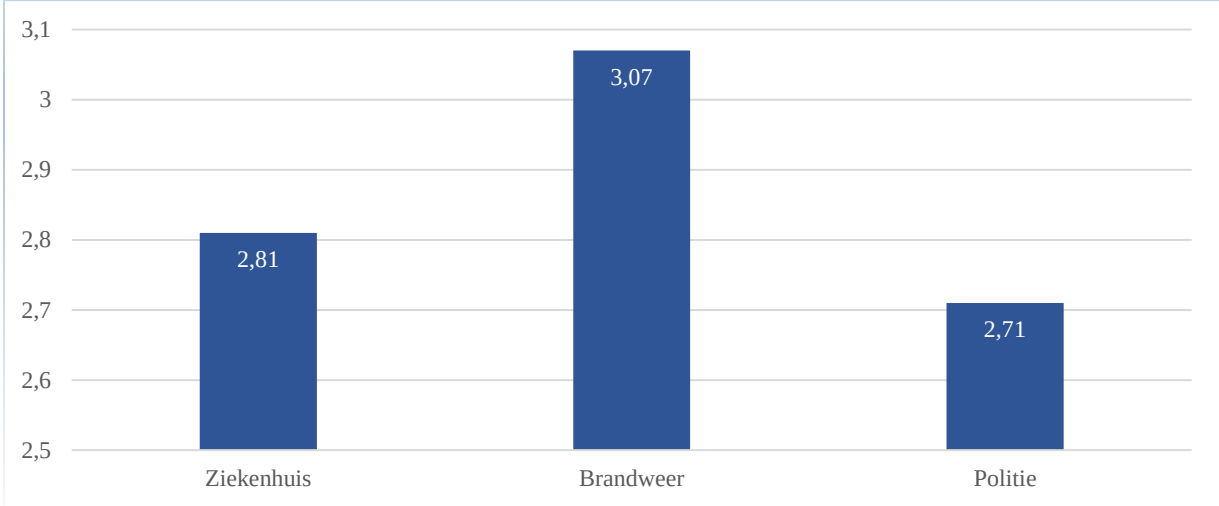
Bron: DE-RISC enquête 2022, N=236

Type data en stakeholder

In bovenstaande grafiek is ook de gemiddelde houding ten opzichte van data delen weergegeven per noodsituatie voor zowel anonieme data als persoonlijke data. Het algemene beeld laat zien dat burgers het meest positief tegenover data delen staan wanneer het anonieme data betreft (2,61 voor alle vignetten tezamen). Voor een directe noodsituatie, collectieve nood en individuele nood zit er weinig verschil in de houding omtrent data delen. Wel staan burgers in het geval van een individuele nood veel minder positief tegenover het delen van hun persoonlijke data dan in het geval van een directe noodsituatie of collectieve nood: 2,03 tegenover 2,32 voor een directe noodsituatie en 2,36 voor een collectieve nood. Het verschil in de houding tussen het delen van anonieme data en persoonlijke data is voor een individuele noodsituatie ook het grootst. Hier is het verschil 0,72, terwijl voor de andere noodsituaties het verschil tussen de 0,40 en 0,50 ligt. Het minst positief staat men tegenover het delen van data in het geval van een dreiging. Voor zowel anonieme data (2,2) als persoonlijke data (1,6) is de houding hiervoor het meest negatief. Het zou kunnen dat burgers deze nood niet als urgent genoeg ervaren om daar hun data voor te willen delen.

Met betrekking tot de verschillende stakeholders, is in figuur 3 af te lezen hoe hoog het vertrouwen per stakeholder is. Deze stakeholders zaten in de verschillende vignetten verwerkt als de nooddienst die opgeroepen werd en dus toegang had tot de data. Zoals verwacht in de theorie, is het vertrouwen veruit het hoogste voor de brandweer (3,07). Het minste vertrouwen hebben burgers in de politie (2,71) en het ziekenhuis neemt een middenpositie in (2,81).

Figuur 3. Vertrouwen per stakeholder



Bron: DE-RISC enquête 2022, N=236

4.2 Belang van individuele factoren voor de houding tegenover data delen

Nu zal ingegaan worden op de samenhang tussen de individuele factoren en de houding omtrent data delen. Op de volgende pagina is de tabel met de effectmaten van de regressieanalyses te vinden per vignet en voor alle vignetten samen. Daarna zullen de resultaten uit deze tabel besproken worden.

Tabel 4. Uitkomsten regressieanalyse

	Directe noodsituatie		Dreiging		Collectieve nood		Individuele nood		Alle vignetten	
	Model 0	Model 1	Model 0	Model 1	Model 0	Model 1	Model 0	Model 1	Model 0	Model 1
Constante	2,578***	0,738	2,678***	1,964*	2,996***	0,882	3,051***	1,306	2,826***	1,222*
Individuele overtuigingen										
Verwachte nut		0,282*		0,368**		0,176		0,350***		0,294***
Sociale invloed		0,091		0,075		0,016		-0,021		0,040
Verwachte risico's		-0,188*		-0,401***		-0,064		-0,124		-0,194**
Vertrouwen DCS		0,064		-0,105		0,161		0,031		0,038
Vertrouwen technologie		-0,132		-0,174		-0,169		-0,100		-0,144
Vertrouwen ziekenhuis		-0,107		0,084		-0,033		-0,132		-0,047
Vertrouwen brandweer		0,368*		-0,138		0,452**		0,523***		0,301**
Vertrouwen politie		-0,023		0,287*		-0,075		0,015		0,051
Vertrouwen overheid		0,102		-0,141		0,046		0,055		0,016
Individuele attributen										
ICT-vaardigheden		0,125*		0,032		0,073		0,040		0,067
Privacy zorgen		-0,126		-0,113		-0,169*		-0,148		-0,139*
Conformisme		-0,069		0,025		0,047		0,096		0,025
Altruïsme		-0,007		0,094		-0,073		-0,394***		-0,095
Risicoaversie		0,061		0,120		0,105		0,164		0,112
Controlevariabelen										
Negatieve ervaringen	-0,072	0,044	-0,138	0,003	-0,095	0,005	-0,014	0,098	-0,080	0,037
Zelfredzaamheid	-0,109	-0,084	-0,120	-0,089	-0,048	0,030	-0,036	0,099	-0,078	-0,011
Leeftijd	0,004	0,009	0,000	0,001	-0,005	0,002	-0,005	-0,002	-0,001	0,003
Geslacht										
Man	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
Vrouw	0,103	0,222	-0,068	-0,101	0,178	0,280*	0,001	0,142	0,054	0,136
x	-1,306**	-0,969*	-1,113**	-0,671	-0,936**	-0,559	-1,119**	-0,668*	-1,119***	-0,717*

	Directe noodsituatie		Dreiging		Collectieve nood		Individuele nood		Alle vignetten	
	Model 0	Model 1	Model 0	Model 1	Model 0	Model 1	Model 0	Model 1	Model 0	Model 1
Opleidingsniveau										
Midden	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
Hoog	0,054	-0,098	-0,238	-0,348*	-0,133	-0,263	-0,058	-0,229	-0,094	-0,235*
Rol										
Medisch	0,002	-0,183	0,095	-0,077	0,176	0,056	0,077	-0,004	-0,088	-0,050
Niet-medisch	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
Bachelorstudent	-0,552*	-0,500*	0,235	0,107	0,165	0,167	0,160	0,212	0,278	0,247
Masterstudent	0,295	0,559*	-0,015	0,146	-0,115	0,118	-0,147	0,171	0,055	0,248
Bezoeker	0,607**	0,560**	0,416*	0,350	0,614**	0,573**	0,124	0,055	0,440**	0,385**
Adjusted R2	0,077	0,177	0,043	0,186	0,088	0,158	0,025	0,204	0,102	0,283

Bron: DE-RISC enquête 2022, N=236
*=p<0,05; **=p<0,01; ***=p<0.001

4.2.1 Individuele overtuigingen

UTAUT-model

Met betrekking tot de factoren uit het UTAUT-model heeft het verwachte nut bij alle noodsituaties behalve voor collectieve nood, een significant en positief effect op de houding tegenover data delen. Dit betekent dat het verwachte nut van een digitaal calamiteiten systeem in het geval van de collectieve noodsituatie die in deze studie is geschetst, namelijk een brand, minder van belang is voor de houding tegenover het delen van data. Voor de overige noodsituaties is het effect het sterkst voor een dreiging (b=0,368), gevolgd door individuele nood (b=0,350) en een directe noodsituatie (b=0,282). Voor alle vignetten samen wordt hetzelfde effect gevonden (b=0,294). Dit bevestigt hypothese 1, welke stelt dat naarmate het verwachte nut van een digitaal calamiteiten systeem toeneemt, de houding tegenover het delen van data met het systeem positiever wordt.

De andere factor uit het UTAUT-model die meegenomen is in deze studie, sociale invloed, heeft geen effect op de houding omtrent data delen. Voor zowel ieder vignet individueel als alle vignetten tezamen wordt geen significant effect gevonden. Hypothese 2 wordt hierdoor niet ondersteund: er bestaat in deze casus geen verband tussen sociale invloed en de houding om data te delen.

Verwachte risico's

Voor een collectieve- en individuele nood hebben de verwachte risico's geen effect op de houding tegenover het delen van data. Een verklaring hiervoor zou kunnen liggen in het relatief sterke significante effect van vertrouwen in de brandweer in het geval van deze situaties. Dit is gecontroleerd door hetzelfde model opnieuw te draaien zonder vertrouwen in de brandweer. Als het vertrouwen in de brandweer leidt tot minder verwachte risico's, zou het weglaten van deze variabele leiden tot een significant effect van verwachte risico's. Voor individuele nood wordt inderdaad gevonden dat het vertrouwen in de brandweer, naast een effect op de houding om data te delen, ook zijn uitwerking heeft op de verwachte risico's: na het weglaten van het vertrouwen in de brandweer, hebben verwachte risico's een negatieve invloed op de houding ten opzichte van data delen. Dat geeft ondersteuning voor wat in de theorie is geschetst: vertrouwen kan risico's verminderen doordat het onzekerheden over het handelen en angsten over de te vertrouwen organisatie (i.e. gedragsonzekerheid) tot op zekere hoogte wegneemt. Dit vinden we echter niet voor collectieve nood: hier lijken andere mechanismen te werken.

Voor het eerste (directe noodsituatie) en tweede vignet (dreiging van een noodsituatie) werd wel een significant effect gevonden: hoe meer risico's, hoe minder positief de houding. De verwachte risico's lijken voornamelijk belangrijk te zijn bij een dreiging van een noodsituatie (b=-0,448). Bij een dreiging kan de burger de verwachting hebben dat data voornamelijk met de politie gedeeld wordt. Het effect van het vertrouwen in de politie op de houding om te delen is over het algemeen lager. Mogelijk vallen de verwachte risico's hierdoor hoger uit. Er is immers een minder groot effect van vertrouwen wat deze risico's zou kunnen compenseren.

In het geval van een directe noodsituatie is de sterkte van het effect kleiner (b=-0,188). Een verklaring hiervoor kan gezocht worden binnen *de prospect theory*: mensen zouden meer risicozoekend gedrag vertonen wanneer de noodsituatie urgenter is (McDermott et al., 2008). Doordat bij een dreiging minder sprake is van directe nood, zullen burgers meer rationeel de voor- en nadelen, in dit geval de verwachte risico's, tegen elkaar afwegen. Er wordt dan meer waarde toegekend aan de directe, verwachte risico's van het delen van data tegenover de eventuele risico's welke gepaard zouden gaan met de dreiging van een noodsituatie. Voor alle vignetten tezamen wordt ook een significant effect gevonden (b=-0,194). Hypothese 3, waarbij gesteld wordt dat hoe meer risico's men verwacht bij het delen van zijn/ haar data, hoe negatiever de houding, wordt grotendeels ondersteund.

Vertrouwen

Met betrekking tot de factor vertrouwen is naar 1) het vertrouwen in de organisaties en 2) het vertrouwen in de technologie gekeken. Voor alle vignetten is zowel het vertrouwen in een digitaal calamiteiten systeem (hypothese 8) als het algemene technologische vertrouwen (hypothese 9) geen bepalende factor voor de houding ten opzichte van data delen. Deze hypothesen worden daarom verworpen.

Met betrekking tot het vertrouwen in organisaties komt uit de analyse naar voren dat vertrouwen in de overheid (hypothese 4) en het ziekenhuis (hypothese 5) geen effect heeft op de houding ten opzichte van data delen. Vertrouwen in de brandweer heeft wel een positief effect. Voor vignet een, drie en vier wordt een significant effect gevonden. Het effect is het hoogst voor individuele nood (b=0,523), gevolgd door collectieve nood (b=0,452) en een directe noodsituatie (b=0,368). Ook voor alle vignetten samen wordt een significant effect gevonden (b=0,395). Op basis hiervan kunnen we hypothese 6 aannemen: hoe hoger het vertrouwen in de brandweer, hoe positiever burgers staan tegenover het delen van data met een digitaal calamiteiten systeem.

Alleen voor een dreiging van een noodsituatie heeft het vertrouwen in de brandweer geen significant effect. Voor dit vignet is wel sprake van een significant effect van het vertrouwen in de politie (b=0,287). Dit betekent dat in het geval van een dreiging, een hoger vertrouwen in de politie een positievere houding tegenover het delen van data met zich mee kan brengen. In dit geval was er sprake van een dreiging tegen een of meerdere personen binnen het ziekenhuis; een situatie waar (over het algemeen) de brandweer niet of in mindere mate voor ingezet zal worden, maar de politie wel. Bij de overige drie situaties is het denkbaarder dat de brandweer ingezet zal worden, waardoor het vertrouwen in de brandweer er in die gevallen meer toe doet. Voor de andere vignetten wordt geen significant effect gevonden voor het vertrouwen in de politie. Het vertrouwen in de politie lijkt alleen van belang te zijn in het geval van een dreiging. Een effect in één geval is te weinig om de hypothese mee te bevestigen. Daarom moet hypothese 7, waarin een meer positieve houding wordt verondersteld naarmate men meer vertrouwen heeft in de politie, verworpen worden.

4.2.2 Individuele attributen

ICT-vaardigheden

Uit de analyse blijkt dat ICT-vaardigheden alleen van belang zijn voor de houding om data te delen voor een directe noodsituatie (b=0,125). Hier lijkt het vooral te gaan om de urgentie van de noodsituatie: als je minder ICT-vaardig bent, weet je in noodsituaties minder goed wat mogelijk is waardoor je minder snel kan handelen. De mensen die meer ICT-vaardig zijn, kunnen bij een minder urgente noodsituatie dingen opzoeken of eerder via een andere weg helpen. In het geval van een directe dreiging is deze mogelijkheid er niet of minder, waardoor de ICT-vaardige mensen eerder bereid zijn om snel te handelen door hun data te delen.

Voor de andere drie vignetten wordt geen effect gevonden. Ook voor alle vignetten samen is geen effect gevonden, waardoor we hypothese 10 moeten verwerpen. Op basis van de data kan niet gesteld worden dat hoe beter de ICT-vaardigheden, hoe positiever de houding tegenover data delen met een digitaal calamiteiten systeem.

Privacy zorgen

Voor alle vignetten tezamen hebben privacy zorgen een effect op de houding om data te delen met het systeem (b=-0,139). Gekeken naar de vignetten los, hebben privacy zorgen alleen een significant effect in het geval van collectieve nood (b=-0,169). Het gaat hier om de algemene

neiging van mensen om zich zorgen te maken over hun privacy, maar de context lijkt hier wel de impact van algemene privacy zorgen op de houding tegenover data delen te beïnvloeden. Het zou kunnen dat door de grootte van de noodsituatie burgers meer op hun hoede zijn of meer rekening houden met mogelijke verliezen (i.e. verlies van privacy of controle over je data) die gepaard kunnen gaan met het delen van hun data. Ook voor de algemene houding (alle vignetten samen) geldt dat hoe meer privacy zorgen iemand heeft, hoe minder positief de houding van diegene is. Op basis hiervan wordt hypothese 11 in beperkte mate ondersteund.

Conformisme, altruïsme en risicoaversie

Conformisme en risicoaversie hebben voor alle vignetten individueel als tezamen geen effect op de houding omtrent data delen, waardoor hypothese 12, 13 (tegengestelde hypothesen over conformisme) en 15 verworpen worden. Altruïsme, i.e. de mate waarin iemand onbaatzuchtig handelt en gericht is op het welzijn van anderen, heeft in één geval een effect op de houding over data delen. Alleen bij het vignet waar sprake is van individuele nood, is een significant effect te zien (b=-0,394). In tegenstelling tot wat werd verwacht, betekent dit dat iemand die meer altruïstisch is, negatiever tegenover het delen van data staat in het geval van een individuele nood. Een verklaring hiervoor zou kunnen zijn dat altruïsten denken aan het grotere, maatschappelijke belang en een individuele nood niet urgent genoeg is doordat daar gemakkelijker een andere oplossing voor gevonden kan worden, of een andere oplossing zelfs beter zou kunnen werken voor de noodsituatie die zich voordoet. Hypothese 14 kan hierdoor niet aangenomen worden: voor te weinig vignetten wordt een significant effect gevonden en het significante effect dat wordt gevonden voor individuele nood, wijst de andere richting op dan in eerste instantie werd verwacht.

4.2.3 Controlevariabelen

Met betrekking tot de controlevariabelen blijkt uit de analyse dat degenen die geen geslacht op hebben gegeven of niet binnen de binaire geslachtscategorieën vallen, negatiever staan tegenover het delen van data. Dit was een kleine groep en bestond voornamelijk uit mensen die hun geslacht liever niet wilden zeggen. Daarmee lijkt het logischer te zijn dat zij ook negatiever staan tegenover data delen, doordat zij mogelijk al grotere privacy zorgen hebben en om die reden ook liever hun geslacht privé houden. In collectieve noodsituaties staan vrouwen positiever tegenover het delen van data.

Verder staan hoogopgeleiden over het algemeen negatiever tegenover het delen van data (b=-0,235 voor alle vignetten). Dit is ook het geval wanneer sprake is van een dreiging van een noodsituatie (b=-0,348). Ook zouden bezoekers van een ziekenhuis eerder bereid zijn om hun data te delen, maar dit zou kunnen liggen aan de gemiddeld relatief lagere leeftijd van de bezoekersgroep in de steekproef.

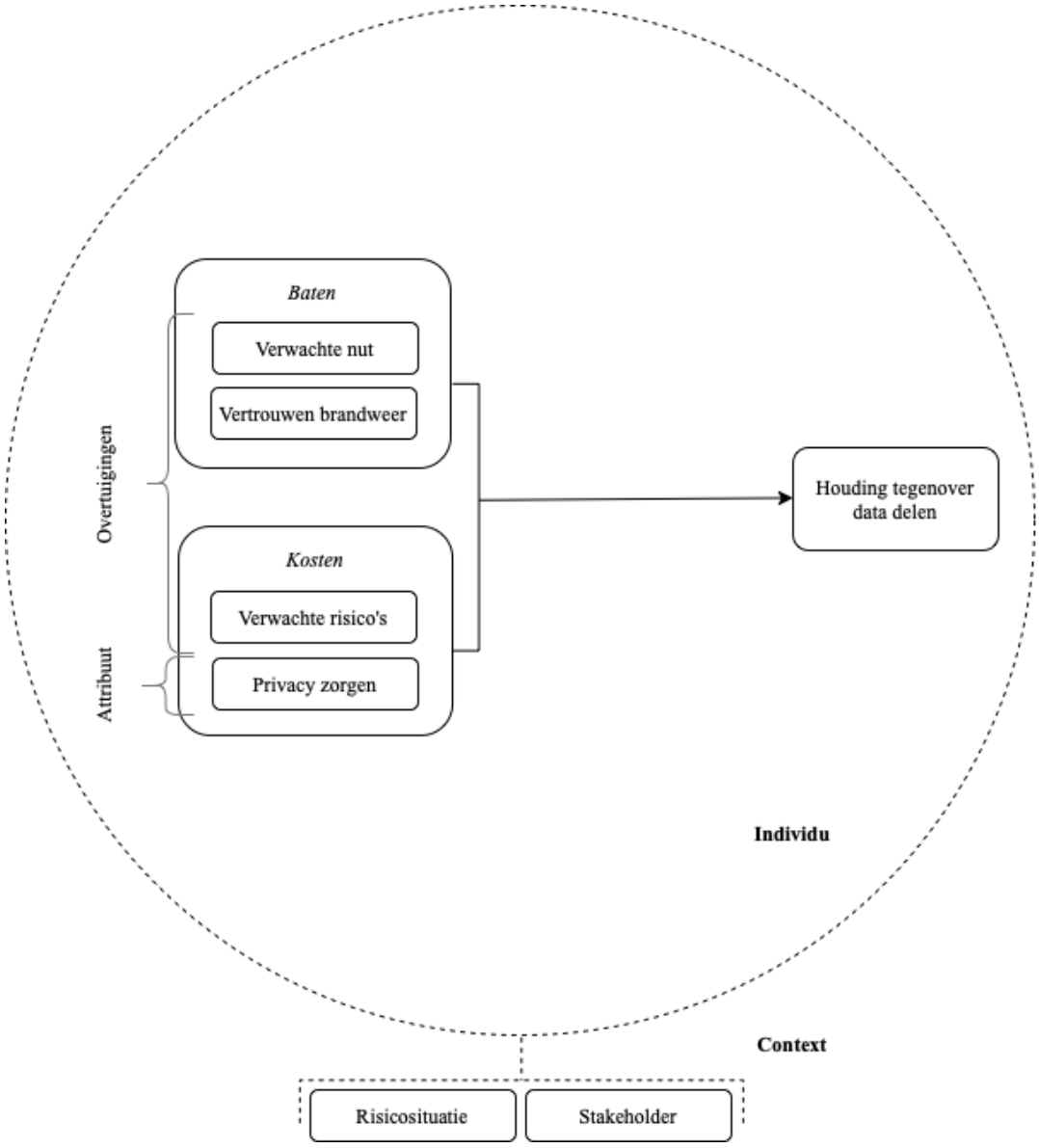
Tabel 5. Resultaten hypothesetoetsing

Hypothesen		**Resultaat**
H1	Verwachte nut → + Houding data delen	Aangenomen
H2	Sociale invloed → + Houding data delen	Verworpen
H3	Verwachte risico's → - Houding data delen	Aangenomen
H4	Vertrouwen overheid → + Houding data delen	Verworpen
H5	Vertrouwen ziekenhuis → + Houding data delen	Verworpen
H6	Vertrouwen brandweer → + Houding data delen	Aangenomen
H7	Vertrouwen politie → + Houding data delen	Verworpen
H8	Vertrouwen systeem → + Houding data delen	Verworpen
H9	Technologisch vertrouwen → + Houding data delen	Verworpen
H10	ICT-vaardigheden → + Houding data delen	Verworpen
H11	Privacy zorgen → - Houding data delen	Aangenomen
H12	Conformeren → + Houding data delen	Verworpen
H13	Conformeren → - Houding data delen	Verworpen
H14	Altruïsme → + Houding data delen	Verworpen
H15	Risicoaversie → - Houding data delen	Verworpen

5. Conclusie en discussie

In deze studie is getoetst of en hoe bepaalde factoren een invloed hebben op de houding van burgers ten opzichte van data delen met een digitaal calamiteiten systeem. Dit is gedaan door allereerst te kijken naar de houding van burgers per noodsituatie en de context waarbinnen data gedeeld wordt. Daarna is dieper ingegaan op de factoren die een invloed hebben op deze houding en de mogelijke verschillen hierin tussen de noodsituaties. Hier komt het onderstaande, nieuwe conceptuele model uit (figuur 4). Deze zal hierna uitgelegd worden.

Figuur 4. Nieuw conceptueel model



5.1 Houding tegenover het delen van data

Over het algemeen lijken burgers positief tegenover het delen van data met een digitaal calamiteiten systeem te staan. Uit de resultaten blijkt dat geen hele grote verschillen zitten tussen de houding om data te delen voor een directe noodsituatie, collectieve nood en individuele nood. Men staat het minst positief tegenover het delen van data bij een dreiging van een noodsituatie. Dit betekent dat vooral de urgentie van de noodsituatie van belang lijkt te zijn voor de houding van burgers om data te delen: hoe urgenter, hoe meer positief men is over het delen van data. De omvang van de noodsituatie lijkt niet van invloed te zijn op de houding.

5.2 De invloed van factoren op de houding

Concluderend kan gesteld worden dat het per noodsituatie verschilt in welke mate individuele factoren een rol spelen in de houding om data te delen. Hieronder zal besproken worden welke factoren van belang zijn, hoe dit verschilt per noodsituatie en mogelijke redenen voor deze verschillen.

Het belang van het verwachte nut

Het verwachte nut van een digitaal calamiteiten systeem is erg belangrijk. Deze factor kwam voort uit het UTAUT-model, waarvoor al veelvuldig is aangetoond dat het een van de belangrijkste factoren is (Venkatesh et al., 2003). Het verwachte nut speelt in het licht van een digitaal calamiteiten systeem vooral mee bij een dreiging of individuele nood, maar ook bij een directe noodsituatie. Opvallend heeft het verwachte nut geen effect op de houding omtrent data delen in het geval van een collectieve nood. Dit staat haaks op de verwachting uit de *prospect theory*: juist in situaties waarbij de dreiging minder groot is in termen van omvang en urgentie, lijkt het verwachte nut er het meest toe te doen.

Mogelijk is de gepercipieerde noodzaak groter om data te delen bij een dreiging of individuele nood, doordat in deze gevallen weinig of geen mensen in de omgeving zijn en omstanders minder snel te hulp kunnen schieten. Dit heet ook wel het omstandereffect (Darley & Latane, 1968): naarmate er meer mensen in de omgeving zijn, wordt de waarschijnlijkheid dat een burger iemand anders in nood helpt kleiner. In tegenstelling tot een dreiging of individuele nood kunnen burgers bij een directe noodsituatie en een collectieve nood de verwachting hebben dat de situatie op een andere manier of door iemand anders opgelost kan worden, bijvoorbeeld doordat eerder hulpverlening ingezet wordt of sneller een alarmcentrale gebeld zal worden. Ingrijpen door de burger zelf wordt dan als minder noodzakelijk beschouwd

en de voordelen van het delen van data met een digitaal calamiteiten systeem lijken minder groot. Ook zullen er in het geval van een collectieve nood veel mensen zijn die hulp nodig hebben, waardoor burgers zich af kunnen vragen waarom het nodig is om data van specifieke personen te verzamelen. Het individu kiest in dit geval voor zichzelf: ze zijn negatiever over data delen en lijken de eigen privacy te willen beschermen.

Verwachte risico's, privacy zorgen en de rol van vertrouwen

Zorgen over het delen van data of privacy blijven in alle gevallen bestaan en spelen een rol in de houding van burgers. Risico's die mensen voorzien wanneer zij hun data delen met het systeem, spelen voornamelijk een rol in een meer en minder urgente noodsituatie. In het geval van een grotere noodsituatie in termen van omvang (i.e. collectieve nood) doen deze verwachte risico's van het systeem (als overtuiging) er minder toe, maar blijven de algemene privacy zorgen die mensen bij voorbaat al hadden (als persoonlijk attribuut), bestaan.

Vertrouwen kan tot op zekere hoogte risico's en zorgen verminderen en is belangrijk voor de manier hoe we over data delen denken. De resultaten onderschrijven de theorieën hierover die stellen dat vertrouwen ervoor zorgt dat mensen ervanuit gaan dat de organisatie zich zal gedragen zoals verwacht (Pavlou, 2003; Gefen, 2000; Luhmann, 1979), waardoor burgers vertrouwen hebben in het handelen van de organisatie (Warkentin et al., 2002) en het daardoor onzekerheden en angsten weg kan nemen (Pavlou, 2003; Bearth & Siegrist, 2020). Dit benadrukt het belang van vertrouwen als veelvuldig onderzocht concept binnen onderzoek naar ICT-diensten.

Verwachte risico's zouden volgens Schaupp et al. (2010) voortkomen uit omgevingsonzekerheid en gedragsonzekerheid. Hoewel omgevingsonzekerheid (over de technologie) niet zozeer een invloed lijkt te hebben op de houding omtrent data delen, lijkt gedragsonzekerheid hier wel belangrijk in. Er zijn aanwijzingen dat vertrouwen in de specifieke organisaties, de politie in het geval van een dreiging en de brandweer in de overige situaties, kan leiden tot een afname in risicopercepties. Daar waar het effect van vertrouwen hoog is, zijn de verwachte risico's niet of minder belangrijk. Voor burgers lijkt het van belang te zijn *met wie* data wordt gedeeld *per noodsituatie* en de resultaten onderschrijven de belangrijke rol die vertrouwen kan spelen in het proces van data delen. Voornamelijk voor het vertrouwen in de brandweer is een belangrijke rol weggelegd. Overeenkomstig met eerder onderzoek (GfK Verein, 2018) blijkt de brandweer van alle hulpverlenende stakeholders ook het meeste vertrouwen te krijgen. De bevinding biedt ondersteuning voor het onderzoek van Carter en Schaupp (2010), waarin zij stellen dat burgers eerder gebruik zullen maken van ICT-diensten

wanneer zij meer vertrouwen hebben in de organisaties die met het systeem gemoeid zijn, en voor de theorie van Nissenbaum (2009) over contextuele integriteit.

Tegelijkertijd lijkt vertrouwen in sommige noodsituaties niet helemaal de verwachte risico's en privacy zorgen, weg te kunnen nemen. Degenen die meer risico's verwachten, blijven een negatievere houding tegenover het delen van data houden. Dit geldt zeker voor een dreiging van een noodsituatie, maar ook voor een directe noodsituatie. Het zou kunnen dat in een bepaalde noodsituatie verwacht wordt dat de betreffende nooddienst minder hulp kan bieden (een brandweer kan minder doen bij een gijzeling dan bij een brand), waardoor het vertrouwen in die nooddienst in mindere mate de risicopercepties kan temperen. Ook een algeheel verminderd vertrouwen in de nooddienst waarmee data gedeeld wordt, zou hierin een rol kunnen spelen. Een andere reden kan zijn dat burgers meer verwachte risico's voorzien, door de manier waarop men verwacht dat de nooddienst te werk zal gaan. Denk aan het gebruik van signaleringsprocedures door de politie in het geval van een dreiging.

Eerder onderzoek liet zien dat individuele overtuigingen, zoals de verwachte risico's en mate van vertrouwen, privacy zorgen kunnen overheersen (Keith et al., 2012; Kehr et al., 2015). Uit de resultaten blijkt dat dit niet altijd het geval hoeft te zijn: algemene privacy zorgen blijven bestaan en hangen samen met een negatievere houding tegenover het delen van data. Situatiespecifiek vinden we dit voor een collectieve noodsituatie. Dit staat haaks op eerder onderzoek van Dinev & Hart (2006). Zij vonden dat privacy zorgen er niet toe deden wanneer mensen een persoonlijk belang bij de situatie hadden. Doordat een collectieve nood veel meer mensen en mogelijk ook jou persoonlijk aangaat, zou de verwachting zijn dat mensen positiever tegenover het delen van data zouden staan. Dit blijkt dus niet zo te zijn. Dit kan wederom liggen aan het omstandereffect: in een situatie waar meer mensen aanwezig zijn, zijn mensen minder positief over data delen en maken zij zich meer zorgen om hun privacy. Gezien het doel van het systeem, kan echter gesteld worden dat het persoonlijk belang in alle situaties gering is, doordat een digitaal calamiteiten systeem meer zit op het maatschappelijk belang.

Daarom zou het kunnen dat, juist door de omvang van een collectieve noodsituatie, burgers zich meer zorgen maken over hun privacy vanwege de grote schaal waarop data verzameld wordt. Zij kunnen daardoor meer zorgen hebben over hoe, wanneer en door wie dit gebruikt zal worden. Interessant zou zijn te achterhalen waar deze privacy zorgen en verwachte risico's vandaan komen en te kijken naar de mogelijke verhoudingen tussen deze privacy zorgen, verwachte risico's en het vertrouwen in organisaties. Het is denkbaar dat algemene privacy zorgen zouden kunnen leiden tot meer verwachte risico's, maar ook tot verminderd vertrouwen in organisaties en/of systemen. Minder vertrouwen kan ook weer leiden tot meer

verwachte risico's. Vertrouwen zou mensen immers een gevoel geven dat de organisatie zou handelen in overeenstemming met de eigen overtuigingen (Warkentin et al., 2002), wat de verwachte risico's kan verminderen (Pavlou, 2003; Bearth & Siegrist, 2020). Uit dit onderzoek weten we niet precies hoe deze factoren elkaar onderling beïnvloeden, maar de resultaten laten zien dat dit per noodsituatie kan verschillen. Door de mechanismen hierachter te achterhalen, kunnen besluitvormingsprocessen beter begrepen worden. Dit kan helpen bij het maken van een aanpak waarmee zorgen zo goed mogelijk weggenomen worden of vertrouwen versterkt. Desalniettemin geven de huidige resultaten ook een aantal aanknopingspunten voor het vormgeven van de besluitvorming omtrent een digitaal calamiteiten systeem en de implementatie hiervan. Hier wordt verder op ingegaan in paragraaf 5.4.

Sociale invloed versus persoonlijke disposities

Een toch wel opmerkelijk resultaat is het effect van altruïsme in het geval van een individuele noodsituatie. Een meer altruïstisch persoon staat in deze situatie negatiever tegenover het delen van data. Het is interessant om te onderzoeken of een dergelijk effect vaker gevonden wordt en zo ja, wat de mogelijke verklaringen hierachter zijn.

Sociale invloed, als andere belangrijke factor uit het UTAUT-model naast het verwachte nut, is niet van belang in de acceptatie van een digitaal calamiteiten systeem. Dit betekent dat mensen zelf aangeven niet te worden beïnvloed door diens sociale kring en wat zij als belangrijk achtten. Dit kan komen door het doel van het systeem. Vanwege de situaties waarbinnen het gebruikt wordt, zouden mensen meer op gevoelens gebaseerde keuzes kunnen maken. Deze zouden rationele factoren kunnen overschrijden (Kehr et al., 2015). Daarbij komt dat, beredeneerd vanuit de *prospect theory,* mensen in mindere mate rationele overwegingen maken als het gaat over keuzes die te maken hebben met bedreigingen voor (het voortbestaan van) de mens.

Welnu, sociale invloed gaat voornamelijk over het conformeren aan en internaliseren van bepaalde waarden. Dit is een rationeel proces. Echter, in een noodsituatie kunnen dit soort rationele processen er niet of minder toe doen. Mensen zullen hierdoor minder ontvankelijk zijn voor de mening van hun omgeving en meer focussen op het gevoel wat zij er zelf bij hebben, waarbij an sich al een bepaalde houding tegenover een digitaal calamiteiten systeem geïnternaliseerd zou kunnen zijn. Interessant is vervolgonderzoek meer te richten op de drijfveren van mensen om data te delen met een digitaal calamiteiten systeem. Enerzijds door voor een breder scala aan persoonskenmerken te kijken welke invloed het heeft op het wel of niet willen delen van data. Hoewel risicoaversie en de mate van conformisme geen effect

hebben op de houding omtrent data delen, laat het effect van altruïsme in het geval van een individuele noodsituatie in ieder geval zien dat bepaalde disposities van personen een rol *kunnen* spelen. Zo zou gekeken kunnen worden in hoeverre burgers het eens zijn met de social responsibility norm; een norm die stelt dat het helpen van anderen belangrijk is. Anderzijds zou, door middel van kwalitatief, inductief onderzoek, dieper ingegaan kunnen worden op de intrinsieke motivatie van mensen, wat een rol kan spelen in het delen van data met een digitaal calamiteiten systeem.

5.3 Theoretische terugkoppeling

Voor de theorie betekent dit dat het verwachte nut, afkomstig uit het UTAUT-model, nog steeds een van de belangrijkste factoren blijft, wat overeenkomt met eerdere bevindingen (Venkatesh et al., 2003). De privacy calculus wordt grotendeels bevestigd en biedt een goede aanvulling om de houding tegenover data delen te kunnen verklaren: ook in het geval van een digitaal calamiteiten systeem lijken mensen de kosten en baten van het delen van data tegen elkaar af te wegen. Hierbij wordt het verwachte nut en het vertrouwen in de brandweer (batenkant) gezet tegenover de risico's en privacy zorgen (kostenkant). Dit geldt voor alle noodsituaties, hoewel de mate waarin de kosten- of batenkant ertoe doet enigszins kan verschillen. Dit sluit aan bij de verwachting van de communicatie privacy management theorie. Situationele factoren, zoals het doel waarvoor data worden gebruikt en de organisatie die een beroep doet op de data, beïnvloeden de manier waarop de kosten en baten afgewogen worden en daarmee de houding van burgers.

Hoewel rationele processen belangrijk zijn, lijkt het een en ander erop te wijzen dat ook irrationele factoren een rol spelen. Mensen lijken in sommige situaties toch meer een beslissing te maken zoals het *risk-as-feelings* perspectief voorschrijft, waardoor meer vanuit emoties of gevoelens gehandeld wordt. Het beeld hierover is echter niet eenduidig en de emoties en persoonlijke ervaringen die ertoe doen verschillen per noodsituatie. De *prospect theory*, waarbij mensen minder rationeel de voordelen en risico's in overweging zullen nemen naarmate de omvang en urgentie van de noodsituatie toeneemt, biedt nauwelijks een verklaring voor deze verschillen. Wel kan de theorie een uitleg geven voor een aantal effecten die überhaupt niet gevonden worden, zoals sociale invloed, en kan het daarmee een interessante theoretische uitgangspositie bieden.

5.4 Praktijkaanbevelingen

De resultaten bieden een aantal aanknopingspunten voor een doelbewuste, legitieme implementatie van een digitaal calamiteiten systeem. Hiervoor dienen de perspectieven en prioriteiten van de burger gecombineerd te worden met het doel van een digitaal calamiteiten systeem, namelijk het waarborgen van de publieke veiligheid. Dit door het tot stand brengen van een nieuw sociaal contract.

Een sociaal contract is een symbolisch contract gebaseerd op een gemeenschappelijke set van principes en waarden (Horn & Kerasidou, 2020). In een onderzoek naar het delen van gezondheidsdata voor het ontwikkelen en verbeteren van nieuwe behandelingen werd ook het belang benadrukt van een sociaal contract (Horn & Kerasidou, 2020), zeker wanneer in het proces van data delen niet direct toestemming wordt gevraagd aan degenen waarvan de data is (Carter et al., 2015). Voor het tot stand brengen van een nieuw sociaal contract, is het belangrijk dat communicatie van de plannen en intenties naar de maatschappij goed wordt vormgegeven. In de context van een digitaal calamiteiten systeem en in het licht van de resultaten betekent dit het volgende:

Allereerst dient in de communicatie en het naar buiten brengen van het systeem, duidelijk de waarde van het systeem aangestipt te worden. Uit de conclusie bleek het verwachte nut van groot belang te zijn voor de houding van burgers om data te delen. Door het systeem als publiek goed neer te zetten en te focussen op een aantal overkoepelende publieke waarden, kan het verwachte nut sterker naar voren komen. Deze waarden dienen in overeenstemming met de verschillende stakeholders en burgers bepaald en vastgelegd te worden, waarbij het algemeen welzijn en collectieve belang nagestreefd wordt.

Ten tweede bleek uit de conclusie dat vertrouwen tot op zekere hoogte verwachte risico's en privacy zorgen kan wegnemen, maar dat dit verschilt per noodsituatie en risico's en zorgen desondanks blijven bestaan. Het volgende wat daarom meegenomen moet worden in een nieuw sociaal contract, is het versterken van vertrouwen en simultaan wegnemen van de verwachte risico's en zorgen die mensen hebben. Dit betekent vastleggen *wat* wordt gedeeld, *wanneer*, met *wie*, voor *hoe lang* en *hoe* dat wordt *vormgegeven*. Het is van belang dat van tevoren duidelijke kaders zijn vastgesteld, omdat op het moment dat data gedeeld worden geen ruimte is om over dit soort zaken na te denken. Door dit vast te stellen, kan meer vertrouwen gecreëerd worden doordat de burger het gevoel krijgt dat naar hun verwachting gehandeld wordt. Dit zal ook de waarde en het verwachte nut van het systeem versterken.

Door middel van de oprichting van een toezichthoudende instantie bestaande uit professionals en burgers, kan toezicht gehouden worden op de werking van het systeem en

gaandeweg het publieke belang in de gaten gehouden worden. Beslissingen die een verandering teweegbrengen in de structuur achter een digitaal calamiteiten systeem en het delen van data hiervoor, zouden gebaseerd moeten worden op de publieke waarden die zijn vastgesteld en op de verwachtingen van burgers. Hierin is een belangrijke rol weggelegd voor de toezichthoudende instantie. Dit is niet alleen belangrijk voor het verankeren van de waarde en het nut van het systeem, maar ook voor het vertrouwen (Putnam, 1992).

Risico's zouden verder aan de voorkant zo veel mogelijk weggenomen kunnen worden door een minimum beveiligingsvereiste te stellen aan alle elektronische systemen via waar de data gedeeld wordt. Daarbij zou een voorlichting gegeven kunnen worden aan degenen met toegang tot de data. Daarna kunnen burgers geïnformeerd worden over de risico's die wel of niet bestaan en de privacyoverwegingen die zijn gemaakt. Ook de uitleg van wet- en regelgeving hierin kan mensen ervan overtuigen dat hun belangen behartigd worden en hun privacy gewaarborgd (Horn & Kerasidou, 2020).

6. Reflectie

Een aantal beperkingen van dit onderzoek dienen in het achterhoofd gehouden te worden. De eerste limitatie is de representativiteit van het sample. Met oog daarop dienen de resultaten met enige voorzichtigheid geïnterpreteerd te worden, doordat deze niet gegeneraliseerd kunnen worden naar de populatie. Een andere limitatie heeft betrekking op de manier waarop de uitkomstmaat is gemeten. Deze wordt ook veel genoemd in ander privacy gerelateerd onderzoek naar het delen van data. Veel onderzoek heeft betrekking op intenties om data te delen (en in dit geval op de houding tegenover data delen) en zegt daarmee niks over het daadwerkelijk delen van data (Keith et al., 2013). Dit is zeker belangrijk met oog op de context waarbinnen een digitaal calamiteiten systeem werkt. Mensen kunnen moeilijk vaststellen wat hun gevoelens en gedrag zullen zijn wanneer een echte noodsituatie zich voordoet. Hierdoor kan een kloof ontstaan tussen het gedrag wat mensen voorspellen en het uiteindelijke, daadwerkelijke deelgedrag (Anderson & Agarwall, 2011). Op deze manier kan een privacy paradox ontstaan, doordat mensen aangeven niet hun data te willen delen, maar uiteindelijk wel hun data zullen willen delen wanneer er echt iets aan de hand is.

Daarnaast was het nog onduidelijk of en zo ja wat voor handelingen mensen moesten uitvoeren om data te delen met het systeem en wat voor data dit precies zouden zijn. Als burgers uiteindelijk bepaalde handelingen uit moeten voeren voor het delen van hun data, dan zou dit veranderingen teweeg kunnen brengen in het deelgedrag. Dit geldt ook voor de soort data. Indien meer bekend over dit soort specificaties van een digitaal calamiteiten systeem, zouden ook deze andere factoren en het effect op het deelgedrag bestudeerd moeten worden.

Ook dient benoemd te worden dat de omgeving waarbinnen een digitaal calamiteiten systeem opereert in dit onderzoek een ziekenhuisomgeving is. Hiervan is bekend dat de mensen redelijk positief staan tegenover data delen, onder andere omdat dit al veel wordt gedaan. Het inzetten van een digitaal calamiteiten systeem binnen een andere omgeving, bijvoorbeeld een commerciële organisatie zoals een evenementenlocatie, kan andere resultaten met zich meebrengen (zie ook Anderson & Agarwall, 2011). De resultaten uit dit onderzoek kunnen daardoor niet zomaar overgenomen worden naar andere contexten.

Theoretisch gezien is er nog ruimte voor andere verklaren factoren. De verklaarde variantie van alle vignetten samen was 28%. Een voorstel zou zijn de irrationele factoren meer uit te diepen en het onderwerp aan te vliegen vanuit een andere theoretische invalshoek. Interessant zou kunnen zijn het risk-as-feelings perspectief verder uit te breiden, zodat gekeken kan worden naar een breder spectrum van emoties, gevoelens en factoren die hierop van invloed zijn.

Een andere theoretische insteek zou hierin ook interessant kunnen zijn. De theorieën die nu zijn meegenomen, waren enerzijds gebaseerd op het rationele aspect van besluitvorming en anderzijds op het irrationele aspect. Door het theoretisch raamwerk in te steken vanuit de meer sociale kant, zou gekeken kunnen worden of de factoren die hieruit voortvloeien beter in staat zijn de houding tegenover het delen van data met een digitaal calamiteiten systeem, te verklaren. Een insteek die zich meer richt op sociale verhoudingen kan juist in dit geval bruikbare inzichten bieden, doordat een digitaal calamiteiten systeem meer op het maatschappelijke nut zit in plaats van persoonlijk nut. Het biedt daarbij de mogelijkheid om beter te bekijken welke normen schuilgaan achter het proces van data delen.

Gedacht kan worden aan sociale theorieën zoals de *social exchange theory* (Thibaut & Kelly, 1959). Het delen van data is voornamelijk gebaseerd op wederzijds vertrouwen en wederkerigheid (Urbonavicius et al., 2021), ook (of juist) in het geval van een digitaal calamiteiten systeem. Daarom zou onder andere naar de norm van reciprociteit (Cialdini, 2001) gekeken kunnen worden. Deze norm is belangrijk binnen interacties en verwijst naar de verwachting dat mensen sterk gemotiveerd zijn om terug te geven wat een ander persoon voor hen heeft gedaan. Deze norm en verwachting kan onder andere van invloed zijn op het vertonen van (wederkerig) altruïstisch gedrag. Zo kan iemand positiever tegenover het delen van data staan vanuit het idee dat diegene hoopt dat het ook voor hem of haar gedaan zou worden, of voelen we ons verplicht om iets te doen wanneer een ander dit ook gedaan zou hebben.

Literatuurlijst

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., & Bearth, A. (2021). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour, 21*(2), 375-386.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In: L.J. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 165-178). Boston, MA: Springer

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision-making. *IEEE Security and Privacy, 3*(1), 26–33.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21.

Bearth, A., & Siegrist, M. (2020). Psychological factors that determine people's willingness-to share genetic data for research. *Clinical Genetics*, *97*(3), 483-491.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165-176.

Berkowitz, L., & Daniels, L. R. (1964). Affecting the salience of the social responsibility norm: effects of past help on the response to dependency relationships. *The Journal of Abnormal and Social Psychology, 68*(3), 275–281.

Brandimarte, L., Acquisti, A. & Loewenstein, G. (2012). Misplaced confidences: privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347.

Butot, V., Bayerl, P. S., Jacobs, G., & de Haan, F. (2020). Citizen repertoires of smart urban safety: Perspectives from Rotterdam, the Netherlands. *Technological Forecasting and Social Change, 158*, 120164.

Caragliu, A., Del Bo, C., & Nijkamp, P. (2013). Smart cities in Europe. In: M. Deakin (Ed.), *Smart Cities* (pp. 185-207). Londen: Routledge.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 2–25.

Carter, P., Laurie, G. T., & Dixon-Woods, M. (2015). The social licence for research: why care. data ran into trouble. *Journal of Medical Ethics, 41*(5), 404-409.

Carter, L., & Schaupp, L. C. (2008, 14-17 augustus). *Efficacy and acceptance in e-file adoption* [Paperpresentatie]. AMCIS 2008: Learning from the past & charting the future of the discipline: 14th Americas Conference on Information Systems, Toronto, Ontario, Canada.

Chen, J., Bauman, A., & Allman-Farinelli, M. (2016). A study to determine the most popular lifestyle smartphone applications and willingness of the public to share their personal ata for health research. *Telemedicine and e-Health, 22*(8), 655-665.

Chiu, C. M., & Wang, E. T. G. (2008). Understanding web-based learning continuance intention: The role of subjective task value. *Information & Management, 45*(3), 194 201.

Cialdini, R. B. (2001). The science of persuasion. *Scientific American, 284*(2), 76-81.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology, 58*(6), 1015–1026.

Crawford, S. E., & Ostrom, E. (1995). A grammar of institutions. *American Political Science Review, 89*(3), 582-600.

Culnan, M. J., P. Armstrong. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.

Culnan, M. J., Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Darley, J. M., & Latane, B. (1968). Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology, 8*(4), 377-383.

Dinev, T., Xu, H., Smith, J.H. & Hart, P. (2012) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*, 61–80.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Druckman, J. N., & McDermott, R. (2008). Emotion and the framing of risky choice. *Political Behavior, 30*(3), 297–321.

Dutton, W. H., Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society, 9*(4), 433–451.

Gefen, D. (1997). *Building users' trust in freeware providers and the effects of this trust on users' perceptions of usefulness, ease of use and intended use of freeware* (Dissertatie). Georgia State University. Geraadpleegd via

https://www.proquest.com/docview/304344043?pq-origsite=gscholar&fromopenview=true

Gefen, D. (2000). E-Commerce: The Role of Familiarity and Trust. *Omega: The International Journal of Management Science, 28*(6), pp. 725–37.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51-90.

GfK Verein. (2018). *Trust in Professions 2016 – a GfK Verein study*. Geraadpleegd via https://www.nim.org/sites/default/files/medien/135/dokumente/2018_ _trust_in_professions_-_englisch.pdf (20 april 2022).

Gigerenzer, G. & Gaissmaier, W. (2011). Heuristic decision making. *Annual review of Psychology, 62,* 451–482.

Goodman, L. A., Corcoran, C., Turner, K., Yuan, N., & Green, B. L. (1998). Assessing traumatic event exposure: General issues and preliminary findings for the Stressful Life Events Screening Questionnaire. *Journal of Traumatic Stress: Official Publication of The International Society for Traumatic Stress Studies*, *11*(3), 521-542.

Haan, F. de, & Butot, V. (2021). Finding safety in the Smart City: a discourse analysis with strategic implications. In: G. Jacobs, I. Suojanen, K. Horton, P. Bayerl. (Eds.), *International Security Management. Advanced Sciences and Technologies for Security Applications* (pp. 225-242). Cham: Springer.

Harborth, D., & Pape, S. (2020). Empirically Investigating Extraneous Influences on the "APCO" Model - Childhood Brand Nostalgia and the Positivity Bias. *Future Internet*, *12*(12), 220.

Hartama, D., Mawengkang, H., Zarlis, M., Sembiring, R. W., Nasution, B. B., Syahruddin, M., ... & Irawan, E. (2016). The Planning of Smart City to Mitigate the Impacts of Natural Disaster in North Sumatera. In: Y. Murayama, D. Velev, P. Zlateva, J. Gonazelez (Eds.). *ITDRR 2016: Information Technology in Disaster Risk Reduction* (pp. 147-154). Cham: Springer.

Homburg, V., Moody, R., Yang, Q., & Bekkers, V. (2020). Adopting microblogging solutions for interaction with government: survey results from Hunan province, China. *International Review of Administrative Sciences, 88*(1), 76-94.

Horn, R., & Kerasidou, A. (2020). Sharing whilst caring: Solidarity and public trust in a data driven healthcare system. *BMC Medical Ethics*, *21*(1), 1-7.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111-136.

IPSOS. (2021, oktober). *Global Trustworthiness Index 2021: Who does the world trust?*. Geraadpleegd via https://www.ipsos.com/sites/default/files/ct/news/documents/2021 10/Global-trustworthiness-index-2021-ipsos.pdf (20 april 2022).

Jameson, S., Richter, C., & Taylor, L. (2019). People's strategies for perceived surveillance in Amsterdam Smart City. *Urban Geography, 40*(10), 1467-1484.

Jarvenpaa, S. L., & Tractinsky, N. (1999). Consumer Trust in an Internet Store: A Cross Cultural Validation. *Journal of Computer Mediated Communication, 5*(2), 1–35.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk, *Econometrica, 47*(2), pp. 263-291.

Keen, P.G.W. (1999). *Electronic Commerce Relationships: Trust by Design*. Englewood Cliffs, NJ: Prentice-Hall.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

Keusch, F., Struminskaya B., Antoun, C., Couper, M. P., & Kreuter, F. (2019). Willingness to Participate in Passive Mobile Data Collection. *Public Opinion Quarterly, 83*(1), 210 35.

Keith, M., Thompson, S., Hale, J., & Greer, C. (2012). Examining the rationality of location data disclosure through mobile devices. *IS Security and Privacy, 8*.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163-1173.

Korzaan, M., Brooks, N., Greer, T. (2009). Demystifying personality and privacy: An empirical investigation into antecedents of concerns for information privacy. *Journal of Behavioral Studies in Business, 7*(1), 1–17.

Kühberger, A., Schulte-Mecklenbeck, M., Perner. J. (1999). The effects of framing, reflection, probability, and payoff on risk preference in choice tasks. *Organizational Behavior and Human Decision Processes, 78*(3), 204–231.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Loewenstein, G., Weber, E. U., Hsee, C. K., Welch, N. (2001). Risk as feelings. *Psychological Bulletin, 127*(2), 267–286.

Luhmann, N. (1979) *Trust and Power*. Londen: John Wiley & Sons.

Malhotra, N. K., Kim, S. S., Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

McDermott, R., Fowler, J. H., Smirnov, O. (2008). On the evolutionary origin of prospect theory preferences. *The Journal of Politics, 70*(2), 335–350.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *Academy of Management Review, 23*(3), 472–90.

McKnight, D. H., Choudhury, V., Kacmar, V. C. (2002). Developing and validating trust measures for e-Commerce: An integrative topology. *Information Systems Research, 13*(3), 334-359.

Melnyk, V., Carrillat, F. A., & Melnyk, V. (2021). The influence of social norms on consumer behavior: A meta-analysis. *Journal of Marketing*, *86*(3), 98-120.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 1–27.

Moloney, M., & Potì, V. (2013). A behavioral perspective on the privacy calculus model. *SSRN Electronic Journal*.

Moody, R.F.I. (2010). *Mapper Power: Geographical Information Systems, Agenda-Setting and Policy Design* (Dissertatie). Erasmus Universiteit Rotterdam. Geraadpleegd via http://hdl.handle.net/1765/18346

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

Norberg, P.A., Horne, D.R., Horne, D.A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100 126.

Norris, F. H. (1990). Screening for traumatic stress: A scale for use in the general population. *Journal of Applied Social Psychology*, *20*(2), 1704–1718.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution based trust. *Information systems research*, *15*(1), 37-59.

Petronio, S., Durham, W. (2008). Communication privacy management theory. In: L. Baxter & D. Braithewaite (Eds.), *Engaging Theories in Interpersonal Communication: Multiple Perspectives* (pp. 309–322). Thousand Oaks, CA: SAGE Publications.

Putnam, R. D. (1992). *Making democracy work: Civic traditions in modern Italy*. Princeton, NJ: Princeton University Press.

Ramesh, A., Rajkumar, S., & Livingston, L. J. (2020). Disaster management in smart cities using IoT and big data. *Journal of Physics: Conference Series, 1716*(1), 1-14.

Revilla, M., Couper, M. P., & Ochoa, C. (2019). Willingness of Online Panelists to Perform Additional Tasks. *Methods, data, analyses, 13*(2), 223–52.

Ring, P.S., & van de Ven, A.H. (1994). Developing processes of cooperative inter organizational relationships. *Academy of Management Review, 19*(1), 90–118.

Ristvej, J., Lacinák, M., & Ondrejka, R. (2020). On smart city and safe city concepts. *Mobile Networks and Applications*, *25*(3), 836-845.

Robinson, C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569-582.

Rohm, A. J., & Milne, G. R. (2002). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000–1011.

Rotter, J. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality, 35*, 651–665.

Sala, E., Knies, G., & Burton, J. (2014). Propensity to consent to data linkage: experimental evidence on the role of three survey design features in a UK longitudinal panel. *International Journal of Social Research Methodology*, *17*(5), 455-473.

Schaupp, L. C., Carter, L., & McBride, M. E. (2010). E-file adoption: A study of US taxpayers' intentions. *Computers in Human Behavior*, *26*(4), 636-644.

Shelton, T., & Lodato, T. (2019). Actually existing smart citizens: expertise and (non)participation in the making of the smart city. *City, 23*(1), 35–52.

Smeets, M. E., & Baars, J. (2016). Vertrouwen in de politie: in de functie of in het functioneren?. *Tijdschrift voor de Politie*, *78*(3), 6-10.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: a taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503-529.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36-49.

Stibe, A., & Cugelman, B. (2019). Social Influence Scale for Technology Design and Transformation. In: D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler, P. Zaphiris (Eds.), *Human-Computer Interaction – INTERACT 2019 (pp.* 561-577). Cham: Springer.

Struminskaya, B., Toepoel, V., Lugtig, P., Haan, M., Luiten, A., & Schouten, B. (2020). Understanding willingness to share smartphone-sensor data. *Public Opinion Quarterly, 84*(3), 725-759.

Szuster, A. (2016). Crucial dimensions of human altruism. Affective vs. conceptual factors leading to helping or reinforcing others. *Frontiers in Psychology, 7*, 519.

Tan, Y. H., & Theon, W. (2001). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce, 5*(2), 61–74.

Thibaut, J. W., & Kelley, H. H. (2017). *The Social Psychology of Groups*. Londen: Routledge.

Tonmoy, F. N., Hasan, S., & Tomlinson, R. (2020). Increasing coastal disaster resilience using smart city frameworks: Current state, challenges, and opportunities. *Frontiers in Water*, *2*, 3.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross cultural perspective on the privacy calculus. *Social Media+ Society*, *3*(1), 1-13.

Ultee, W., Arts, W., & Flap, H. (2011). *Sociologie: Vragen, Uitspraken, Bevindingen.* (p. 106 113) (3e druk). Groningen/Houten: Noordhoff Uitgevers.

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, *136*, 76-85.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157-178.

Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*(5), 328-376.

Vereniging van Nederlandse Gemeenten (VNG). (2022). Trendanalyse #3 – Digital Twins. *Trendrapport Informatiesamenleving 2022.* Den Haag: Vereniging van Nederlandse Gemeenten

Volk, R., Stengel, J., & Schultmann, F. (2014). Building Information Modeling (BIM) for existing buildings - Literature review and future needs. *Automation in construction*, *38*, 109-127.

Waind, E. (2020). Trust, security and public interest: Striking the balance: A review of previous literature on public attitudes towards the sharing, linking and use of administrative data for research. *International Journal of Population Data Science, 5*(3), 1-11.

Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research, 38*(3), 505– 520.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542.

Wang, X. T. (1996). Framing effects: Dynamics and task domains. *Organizational Behavior and Human Decision Processes, 68*(2), 145–157.

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets*, *12*(3), 157-162.

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems*, *13*(1), 2-30.

Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e government and trust in government. *Journal of Public Administration Research and Theory, 15*(3), 371-391.

Wenz, A., Jäckle, A., & Couper, M.P. (2017). Willingness to use mobile technologies for data collection in a probability household panel. *Survey Research Methods, 13*(1), 1-22.

Whetten, D. A. (2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review*, *5*(1), 29 55.

Ye, C., Seo, D., Desouza, K. C., Sangareddy, S. P., & Jha, S. (2008). Influences of IT substitutes and user experience on post-adoption user switching: An empirical investigation. *Journal of the American Society for Information Science and Technology*, *59*(13), 2115-2132.

Bijlagen

Bijlage 1. Tabel alle items

Variabele	Items (0 = helemaal mee oneens – 4 = helemaal mee eens)
Houding tegenover data delen (gesteld per vignet)	1. Ik zou het net als … een goed idee vinden om mijn data te delen als deze **NIET** herleidbaar zijn naar mij als persoon. 2. Ik zou het ook een goed idee gevonden hebben om mijn data te delen met het calamiteiten management systeem als de data **NIET** herleidbaar zijn naar mij als persoon. 3. Wanneer ik met dezelfde situatie geconfronteerd wordt, zou ik het net als … een goed idee vinden om **NIET** herleidbare data te delen. 4. Ik zou het net als … een goed idee vinden om mijn data te delen als deze **WEL** herleidbaar zijn naar mij als persoon. *(verwijderd)* 5. Ik zou het ook een goed idee gevonden hebben om mijn data te delen met het calamiteiten management systeem als de data **WEL** herleidbaar zijn naar mij als persoon. *(verwijderd)* 6. Wanneer ik met dezelfde situatie geconfronteerd wordt, zou ik het net als … een goed idee vinden om **WEL** herleidbare data te delen. *(verwijderd)*
Realisme vignetten (gesteld per vignet)	1. De situatie is realistisch. 2. Ik kan me voorstellen dat mensen deze situatie overkomt.
Verwachte nut	1. Ik denk dat een digitaal calamiteiten systeem nuttig is in mijn dagelijks leven. *(verwijderd)* 2. Een digitaal calamiteiten systeem maakt dat hulpdiensten hun taken sneller kunnen vervullen. 3. Het gebruiken van een digitaal calamiteiten systeem zal helpen bij het oplossen van risicosituaties. 4. Een digitaal calamiteiten systeem verhoogt de kans op effectief handelen in het geval van een risicosituatie.
Sociale invloed	1. Mensen die mijn gedrag beïnvloeden, zullen het een goed idee vinden dat ik mijn data beschikbaar stel voor een digitaal calamiteiten systeem. 2. Mensen die belangrijk voor mij zijn, zullen het een goed idee vinden dat ik mijn data beschikbaar stel voor een digitaal calamiteiten systeem.

	3. Over het algemeen zullen de meeste mensen in mijn omgeving mij steunen wanneer ik het een goed idee vind om mijn data beschikbaar te stellen voor een digitaal calamiteiten systeem.
Verwachte risico's	1. Het delen van mijn **anonieme data** met een digitaal calamiteiten systeem zou veel onverwachte problemen met zich mee kunnen brengen. 2. Het delen van mijn **anonieme data** met een digitaal calamiteiten systeem zou riskant kunnen zijn. 3. De mogelijke verliezen die gepaard kunnen gaan met het delen van mijn **anonieme data** met een digitaal calamiteiten systeem zouden groot kunnen zijn. 4. Het delen van mijn **persoonlijke data** met een digitaal calamiteiten systeem zou veel onverwachte problemen met zich mee kunnen brengen. 5. Het delen van mijn **persoonlijke data** met een digitaal calamiteiten systeem zou riskant kunnen zijn. 6. De mogelijke verliezen die gepaard kunnen gaan met het delen van mijn **persoonlijke data** met een digitaal calamiteiten systeem zouden groot kunnen zijn.
Vertrouwen DCS	1. Ik verwacht dat een digitaal calamiteiten systeem informatie op een eerlijke manier communiceert. 2. Ik verwacht dat een digitaal calamiteiten systeem in staat is om haar taak uit te voeren. 3. Ik verwacht dat een digitaal calamiteiten systeem eerlijk zal zijn. 4. Ik verwacht dat een digitaal calamiteiten systeem het beste met burgers voor zal hebben.
Vertrouwen technologie DCS	1. Ik heb er vertrouwen in dat versleuteling van data en andere technologische ontwikkelingen met betrekking tot een digitaal calamiteiten systeem, het gebruik ervan veilig zou maken. 2. Ik ben er zeker van dat juridische en technologische structuren achter een digitaal calamiteiten systeem mij goed beschermen tegen problemen. 3. Een digitaal calamiteiten systeem zal over het algemeen een robuuste en veilige omgeving zijn. 4. Een digitaal calamiteiten systeem biedt voldoende beveiliging om ervoor te zorgen dat ik me comfortabel voel indien het gebruikt wordt.

Vertrouwen technologie internet	1. Ik heb er vertrouwen in dat versleuteling van data en andere technologische ontwikkelingen met betrekking tot het internet, het gebruik ervan veilig maakt. 2. Ik ben er zeker van dat juridische en technologische structuren op het internet mij goed beschermen tegen problemen. 3. Het internet is over het algemeen een robuuste en veilige omgeving. 4. Het internet biedt voldoende beveiliging om ervoor te zorgen dat ik me comfortabel voel bij het gebruik ervan.
Vertrouwen stakeholder (vier keer gesteld: voor het ziekenhuis, de brandweer, politie en overheid)	1. Ik vind dat [stakeholder] informatie op een eerlijke manier communiceert. 2. Ik vind dat [stakeholder] in staat is om haar taak uit te voeren. 3. Ik vind dat [stakeholder] eerlijk is. 4. Ik vind dat [stakeholder] het beste voor heeft met burgers.
Privacy zorgen	1. In vergelijking met anderen geef ik meer om de manier waarop met mijn data omgegaan wordt. 2. Het allerbelangrijkste voor mij is het behouden van mijn privacy wanneer ik mijn data deel met andere organisaties. 3. Over het algemeen maak ik me grote zorgen over eventuele privacyschendingen.
Autonomie	1. Ik vind het vervelend als ik geen controle heb over de persoonlijke informatie die ik aan een digitaal calamiteiten systeem geef. 2. Ik vind het vervelend als ik geen controle heb met betrekking tot beslissingen over hoe mijn persoonlijke informatie verzameld, gebruikt en gedeeld wordt met een digitaal calamiteiten systeem. 3. Ik maak me zorgen wanneer ik geen of minder controle heb over mijn persoonlijke data. 4. Als ik mijn data deel, verlies ik daar de controle over. *(verwijderd)* 5. Als ik data deel, kunnen daar consequenties aan vast zitten die niet meer omgekeerd worden. *(verwijderd)*

Altruïsme	1. Anderen helpen is een van de meest belangrijke dingen in het leven. 2. Ik werk graag voor het welzijn van anderen. 3. Mijn familie heeft de neiging om degenen die het minder hebben dan ons te helpen. *(verwijderd)* 4. Ik ben het eens met het oude gezegde: “het is zaliger te geven dan te ontvangen”. *(verwijderd)*
Zelfredzaamheid	1. Ik heb genoeg maatregelen genomen om mij voor te bereiden op een eventuele risicosituatie. *(verwijderd)* 2. Ik denk dat ik tijdens een risicosituatie in (de omgeving van) het Erasmus MC kan helpen de gevolgen te beperken. *(verwijderd)* 3. Ik denk dat ik tijdens een risicosituatie in (de omgeving van) het Erasmus MC zonder hulp van anderen kan vluchten naar een veilige plek. 4. Ik denk dat ik goed om kan gaan met de (eventuele) gevolgen van een risicosituatie.
Conformisme	1. Ik heb een voorkeur om te doen wat andere mensen doorgaans doen. 2. Ik heb een voorkeur om me te gedragen zoals iedereen doet. 3. Ik volg het gedrag dat andere mensen gebruikelijk doen. 4. Ik vermijd het om te handelen op een manier die ongewoon is. *(verwijderd)* 5. Ik doe niet graag wat mensen gebruikelijk doen. *(verwijderd)* 6. Ik kopieer niet het gedrag dat iedereen doet.
Risicoaversie	1. Ik voel me niet op mijn gemak als ik risico's neem. 2. Ik heb een voorkeur voor situaties die voorspelbare uitkomsten hebben. 3. Voordat ik een beslissing neem, wil ik er absoluut zeker van zijn hoe het zal aflopen. 4. Ik vermijd situaties waarvan de uitkomsten onzeker zijn. 5. Ik voel me op mijn gemak als ik in nieuwe situaties moet improviseren. 6. Ik voel me nerveus als ik beslissingen moet nemen in onzekere situaties.
ICT-vaardigheden	Hoe zou u uw ICT-vaardigheden beoordelen?

Bijlage 2. Gerapporteerde realisme en betrouwbaarheid realismescores

	Cronbach's Alpha	Gemiddelde (SD)	Range (min. – max.)
Realisme directe noodsituatie	0,916	2,25 (0,98)	0 - 4
Realisme dreiging van noodsituatie	0,908	2,33 (0,88)	0 - 4
Realisme collectieve nood	0,897	2,75 (0,82)	0 - 4
Realisme individuele nood	0,859	2,68 (0,87)	0 - 4

Bron: DE-RISC enquête 2022, N=236

Bijlage 3. Factoranalyse

	Component																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
NUT 1	0,501																
NUT 2	0,762																
NUT 3	0,706																
NUT 4	0,776																
INVL 1		0,707															
INVL 2		0,676															
INVL 3		0,493															
RISICO 1			0,672														
RISICO 2			0,750														
RISICO 3			0,791														
RISICO 4			0,503														
RISICO 5			0,460														
RISICO 6			0,512														
VT DCS 1				0,808													
VT DCS 2				0,745													
VT DCS 3				0,814													
VT DCS 4				0,713													
VT TECH 1					0,771												
VT TECH 2					0,736												
VT TECH 3					0,614												
VT TECH 4					0,544												
VT TECH 5					0,810												
VT TECH 6					0,763												
VT TECH 7					0,711												
VT TECH 8					0,749												
VT ZKH 1						0,588											
VT ZKH 2						0,727											
VT ZKH 3						0,644											
VT ZKH 4						0,665											
VT BRW 1							0,616										
VT BRW 2							0,694										

VT BRW 3	0,709						
VT BRW 4	0,635						
VT POL 1	0,767						
VT POL 2	0,700						
VT POL 3	0,799						
VT POL 4	0,731						
VT OVRH 1		0,842					
VT OVRH 2		0,760					
VT OVRH 3		0,853					
VT OVRH 4		0,820					
ZORGEN 1			0,686				
ZORGEN 2			0,775				
ZORGEN 3			0,790				
AUTON 1			0,818				
AUTON 2			0,784				
AUTON 3			0,781				
AUTON 4			0,508				
ALTRU 1				0,779			
ALTRU 2				0,742			
ALTRU 3				0,725			
ALTRU 4				0,443			
ZELFRED 2					0,509		
ZELFRED 3					0,772		
ZELFRED 4					0,763		
CONFOR 1						0,765	
CONFOR 2						0,861	
CONFOR 3						0,858	
CONFOR 4						0,563	
CONFOR 6						0,692	
AVERS 1							0,721
AVERS 2							0,705
AVERS 3							0,767
AVERS 4							0,775
AVERS 5							0,643
AVERS 6							0,642

V INDIVIDU 1	0,782			
V INDIVIDU 2	0,724			
V INDIVIDU 3	0,664			
V COLL 1		0,799		
V COLL 2		0,785		
V COLL 3		0,792		
V DREIGING 1			0,868	
V DREIGING 2			0,877	
V DREIGING 3			0,877	
V DIRECT 1				0,897
V DIRECT 2				0,882
V DIRECT 3				0,900

Bron: DE-RISC enquête 2022, N=236

Bijlage 4. Correlaties en VIF-waarden onafhankelijke variabelen

	1.	2.	3.	4.	5.	6.	7.	VIF
1. Verwachte nut	1	0,512**	-0,271**	0,505**	0,485**	0,236**	0,249**	1,654
2. Sociale invloed	0,512**	1	-0,352**	0,492**	0,558**	0,380**	0,297**	1,796
3. Verwachte risico's	-0,271**	-0,352**	1	-0,279**	-0,482**	-0,381**	-0,325**	1,427
4. Vertrouwen DCS	0,505**	0,492**	-0,279**	1	0,503**	0,388**	0,383**	1,765
5. Vertrouwen technologie	0,485**	0,558**	-0,482**	0,503**	1	0,562**	0,369**	2,359
6. Vertrouwen ziekenhuis	0,236**	0,380**	-0,381**	0,388**	0,562**	1	0,561**	2,063
7. Vertrouwen brandweer	0,249**	0,297**	-0,325**	0,383**	0,369**	0,561**	1	2,250

Bron: DE-RISC enquête 2022, N=236
*=p<0.05; **=p<0.01

Bijlage 4 (vervolg). Correlaties en VIF-waarden onafhankelijke variabelen

	1.	2.	3.	4.	5.	6.	7.	VIF
8. Vertrouwen politie	0,278**	0,321**	-0,283**	0,362**	0,416**	0,524**	0,632**	2,192
9. Vertrouwen overheid	0,132*	0,250**	-0,201**	0,158*	0,357**	0,393**	0,232**	1,480
10. Privacy zorgen	-0,256**	-0,356**	0,276**	-0,234**	-0,414**	-0,244**	-0,099	1,388
11. Altruïsme	0,174**	0,238**	-0,138*	0,224**	0,238**	0,193**	0,328**	1,214
12. Conformisme	0,093	0,081	0,072	0,127	0,052	0,078	0,063	1,166
13. Risicoaversie	0,142*	0,099	-0,054	0,189**	0,020	-0,051	0,034	1,268
14. ICT-vaardigheden	-0,039	-0,116	0,046	-0,164*	-0,123	-0,102	-0,010	1,104

Bron: DE-RISC enquête 2022, N=236
*=p<0.05; **=p<0.01

Bijlage 4 (vervolg). Correlaties en VIF-waarden onafhankelijke variabelen

	8.	**9.**	**10.**	**11.**	**12.**	**13.**	**14.**	**VIF**
8. Vertrouwen politie	1	0,469**	-0,193**	0,158*	0,103	-0,019	-0,076	2,192
9. Vertrouwen overheid	0,469**	1	-0,274**	0,157*	0,126	-0,051	-0,081	1,480
10. Privacy zorgen	-0,193**	-0,274**	1	-0,075	-0,122	0,153*	0,020	1,388
11. Altruïsme	0,158*	0,157*	-0,075	1	0,019	0,004	-0,138*	1,214
12. Conformisme	0,103	0,126	-0,122	0,019	1	0,266**	-0,065	1,166
13. Risicoaversie	-0,019	-0,051	0,153*	0,004	0,266**	1	-0,188**	1,268
14. ICT-vaardigheden	-0,076	-0,081	0,020	-0,138*	-0,065	-0,188**	1	1,104

Bron: DE-RISC enquête 2022, N=236
*=p<0.05; **=p<0.01

Bijlage 5. Gemiddelde houding en correlatie naar soort noodsituatie

	Gemiddelde (SD)	**Correlaties**			
		Directe noodsituatie	**Dreiging van noodsituatie**	**Collectieve nood**	**Individuele nood**
1. Directe noodsituatie	2,20 (1,13)	1	0,406**	0,491**	0,497**
2. Dreiging van noodsituatie	2,70 (1,12)	0,406**	1	0,528**	0,508**
3. Collectieve nood	2,79 (1,03)	0,493**	0,528**	1	0,567**
4. Individuele nood	2,75 (0,98)	0,497**	0,508**	0,567**	1

Bron: DE-RISC enquête 2022, N=236
*=p<0.05; **=p<0.01