Grip Op Eigen Gegevens

Een analyse van de mogelijkheden en beperkingen om Nederlandse burgers controle te geven over hun persoonlijke gegevens.

Danny Lämmerhirt
Julia Jansen

Mei 2024

waag futurelab

Grip op eigen gegevens

Danny Lämmerhirt
Julia Jansen

Met medewerking van: Alain Otjens, Aris Ham, Job Spierings en Simone van der Burg

Samenvatting

In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft Waag Futurelab onderzoek gedaan naar de bestaande instrumenten die ter beschikking staan van burgers om controle te hebben over het delen en gebruik van persoonsgerelateerde gegevens. Waag werd gevraagd na te gaan welke functies de instrumenten hebben, op welke gegevens ze kunnen worden toegepast en welke vormen van toegang tot gegevens ze bieden voor burgers. Het onderzoek maakt deel uit van het nationaal Actieplan Open Overheid 2023-2027.

Onderzoeksdoelen en aanpak

Het doel van dit onderzoek was om een inventarisatie te maken van bestaande instrumenten in Nederland die burgers meer grip geven op hun data. We verzamelden 109 instrumenten uit verschillende bronnen en analyseerden hun functies en gebruikersinterfaces. Daarna interviewden we de belanghebbenden van drie instrumenten in drie casestudies.

Inzichten

Op basis van onze instrumentanalyse blijkt dat de overheid er nog niet in slaagt burgers zeggenschap te geven over hun gegevens. Het is vooral belangrijk om in de toekomst de volgende punten aan te pakken.

1. **Burgers worden geconfronteerd met een jungle aan instrumenten die hen 'grip' moeten geven op hun data (n=109):** Er is sprake van data silo's binnen verschillende overheidsinstanties. Hierdoor wordt er van burgers verwacht om zelf op de hoogte te zijn over welke overheidsinstantie gegevens over hen verzamelt, wat ervoor zorgt dat het lastig is voor hen om grip te krijgen op de gegevens die er over hen verwerkt worden. Daarnaast worden de meeste instrumenten die bedoeld zijn om burgers meer controle te geven geïmplementeerd door individuele organisaties, onafhankelijk van de overheid. Hierdoor moeten burgers de verscheidenheid aan instrumenten die verschillende organisaties hanteren leren kennen om zo hun rechten (inzage, correctie, verwijdering, beperking van verwerking, overdraagbaarheid en bezwaar tegen het gebruik van gegevens) uit te kunnen oefenen.
2. **Instrumenten besteden selectief aandacht aan *sommige* AVG-rechten (niet aan alle):** Bestaande instrumenten bieden burgers slechts beperkte mogelijkheden om rechten op hun gegevens uit te oefenen. In de meeste gevallen kunnen burgers hun rechten op inzage en correctie uitoefenen. Burgers kunnen niet zien welke gegevens precies worden gebruikt voor welke diensten en welke beslissingen aan

de hand van deze gegevens worden gemaakt. Ook het delen van gegevens tussen overheidsdiensten kan niet door burgers worden beïnvloed. Daarnaast zijn er weinig instrumenten beschikbaar om bezwaar te maken tegenover besluiten die gemaakt zijn op basis van persoonsgegevens.

3. **Tot nu toe staat het versoepelen van bureaucratische processen centraal en niet de kwaliteit van de diensten:** betrokkenen geven aan dat de beschikbare instrumenten goed dienen om gegevensuitwisseling tussen overheden en burgers te versoepelen en te zorgen voor een verbeterd gebruiksgemak. Het belang van efficiëntie, kostenverlaging, of het versoepelen van gegevens-gebaseerde beslissingen over het toekennen van diensten of producten, is volgens betrokkenen ontwikkelaars en overheidsinstellingen belangrijk. Het is niet duidelijk of ook burgers hierdoor de dienstverlening als beter ervaren én of ze daadwerkelijk altijd betere toegang krijgen tot bepaalde diensten.
4. **Onduidelijke technische en juridische randvoorwaarden beperken de implementatie van instrumenten voor dataportabiliteit:** er bestaat tot op heden geen gestructureerde toegang tot gegevens uit de basisregisters voor data bemiddelaars. Sommige instrumenten gebruiken 'screenscraping' om gegevens van burgers te verzamelen in plaats van data-uitwisseling middels een Application Programming Interface (API). Daardoor hebben burgers zelf en databemiddelaars minder invloed op het delen van gegevens. Andere apps maken gebruik van toegangsrechten van individuele steden om gegevens uit basisregisters op te vragen. Het ontbreekt aan een gestandaardiseerde aanpak om de ontwikkeling van instrumenten voor gegevensuitwisseling te ondersteunen en rechten en plichten duidelijk vast te leggen.

Aanbevelingen

Aanbevelingen 1 en 2 hebben betrekking op de beperkte rol van AVG-rechten in de huidige overheidsdiensten. Aanbeveling 3 draait om kader voor gegevensuitwisseling die een gelijkwaardige machtsverhouding tussen burgers en overheid bevorderen.

1. Ontwikkel instrumenten die het voor burgers mogelijk maken om meer data rechten uit te oefenen

We roepen overheden en ontwikkelaars op om:

- **Burgers meer inzicht te geven** in welke persoonlijke gegevens op welke manier worden gebruikt bij de totstandkoming van voor hen relevante besluitvorming.
- **Aandacht te geven aan de rechten van burgers en hen meer controle te geven wanneer er iets misgaat in de verwerking van persoonsgegevens.** Tot nu toe zijn er geen diensten beschikbaar die burgers de kans geven om fouten in de omgang met hun data door overheden te herstellen, waardoor ze mogelijk toeslagen, sociale bijstand of andere zaken mislopen terwijl ze daar wel recht op hebben.

- **Rekening te houden met de digitale kloof**. Een deel van de burgers (20% in Amsterdam) heeft geen toegang tot digitale technologieën, door weinig financiële middelen of een gebrek aan digitale vaardigheden. Als overheidsinstellingen hun diensten digitaal aanbieden, dan kan dat deze groep mensen benadelen. Daarom is het belangrijk om een analoog aanbod te creëren, bestaande uit toegankelijke contactpersonen en processen, zodat burgers ook zonder digitale technologie controle kunnen uitoefenen op hun gegevens.

2. Stel de kwaliteit van dienstverlening centraal, en niet de digitalisering daarvan.

We roepen overheden, uitvoeringsorganisaties en andere publieke dienstverleners op om:

- **De instrumenten te ontwikkelen waarmee burgers grip krijgen op hun gegevens als onderdeel van de totale dienstverlening aan burgers.** Dit betekent dat de ervaring van de burger centraal moet staan bij de ontwikkeling. Dit vereist het in kaart brengen van verschillende situaties en behoeften van burgers, en op basis daarvan het ontwikkelen van een verscheidenheid aan technische hulpmiddelen, diensten en processen die burgers helpen hun rechten tegenover de overheid uit te oefenen.
- **Aandacht te geven aan kwaliteitseisen van data-gebaseerde dienstverlening.** Met het toenemende gebruik van gegevens binnen de digitale welvaartsstaat is het essentieel dat de overheid de kwaliteit van haar diensten op het gebied van gegevensbeheer voortdurend controleert. Het is belangrijk dat burgers niet de dupe worden van geautomatiseerde processen voor gegevensverwerking. Burgers moeten erop kunnen vertrouwen dat de diensten in hun belang worden geleverd, wat betekent dat de overheid de verantwoordelijkheid draagt om ervoor te zorgen dat automatisering geen extra problemen voor hen oplevert.

3. Ontwikkel kader voor gegevensuitwisseling die een gelijkwaardige machtsverhouding tussen burgers en overheid ondersteunen

We roepen beleidsmakers op om:

Technische standaarden voor gegevensuitwisseling (bijvoorbeeld APIs) te ontwikkelen waarbij de rechten van burgers centraal staan. API's spelen een cruciale rol in de machtsverhouding tussen burgers en de overheid, omdat ze verschillende rechten kunnen verankeren. Deze rechten omvatten het recht op inzage in waar persoonlijke data zich bevindt, welke overheidsinstanties data delen, wat er met die data gebeurt, en wie hierop controle mag uitoefenen. Het zou in lijn zijn met de AVG om open standaarden te gebruiken en te zorgen dat verschillende organisaties met toestemming van burgers gegevens kunnen opvragen.

Nog beter zou het zijn om een brede maatschappelijke discussie te voeren over welke normen ten grondslag moeten liggen aan de ontwikkeling van API's. Naast burgers zouden ook maatschappelijke organisaties en onderzoeksinstellingen die zich met deze vraagstukken bezighouden, aan deze discussie moeten deelnemen.

- **Toezichtkaders op een uniforme manier binnen overheidsorganisaties te implementeren:** de rollen, rechten en plichten van overheden en commerciële data bemiddelaars moeten duidelijk worden gedefinieerd en actief worden gecontroleerd door de overheid. Het is van cruciaal belang om transparant te zijn over dit beleid richting de samenleving. Bovendien is het belangrijk om input te krijgen vanuit maatschappelijke hoeken bij de ontwikkeling van deze toezichtskaders en bij de implementatie ervan.
- **Eigenaarschap van gegevens in de handen van burgers te leggen:** Overheden kunnen ook het beheer van data overdragen aan de burgers zelf. Een voorbeeld hiervan is België, waar de Vlaamse overheid streeft naar de ontwikkeling van individuele 'solid pods', een soort datakluisjes waarmee burgers hun eigen data kunnen beheren. In dit systeem moet de overheid toestemming vragen aan burgers om de data te delen die zij nodig heeft. Hierdoor keert de machtsdynamiek om en wordt de burger daadwerkelijk de primaire beheerder van gegevens.

Inhoud

Inleiding

Steeds meer interacties tussen burgers, overheden en derde partijen worden gedreven door het verzamelen, verwerken en delen van grote hoeveelheden gegevens. Bij de interacties tussen samenleving en overheid, maar ook bij de uitvoering van publieke diensten, spelen algoritmische technologieën en digitale data in toenemend mate een sturende rol. Persoonlijke data zijn belangrijk om de dienstverlening aan de behoeften van de maatschappij aan te passen. Maar het is ook belangrijk dat de maatschappij controle blijft houden over welke gegevens verwerkt worden, in welke contexten.

Een antwoord hierop is om burgers meer 'grip' op hun eigen gegevens te geven. Tot nu toe ontbreekt er een overzicht over manieren waarop burgers grip kunnen krijgen op het verzamelen, delen en gebruik van gegevens door overheidsdiensten. In dit rapport verkennen we welke instrumenten beschikbaar zijn die burgers in staat stellen om 'grip' te krijgen op de gegevens die de overheid over hen verwerkt. Waag Futurelab voerde dit onderzoek uit in opdracht van het ministerie voor Binnenlandse Zaken en Koninkrijksrelaties en de Maatschappelijke Coalitie Over Informatie Gesproken. Het onderzoek maakt deel uit van het nationaal Actieplan Open Overheid 2023-2027. Wij stellen de volgende onderzoeksvragen:

1. Welke initiatieven en technologieën bestaan er in Nederland om mensen controle te geven over de gegevens die overheden van hen verwerken?
2. Welke AVG-rechten kunnen worden uitgeoefend en over welke gegevens?
3. Welke mogelijkheden en uitdagingen zien belanghebbenden bij de ontwikkeling van instrumenten en hoe beïnvloedt dat wie controle over persoonsgegevens heeft?

Dit rapport biedt meerdere inzichten: overheidsorganisaties hebben aandacht besteed aan sommige aspecten van de AVG. Zo is er tot nu toe aandacht voor meer inzage, correctie, en het overdragen van gegevens, maar minder aandacht voor rechten om de gegevensverwerking beperken of het geven van de mogelijkheid aan burgers om een bezwaar in te dienen. We vonden meer dan 100 instrumenten om verschillenden AVG-rechten uit te oefenen waarvan slechts enkele instrumenten organisatie-overkoepelend zijn. De ontwikkeling van de instrumenten die we hebben bekeken laat daarbij verschillende spanningsvelden zien tussen de belangen van verschillende burgers en overheden, machtsrelaties tussen beide, en noties van 'grip'. Automatisering van gegevensuitwisseling wordt vaak door de overheid gezien als oplossing om de foutmarges te beperken, maar ze beperken ook het handelingsvermogen van burgers. Door die automatisering verminderen de bureaucratische processen en versoepelen interacties met overheden. Echter, onderzoek naar de behoeften van burgers laat zien dat burgers verschillende handelingsmogelijkheden willen hebben om hun AVG-rechten uit te oefenen.

1 Achtergrond: Controle van persoonlijke gegevens

Overheden gebruiken steeds meer gegevens om diensten digitaal te kunnen verschaffen, zoals de toewijzing van sociale ondersteuning. Ook worden digitale middelen gebruikt om risico's te kunnen inschatten bij verschillende burgers, zoals bijvoorbeeld het risico op fraude, het risico dat iemand in de schulden geraakt of in de criminaliteit belandt. Burgers worden op grond van de gegevens die over hen worden verzameld gecategoriseerd en dit beïnvloedt de dienstverlening richting burgers en is een elementair onderdeel van institutionele besluitvorming over hen. Om die reden kunnen gegevens een grote invloed uitoefenen op de levens van individuele burgers. Het is belangrijk om erachter te komen hoe burgers controle kunnen krijgen over de manier waarop er informatie over hen wordt verzameld, gedeeld en gebruikt. Daarbij zijn er verschillende interpretaties van het begrip 'grip' en wat het betekent om grip te hebben op je gegevens. De verschillende interpretaties hebben betrekking op de relaties tussen burger en overheid. Het definiëren van grip is daarom een belangrijk startpunt bij het onderzoeken van de mate waarin controle kan worden uitgeoefend door burger, overheid of een derde partij.
Recente schandalen, zoals de toeslagenaffaire, hebben in Nederland de urgentie vergroot om de controle van burgers over de persoonsgegevens die de overheid over hen verwerkt te verbeteren. Deze affaire heeft de aandacht gevestigd op de schadelijke impact die bureaucratische processen en gegevensverwerkingssystemen kunnen hebben op duizenden gezinnen. Naast de toeslagenaffaire zijn de Nederlandse publieke informatiesystemen, zoals het basisregistratiesysteem, bekritiseerd als 'digitale kooi', waarin ambtenaren veel invloed kunnen uitoefenen op de toekenning van gelden en diensten, waaronder bijvoorbeeld toeslagen, aan burgers, zonder dat burgers daarop veel invloed hebben (Peeters and Widlak 2018).
Daarnaast hebben geautomatiseerde fraudedetectiesystemen zoals Systeem Risico Indicatie (SyRI) laten zien hoe mensen in lage-inkomenswijken in Nederland onterecht worden geprofileerd als mogelijke fraudeurs bij het aanvragen van sociale voorzieningen van de overheid. SyRI werd uiteindelijk als illegaal beschouwd en in strijd met het VN-Handvest voor de Rechten van de Mens. Het gebrek aan transparantie rondom dergelijke systemen, zowel richting het publiek als richting de Tweede Kamer, leidde tot georganiseerde publieke protesten van mensenrechtenorganisaties en kritiek in de media (Wieringa 2023). Enquêtes tonen aan dat dergelijke gevallen het vertrouwen van burgers in de overheid hebben ondermijnd. De overheid wil dit verbeteren.

1.1 De politieke context en overheidsinitiatieven

In de afgelopen jaren heeft de Nederlandse overheid, samen met diverse instellingen in de publieke sector, verschillende wetten en beleidsprogramma's geïntroduceerd om burgers

meer controle te geven over hun persoonsgebonden gegevens. Een belangrijk uitgangspunt van dergelijke initiatieven is de Algemene Verordening Gegevensbescherming (AVG), die als juridisch kader fungeert voor het recht op inzage in opgeslagen gegevens, het recht op correctie van gegevens, en het recht om klachten in te dienen over gegevensverwerking. De overheid streeft ernaar om de informatiehuishouding van overheidsinstanties te verbeteren en individuen meer zeggenschap te geven over hun gegevens (Enthoven, van Bergeijk, and Wiemers 2023). Dit was de reden voor het lanceren van het programma Regie op gegevens[1].

In 2022 heeft staatssecretaris van Digitalisering, Alexandra van Huffelen, een agenda gepresenteerd voor digitalisering die gedreven wordt door waarden. In deze agenda wordt onder meer voorgesteld dat iedereen controle moet kunnen uitoefenen over zijn of haar digitale gegevens: burgers moeten zeggenschap krijgen over persoonlijke gegevens, er moeten applicaties worden ontwikkeld om de digitale identiteit te beheren en de algoritmen die worden gebruikt door overheidsinstellingen moeten beter worden gereguleerd. De agenda stelt dat individuen en organisaties het recht moeten hebben om inzicht te krijgen in de digitale gegevens die de overheid over hen verzamelt en met welke partijen deze gegevens worden gedeeld, om te zien op basis van welke gegevens besluitvorming over hen tot stand komt en om onjuiste gegevens te corrigeren indien nodig.[2]

Belangrijke recente wetgeving met betrekking tot het delen van gegevens is de tweedelige Wet Digitale Overheid (WDO), waarvan het eerste deel in juli 2023 van kracht was.[3] Het eerste deel van deze wet regelt onder andere het digitaal inloggen bij overheidsinstanties. Het doel is om verschillende inlogmiddelen, zowel vanuit de overheid als de markt, toe te staan, om zo burgers meer keuze en gebruiksgemak te bieden. Het tweede deel van de wet zal gaan over het verantwoord delen van digitale persoonsgegevens met zowel overheids- als niet-overheidsinstanties. Een essentieel onderdeel hiervan is een vernieuwd stelsel voor de basisregistraties, bekend als het Federatief Datastelsel[4], waarbij gegevens op één centrale plaats worden geregistreerd en niet kunnen worden gekopieerd of verstuurd. Dit wordt verder uitgewerkt in het Actieplan Data bij de Bron[5], dat als doel heeft om de informatiehuishouding bij de overheid te verbeteren en transparantie te bevorderen, net als de kwaliteit van data en

[1] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens/

[2] Om deze doelen te bereiken, staat er in deze agenda dat de 15 belangrijkste databronnen gebruikt door de overheid toegankelijk moeten zijn voor burgers, waarbij de ontwikkeling van nieuwe technologieën wordt ondersteund en de behoeften van burgers op het gebied van gegevenscontrole worden onderzocht door het Ministerie van Binnenlandse Zaken.

[3] https://wetgevingskalender.overheid.nl/Regeling/WGK005654

[4] "De komende jaren is de belangrijkste opgave het ophalen van gegevens bij de bron eenvoudiger te maken en deze vervolgens gecombineerd te gebruiken. Ook in andere sectoren en voor andere doelen dan waarvoor de gegevens oorspronkelijk verzameld zijn" (voetnoot: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/) Zie ook pg. 57 van de geactualiseerde werkagenda Waardegedreven Digitaliseren.

[5] https://www.digitaleoverheid.nl/data-bij-de-bron/)

dataminimalisatie[6]. Om de toepassingen van het Federatief Datastelsel te testen, is er een 'innovatiewerkplaats' opgezet namens Digilab[7].

1.2 Waarom de doeleinden van 'grip' van belang zijn

Het is van belang dat het vergroten van persoonlijke controle over gegevens wordt gekoppeld aan verschillende politieke doelstellingen. Daarom moeten initiatieven voor het verstevigen van grip rekening houden met de verschillende en soms tegenstrijdige belangen, rollen en relaties tussen burgers, derde partijen en overheidsinstanties. Op die manier voorkomen ontwikkelaars van digitale informatiesystemen de kans dat zij leed veroorzaken en vergroten ze de kans dat ze bijdragen aan het verbeteren van de levenssituaties van burgers. Een beleidsbrief aan de Tweede Kamer uit 2019 benadrukt dat persoonlijke controle over gegevens niet alleen juridische, maar ook ethische en economische doelen zal bevorderen[8]. Volgens de beleidsbrief zal de toegang tot persoonlijke gegevens de efficiëntie van publieke dienstverlening verhogen en economische activiteiten buiten de overheid stimuleren. Hieruit kunnen we concluderen dat persoonlijke gegevens een hybride karakter hebben - ze zijn niet alleen van persoonlijk belang voor burgers, maar zijn ook een instrument voor overheden om hun eigen diensten te optimaliseren, en ze helpen het optimaliseren van commerciële diensten van derden. Vaak wordt controle over persoonlijk gegevens en het uitwisselen hiervan als voorwaarde gezien voor verschillende positieve gevolgen. Kortom, bij het gesprek over grip op gegevens zijn belangen in het spel van verschillende actoren.

Er zijn verschillende manieren om met deze belangen om te gaan. Wetenschappelijke literatuur benoemt meerdere vormen van controle of grip: meestal wordt de nadruk gelegd op de controle van burgers over gegevens, zoals wanneer burgers om toestemming wordt gevraagd om gegevens te gebruiken. Echter, volgens literatuur in het sociaalwetenschappelijke domein is controle over gegevens ook afhankelijk van bestaande relaties tussen actoren, zoals burgers, overheden en commerciële partijen. Ook is controle over gegevens afhankelijk van de specifieke situaties waarin om gegevens wordt gevraagd; zoals bijvoorbeeld bij het aanvragen van een paspoort, het bepalen of iemand in aanmerking komt voor huursubsidies of toeslagen. Bovendien wordt controle over gegevens niet alleen mogelijk gemaakt door diensten die gegevens beheren, behandelen of verspreiden, maar ook door de relaties met een bredere infrastructuur van wetten, praktijken en technologieën.

Elke vorm van controle werpt een ander perspectief op de relaties tussen burgers, overheden, commerciële organisaties en maatschappelijke organisaties. Een recent rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) nam een

[6] Het principe van dataminimalisatie vloeit voort uit de AVG en bepaalt dat alleen gegevens die noodzakelijk zijn voor een doel mogen worden opgevraagd en verwerkt.
[7] Zie https://digilab.overheid.nl/).
[8] Beleidsbrief, nadere uitwerking: https://open.overheid.nl/documenten/ronl-5ffcc31b-51d1-4d2d-98aa-f2b0bdf27512/pdf

vergelijkbaar standpunt in[9]. Het rapport maakt onderscheid tussen **directe burgerlijke controle** (waarbij burgers de vaardigheden hebben om zelf hun levenssituaties te verbeteren), **indirecte controle** (waarbij burgers ondersteuning krijgen van andere actoren, zoals maatschappelijke organisaties, die namens hen hun levenssituaties kunnen verbeteren), en **collectieve controle** (door burgers gezamenlijk te betrekken bij het plannen van de overheidsaanpak van diensten). Grip is dus niet alleen een individuele vaardigheid van burgers, of een juridisch vraagstuk, maar hangt af van verschillende actoren in het speelveld, in welke situaties mensen grip op gegevens willen uitoefenen, de machtsposities van burgers, overheden en dienstverleners, juridische afspraken en beschikbare technologieën.

Onderstaand bespreken we drie perspectieven op grip en in welke mate ze 'grip op gegevens' definiëren.

1.3 De wettelijke basis van grip op gegevens

Het eerste perspectief op 'grip' behelst directe controle van individuen over specifieke gegevens en verwerking daarvan. De AVG-wetgeving definieert verschillende rechten om individuen controle over persoonsgebonden gegevens te bieden. Deze rechten omvatten onder andere het recht op inzage, correctie, verwijdering, beperking van verwerking, overdraagbaarheid en bezwaar tegen het gebruik van gegevens. De AVG regelt dat gegevens alleen voor specifieke doeleinden mogen worden gebruikt (het principe van minimale gegevensverwerking) en dat mensen toestemming moeten geven voordat hun gegevens worden gebruikt. Ook biedt de AVG mensen inzage in welke categorieën hun gegevens worden verwerkt, voor welke doeleinden en door welke partijen, en verplicht de wet het beschikbaar stellen van een gestructureerde kopie van de gebruikte gegevens. Naast de AVG zijn er andere wetten van toepassing op (persoons)gegevens die door de overheid worden verwerkt, zoals de Wet basisregistratie personen, die de redenen voor verzameling en verwerking van gegevens bepaalt, evenals de procedures voor het uitoefenen van rechten door burgers. Burgers hebben niet volledig controle over BRP-gegevens middels AVG-rechten, omdat overheidsinstellingen dezelfde gegevens voor de uitvoer van publieke taken nodig hebben. Daardoor zijn de rechten van burgers op BRP-gegevens beperkt.

In lijn met die beperkingen, definieert het programma 'Regie op gegevens' het concept van 'grip' met nadruk op drie AVG-rechten: de rechten op inzage, correctie en overdraagbaarheid van gegevens (data portability). In hoofdstuk 3 zien we dat de meeste instrumenten die overheidsorganisaties bieden het AVG-recht op inzage en het recht op correctie mogelijk maken, en dat er daarnaast buiten de overheid verschillende oplossingen bestaan om het recht op overdraagbaarheid van gegevens uit te oefenen.

[9] https://www.wrr.nl/publicaties/rapporten/2023/11/30/grip

Op een conceptueel niveau discussiëren rechtsdeskundigen over de betekenis van controle of grip, en de problemen die hiermee kunnen worden aangepakt. De rechtsgeleerden Lazaro en Meyer argumenteren dat persoonlijk 'controle' over gegevens een prominent begrip in EU-beleidsdocumenten is. In zulke documenten heeft 'controle' verschillende betekenissen en verwijst het vaak naar een reeks microrechten om mensen zogenaamd de controle te geven (Lazaro en Meyer 2015). Ideeën over controle putten volgens hen inspiratie uit concepten als informatieve zelfbeschikking of soevereiniteit (zie ook Hummel, Braun, and Dabrock 2020), die gebaseerd zijn op liberale opvattingen van individuen die geïnformeerd beslissingen nemen over welke gegevens ze met wie delen. Dit liberale perspectief stoelt op een cognitieve visie op de mens, die individuen beschouwen als rationele spelers die weloverwogen beslissingen over het wel of niet verzamelen, delen of gebruiken van gegevens kunnen nemen. Dit model impliceert dat individuele mensen rechten hebben en leidt tot vragen over de juiste definitie van geïnformeerde besluitvorming en toestemming (informed consent) voorafgaand aan het uitwisselen van gegevens. Ook wordt gesuggereerd dat de gegevens waarover de besluitvorming gaat alleen toebehoren aan het individu, en niet ook aan anderen. Maar verschillende juridische deskundigen, ethici en sociologen bekritiseren deze uitgangspunten. Ze vragen zich af of het cognitieve perspectief op de rationele mens wel klopt, en of die wel een geïnformeerd besluit kan nemen over gegevens die digitaal worden gedeeld. Ook vragen ze zich af of gegevens wel altijd alleen aan een individu toebehoren, en dat het belang alleen persoonlijk kan worden geduid. De betekenis van veel gegevens komt alleen in een context naar voren. Sommige auteurs verdedigen daarom een ander perspectief op 'grip' op gegevens.

1.4 Grip op levensomstandigheden door gegevensgebruik

Een tweede perspectief op 'grip op gegevens' behelst grip op levensomstandigheden door het gebruik van gegevens. Vaak hangt dit samen met het gebruik van deze gegevens door derde partijen. We leiden deze opvatting van grip op gegevens af uit de literatuur rond de waarde van gegevens in gebruikscontexten en publieke dienstverlening. Zoals in sectie 1.2 besproken, hebben diverse partijen verschillende belangen als het gaat om het gebruik, beheer en opslaan van gegevens. Gegevens zoals inkomen zijn bijvoorbeeld niet alleen persoonsgebonden, maar dienen *ook als middel* voor dienstverlening. Daarom beweren wetenschappers steeds vaker dat de betekenis van gegevens en de belangen bij het beschermen of delen ervan afhangen van de context waarin ze worden gebruikt (Solove 2024). Dit betekent dat persoonlijke gegevens kunnen worden beschouwd als een sociaal construct waarvan de gevoeligheid afhangt van de gebruikscontext, interpretaties van gegevens en hetgeen je ermee kunt bereiken (zie van Zoonen 2016; Fiske et al. 2022).
Sociologisch onderzoek argumenteert dat de gevoeligheid en waarde van gegevens worden bepaald door interacties tussen burgers, overheden en andere groepen. Een vergelijkbaar argument is dat de opvattingen van mensen over privacy contextafhankelijk zijn (Nissenbaum 2004). Onderzoek naar de controle van burgers over gegevens laat

zien dat het ervaren van 'goede' controle over gegevens varieert per gegevenstype, gebruiksdoel, degene die betrokken zijn bij de verwerking van gegevens en welke regels er zijn voor de gegevensverwerking (van Zoonen 2016).

Dit perspectief op gegevens veronderstelt dat de bezorgdheid van burgers over het gebruik van hun gegevens afhankelijk is van hoe mensen hun gegevens interpreteren en waarvoor ze denken dat deze gegevens worden ingezet (Vitak et al. 2023). Onderzoek over bestaande technologieën in Nederland laat bijvoorbeeld zien dat mensen apps vertrouwen voor financiële gegevensuitwisseling als deze de DigiD gebruikt, omdat DigiD met de overheid geassocieerd wordt (Mare 2021, Mens & Mare 2021). Als we kijken naar concrete voorbeelden van interacties tussen overheid en burgers, worden de individualistische noties van grip uitgedaagd. Voor mensen is het minder noodzakelijk om de controle over hun gegevens te hebben als ze kunnen vertrouwen op rechtvaardige machtsdynamieken en dienstverlening. Omdat veel van deze situaties worden gevormd door wetten en regels, hebben mensen alleen op een indirecte manier grip (WRR 2023) op hun leven en zijn er heldere voorwaarden nodig om dienstverlening inclusief en rechtvaardig te organiseren.

Het belang van grip op verschillende facetten van het leven wordt de afgelopen jaren vaker onderschreven. Volgens de WRR draagt grip bij aan zekerheid; grip betekent dat mensen in staat zijn hun omgeving effectief te beïnvloeden en zo hun doelen te bereiken (WRR, 2023). Levenssituaties zijn afhankelijk van publieke dienstverlening die beurtelings afhankelijk is van de toegang en het gebruik van persoonsgegevens. Vanuit dit perspectief zijn niet de gegevens op zichzelf de belangrijkste aanjager van de noodzaak tot meer grip, maar ze zijn een bron waardoor relaties tussen burgers en publieke dienstverleners opnieuw ter discussie worden gesteld. Dit perspectief op ‘grip’ verschuift dus focus van de gegevens zelf naar de relaties die door het gebruik van gegevens ontstaan en/of worden gecontinueerd.

1.5 Collectieve grip door maatschappelijke infrastructuur

Het derde perspectief op ‘grip’ is de opvatting dat de controle over 'persoonlijke gegevens' afhankelijk is van de relaties met een breder netwerk van infrastructuren. Infrastructuren, zoals informatietechnologieën, wetten of organisaties zijn collectief vastgestelde middelen om controle uit te oefenen op gegevens; ze hebben invloed op hoe rechten op gegevens worden verdeeld, welke soorten gebruik van gegevens mogelijk is en hoe de meerwaarde van gegevens wordt bepaald. Vanuit dat perspectief zijn de AVG-rechten een belangrijke, maar niet noodzakelijk voldoende voorwaarde om de machtspositie van burgers ten opzichte van overheden, technologische systemen en organisaties te herstructureren. Hiervoor zijn collectief vastgestelde middelen nodig, zoals onafhankelijke (maatschappelijke) organisaties die als bemiddelaar kunnen optreden tussen burgers en overheden (Bernholz 2021).

Tussenpartijen spelen hierbij een belangrijke rol; zij kunnen op basis van AVG-rechten gegevens van burgers verzamelen en nieuwe diensten ontwikkelen. Deze 'data-bemiddelaars' bevinden zich tussen degene die data deelt en de ontvanger van data en vervullen verschillende functies, zoals het beheer, opschoning, data-uitwisseling en het verlenen van toegang en gebruiksrechten (Janssen and Singh 2022). Binnen de wetenschap zijn er ontwikkelingen aan de gang op het gebied van het creëren van verschillende soorten 'data-bemiddelaars' (Micheli et al. 2020). Data-bemiddelaars dienen in toenemende mate als belangrijke regelgever voor de uitwisseling, het beheer en gebruik van gegevens.

Data bemiddelaars krijgen in toenemend mate aandacht als beheerders van data die met hulp van juridische en technische middelen de standaarden voor goede uitwisseling en gebruik van gegevens definiëren en de normen, rollen, en relaties bepalen die tussen burgers en organisaties bestaan (Janssen en Singh 2022). Ze bepalen bijvoorbeeld de voorwaarden voor verwerking en gebruik van gegevens, stellen vast wie er toegang toe mag hebben, wie de gegevens mag gebruiken en voor welke doeleinden (Milne, Sorbie, and Dixon-Woods 2021). Software-architecturen spelen een belangrijke rol bij het uitoefenen van 'controle' omdat de mate van grip op gegevens daarvan afhankelijk is (Gray, Gerlitz, en Bounegru 2018). Deze architectuur definieert de relatie tussen degene die de data deelt, de bemiddelaar en de data-gebruiker via de backend code en gebruikersinterface, maar ook via de regels die de gebruiker worden opgelegd.

Ook speelt regelgeving een belangrijke rol bij de controle van data-bemiddelaars over gegevens, die bepaalt hoe burgers en derde partijen toegang krijgen tot gegevens. Een voorbeeld is het Nederlandse basisregistratiesysteem. Peeters en Widlak betogen dat de architectuur van publieke informatiesystemen een controlerende functie heeft, omdat het categorieën van burgers bepaalt die beslissingen van ambtenaren beïnvloeden wie wel of niet diensten mag ontvangen, hoe gegevens kunnen worden gewijzigd en door wie (2018).

Dit betekent dat als we willen begrijpen hoe mensen controle krijgen over data, we aandacht moeten besteden aan de technologische mogelijkheden en afhankelijkheden tussen spelers in dit veld. Deze technische en sociale relaties bieden een meer collectief perspectief op 'grip' op gegevens, omdat ze tussen mensen ontstaan en ook de (machts-)relaties en interacties tussen mensen beïnvloeden. Zoals verschillende artikelen betogen, worden deze regels, standaarden en machtsrelaties tot nu toe vaak achter gesloten deuren bepaald door commerciële organisaties en overheden (Nebbiai 2022). Als we willen dat burgers meer 'grip' krijgen, dan is het essentieel om democratische wetten, regels, standaarden en technische infrastructuren vast te stellen in een publieke dialoog. Ook dit biedt een perspectief op grip.

1.6 Conclusie

We zien dat het begrip 'grip' op verschillende manieren kan worden geïnterpreteerd. Grip kan op individueel, contextueel en sociaal niveau worden begrepen, maar het kan ook diep verweven zijn in een netwerk van sociale en technische infrastructuren en regels. Natuurlijk heeft 'grip' betrekking op fundamentele datarechten, die vervolgens relaties tussen burgers en overheden voortbrengen. Echter, de manier waarop, waarom en met welke effecten deze rechten worden uitgeoefend, moet worden gezien in relatie tot aannames over de rationele capaciteiten van een persoon, de context waarin data worden gedeeld, en de architecturale en sociale relaties die de transacties van het verzamelen, delen en gebruiken van data vormgeven.

Daarnaast speelt de organisatorische context waarin burgers 'controle' kunnen verkrijgen een belangrijke rol. Wanneer overheden, uitvoeringsorganisaties en derde partijen controlemechanismen voor persoonlijke gegevens gebruiken, is het van belang om onderzoek te doen naar de manier waarop burgers deze controle verkrijgen en voor welke doeleinden.

2 Methodologie

In het empirische gedeelte van dit onderzoek definiëren we controle over gegevens aan de hand van de rechten die via de AVG aan individuen worden verleend. We vragen ons af hoe deze rechten worden vertaald in technologieën, hoe deze technologieën zijn ingebed in organisatorische praktijken en netwerken van overheden en voor welke doeleinden rechten kunnen worden uitgeoefend. Hierbij stellen we de volgende onderzoeksvragen:

1. Welke initiatieven en technologieën bestaan er in Nederland om mensen controle te geven over de gegevens van hen die overheden verwerken?
2. Welke AVG-rechten kunnen worden uitgeoefend en over welke gegevens?
3. Welke mogelijkheden en uitdagingen zien belanghebbenden bij de ontwikkeling van instrumenten en hoe beïnvloedt dat wie controle heeft over persoonsgegevens?

Om deze onderzoeksvragen te beantwoorden, hebben we eerst een lijst samengesteld met instrumenten om controle uit te oefenen die momenteel beschikbaar zijn bij Nederlandse overheidsorganisaties en rond de basisregistratiegegevens. We hebben de gebruikersinterfaces van de instrumenten geanalyseerd om te zien welke AVG-rechten uit te oefenen zijn voor de gebruiker. Dit heeft geresulteerd in een lijst met beschikbare technologieën die we hebben verwerkt in een visualisatie (https://grip-op-eigen-gegevens.waag.org). Daarnaast wilden we begrijpen welke factoren de ontwikkeling van deze hulpmiddelen beïnvloeden, voor welke levenssituaties ze worden ontwikkeld en hoe de instrumenten specifieke vormen van grip mogelijk maken.

2.1 Aanpak dataverzameling en analyse van instrumenten

Voor onze dataverzameling hebben we een lijst met URL's samengesteld van overheidsinstanties en derde partijen die burgers tools bieden om persoonlijke gegevens te beheren bij hun interactie met overheden of rond de gegevens uit de basisregisters. Om instrumenten te zoeken hebben we officiële URL lijsten van nationale en vier gemeentelijke overheidswebsites en uitvoeringsorganisaties geraadpleegd, apps op app stores gezocht, deskundigen geïnterviewd en een zoekstrategie toegepast gebaseerd op trefwoorden (zie bijlage voor meer informatie over de strategie). We hebben ons geconcentreerd op instrumenten die momenteel beschikbaar zijn voor gebruik door burgers, waarbij we prototypen of concepten voor toekomstige tools buiten beschouwing hebben gelaten. Hoewel we hebben getracht om open en algemene zoektermen te gebruiken, is het mogelijk dat bepaalde partijen (zoals maatschappelijke organisaties) andere termen gebruiken voor hun instrumenten. Dit heeft ervoor gezorgd dat we hun instrumenten niet hebben gevonden. De resultaten van de analyse zijn niet bedoeld om representatief of alomvattend te zijn, maar om de diversiteit aan beschikbare

instrumenten te laten zien waarvan burgers vandaag de dag gebruik kunnen maken. De volledige lijst van bronnen omvat:

- Literatuuronderzoek
- Gestructureerde Google zoek (zie bijlage)
- Gestructureerde analyse van apps op app stores
- Analyse van overheidswebsites
- Expertconsultaties

In onze analyse hebben we bestudeerd hoe de burgerrechten van de AVG-wet momenteel door verschillende instrumenten mogelijk – of niet mogelijk – gemaakt worden. Om te begrijpen hoe instrumenten controle over persoonsgegevens mogelijk maken, hebben we de zogenaamde *walkthrough* methode gebruikt (Light, Burgess, and Duguay 2018). De walkthrough methode is een manier om systematisch de beschikbare grafische gebruikersinterfaces (GUI's) van webservices en mobiele apps te analyseren. We bekeken de functies van instrumenten, maar ook verwachte gebruikssituaties waarvoor ontwerpers ontwikkelen. GUI's bieden inzicht in concrete visies en functies van 'grip' omdat ze een beoogd doel hebben, culturele betekenissen in app-functies integreren en omdat ze de ideale gebruikers en bijpassende toepassingen voor ogen hebben. Volgens de walkthrough-methode hebben we voor elk instrument screenshots verzameld van iedere pagina die gebruikers konden aanklikken, om de route die zij doorlopen te documenteren. We hebben screenshots van app-functies geanalyseerd op grond van de soorten AVG-rechten die burgers kunnen uitoefenen via de interface. We baseren onze analyse van 'grip' op de gegevensrechten die zijn vastgelegd in de Nederlandse AVG-wet. In het geval dat bepaalde AVG-rechten niet konden worden uitgeoefend, hebben we de redenen hiervoor geanalyseerd aan de hand van juridische, organisatorische en technologische factoren.

2.2 Aanpak casestudies: Interviews en documentenanalyse

Om een dieper inzicht te verkrijgen in de ervaringen van experts met de ontwikkeling en het gebruik van verschillende tools hebben we drie casestudies opgezet. De casestudies bestaan uit deskresearch en expertinterviews. In dit onderzoek hebben we ervaringen van burgers buiten beschouwing gelaten. Het onderzoek werd uitgevoerd in opdracht van de Maatschappelijke Coalitie over Informatie Gesproken (MCOIG) en het Ministerie van Binnenlandse Zaken en was hoofdzakelijk bedoeld om te onderzoeken wat de voor- en nadelen zijn van de instrumenten voor burgers, ook was het doel te onderzoeken wat voor functies die instrumenten hebben. Het doel van het casestudie onderzoek was om te onderzoeken welke acties via deze instrumenten mogelijk gemaakt worden voor burgers en welke factoren de verdere ontwikkeling van deze instrumenten beïnvloed.

We hebben cases geselecteerd op basis van de volgende criteria:

- De instrumenten moesten in gebruik zijn (gebaseerd op downloadstatistieken in appstores)
- De instrumenten moesten verschillende typen benaderingen tot data-controle weerspiegelen (informatietools, datasluizen om toestemming te beheren, datakluizen voor gegevensopslag),
- De instrumenten moesten door verschillende ontwikkelaars worden ontwikkeld (binnen of buiten de overheid).

Dit heeft geresulteerd in onderzoek naar een MijnOmgeving, een datasluis voor financiële toepassingen genaamd Ockto en een datakluis voor niet-commerciële doeleinden binnen overheidsinstellingen die Yivi heet. In de casestudies hebben we middels expertinterviews en documentanalyse onderzocht wat de achterliggende motivaties zijn voor ontwikkelaars, dataleveranciers en datagebruikers en welke problemen zij willen oplossen met een instrument. Daarbij vroegen we voor welke gebruikersbehoeften het instrument primair is ontworpen en welke vorm van grip het ondersteunt. Daarnaast wilden we weten hoe instrumenten momenteel worden gebruikt, en welke afhankelijkheden het ontwerp van een instrument beïnvloeden. De casestudies worden afgesloten met een bredere reflectie op de manier waarop AVG-rechten de informatierelaties tussen overheden, burgers en de ontwikkelaars en gebruikers van de instrumenten herschikken. Voor de casestudies spraken we met 7 medewerkers van de volgende organisaties:

- Logius
- Gemeente Nijmegen
- Ockto B.V.
- SIDN
- Aegon
- BS&F
- ICTU

3 Landschap van instrumenten

We hebben vier categorieën instrumenten gevonden die zich door hun functionaliteiten onderscheiden: MijnOmgevingen, brieven en webformulieren, sluizen en kluizen voor het overdragen van gegevens, en specifieke instrumenten, om een recht uit te oefenen.

Categorie instrumenten	Kenmerken interface	Type ontwikkelaar /aanbieder	Voorbeelden
MijnOmgevingen	Een gepersonaliseerd overzicht van gegevens en aanvragen die bewaard worden in databases elders. Burger logt in via DigiD. Sommige MijnOmgevingen worden ook aangeboden via een smartphone-applicatie.	Overheidsorganisaties, uitvoeringsorganisaties en zelfstandige bestuursorganen	Mijn UWV, Mijn Overheid, Mijn Werkmap
Brief schrijven of webformulier invullen	Correspondentie. Burger schrijft zelf brief of vult een verzoek in een formulier in en verzendt die naar een organisatie.	Overheidsorganisaties, uitvoeringsorganisaties en zelfstandige bestuursorganen	UWV: Bezwaar indienen Gemeente Amsterdam: Uitreksel BRP
Kluizen	Burger heeft een applicatie op eigen (smartphone)apparaat, waar data in wordt opgeslagen en van waaruit informatie wordt gedeeld.	Derde partijen, soms aangeboden via overheden	Yivi app
Sluizen	Burger heeft een applicatie op eigen apparaat waar data tijdelijk in wordt opgeslagen om het vervolgens door te sturen, waarna de data weer van het toestel wordt verwijderd. Of de burger kan via de app toestemming verlenen aan organisaties om bij een andere organisatie gegevens op te halen.	Derde partijen, bijvoorbeeld banken.	Ockto app
Specifieke instrumenten om één bepaald AVG-recht uit te oefenen	Verschillend		Rijksdienst voor identiteitsgegevens: Meldpunt Fouten in Overheidsregistraties

Tabel 1: Overzicht van tool typen

3.1 De belangrijkste inzichten

Opvallend is dat bijna alle instrumenten door publieke instellingen of commerciële bedrijven worden ontwikkeld. Overheden bieden MijnOmgevingen, brieven, e-mails, en formulieren aan. Deze tools maken het meestal mogelijk om inzage in categorieën van gegevens te krijgen, en gegevens te corrigeren. Derde partijen, zoals universiteiten en privébedrijven bieden zogenaamde datasluizen en kluizen aan. Dit zijn technologieën die dataportabiliteit (overdracht van gegevens) mogelijk maken. Een sluis regelt de machtigingen en overdrachten tussen servers zonder ergens daar tussenin gegevens op te slaan. Een kluis biedt dezelfde functionaliteit, maar slaat ook gegevens op in een persoonlijke database zoals op een smartphone. Deze technologieën maken data-uitwisseling mogelijk en geven een overzicht van de datacategorieën die worden uitgewisseld en ook de partijen die data ontvangen. Opvallend is het gebrek aan maatschappelijke ontwikkelaars als tool ontwikkelaars. Behalve Radboud Universiteit en Bits of Freedom hebben we geen organisatie gevonden die tools ontwikkelt voor maatschappelijke doeleinden zoals sociale dienstverlening, rechtsbijstand of het indienen en verwerken van bezwaren over besluiten van sociale diensten. Derde partijen zijn meestal commerciële bedrijven wier businessmodel bestaat uit het verzamelen, opschonen, en versoepelen van gegevensuitwisseling voor andere dienstverleners in de wonings- en financiële markt.

Verder maakt ons onderzoek duidelijk dat publieke instellingen en derde partijen een selectieve focus op bepaalde AVG-rechten leggen met hun instrumenten. Aan de ene kant is dit een positieve ontwikkeling. Het laat zien dat de overheidsdienst de politieke doelstellingen van het programma Regie op Gegevens implementeert en zorgt voor meer inzicht, mogelijkheden voor correctie en dataportabiliteit. Aan de andere kant bieden ze burgers slechts zeer selectieve instrumenten om hun rechten uit te oefenen. De uitwisseling van gegevens wordt alleen maar door derde partijen aangeboden middels kluizen en sluizen. Die instrumenten bieden geen mogelijkheid om gegevens bij de bron te corrigeren of te verzoeken om minder of geen gegevens te verwerken. Publieke instellingen daarentegen richten zich op het verspreiden van informatie over gegevensverwerking en -correctie, waardoor burgers niet alleen gegevens kunnen aanpassen, maar ook overheden kunnen helpen gegevens over burgers actueel te houden. Naast gegevens van basisregistraties bieden instrumenten weinig inzicht in andere gegevens die over burgers verzameld en verwerkt worden en weinig inzicht in *hoe* de gegevens in processen gebruikt worden. Dit kan een probleem zijn als burgers willen optreden tegen besluiten of als de gegevens door de overheid verkeerd worden verwerkt.

Figuur 1: Visualisatie van bestaande instrumenten

Andere rechten, zoals het recht op bezwaar, krijgen minder aandacht. Zoals we op de volgende pagina's toelichten, is de technische implementatie van deze rechten nog steeds beperkt. Een voorbeeld hiervan zijn de MijnOmgevingen, maar ook het Meldpunt Fouten, waarbij er meestal sprake is van het recht op inzage en correctie van gegevens categorieën en de verwerkende instantie, maar geen inzicht wordt geboden in welke gegevens worden verwerkt om te komen tot specifieke besluitvorming. Tot nu zijn brieven de meest gebruikelijke instrumenten om gegevens te verwijderen, het delen van gegevens tussen overheidsinstanties te beïnvloeden of klachten in te dienen over de gegevens die worden verzameld en gebruikt. Slechts in sommige gevallen kunnen burgers invloed uitoefenen op welke organisaties toegang krijgen tot hun persoonsgegevens.

En andere observatie is dat elke organisatie eigen tools implementeert en er weinig tools zijn die AVG-rechten instelling overkoepelend uitvoerbaar maken. Tot nu toe zijn

MijnOmgevingen, brieven, en e-mails meestal aangeboden door één specifieke organisatie waarmee een burger rechtstreeks communiceert. Dit betekent dat burgers zich tot iedere specifieke organisatie moeten richten, om inzage te krijgen of gegevens te corrigeren in plaats van dat zij centraal toegang hebben tot alle gegevens die door overheidsorganisaties worden verzameld en daar hun rechten kunnen uitoefenen. Ook vereist dit van de burgers dat ze weten welke instellingen over welke gegevens beschikken. Instrumenten voor data portabiliteit, zoals kluizen en sluizen, kunnen gegevens van verschillende databronnen halen en in een centrale plek verzamelen of direct naar een ontvanger doorsturen.

Dit kan verschillende problemen opleveren. Aan de ene kant creëert het extra werk (en extra kosten) voor publieke instellingen als ze hun eigen tools implementeren in plaats van een overkoepelend platform te gebruiken. Aan de andere kant worden instrumenten ontwikkeld vanuit het perspectief van de verantwoordelijkheden van de publieke dienst en de overheid (zie ook hoofdstuk 4), niet vanuit het perspectief van de behoeften van burgers. Dat betekent dat burgers zich zullen moeten blijven wenden tot verschillende instanties om AVG-rechten uit te oefenen.

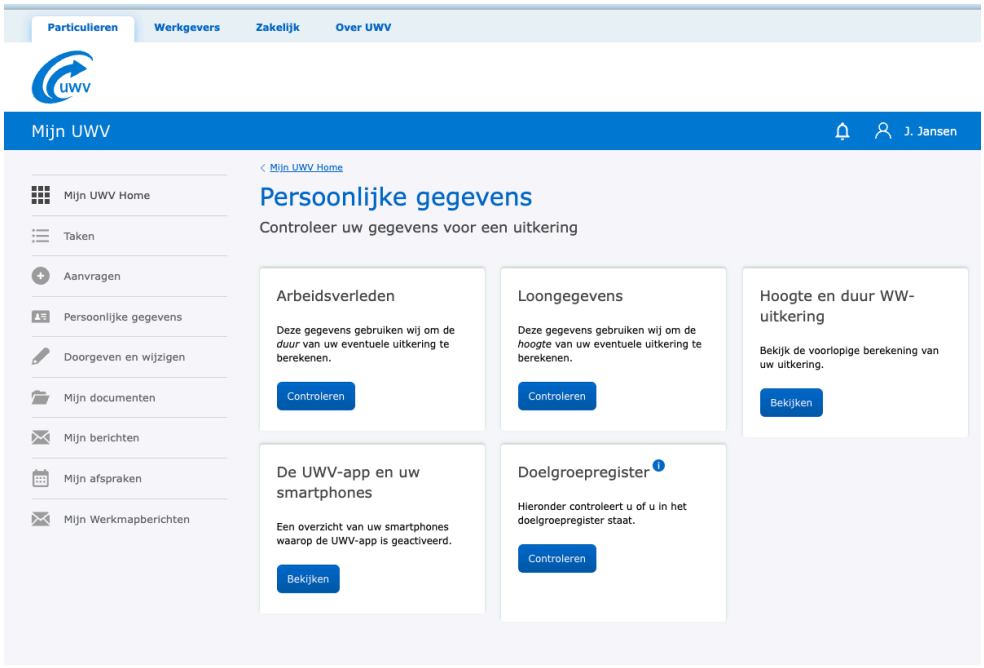
Volgens ons onderzoek zijn er meer dan 100 (n=109) tools die Nederlandse bewoners kunnen gebruiken, vaak om enkel een paar AVG-rechten uit te oefenen bij één publieke instelling. Dat geldt voor MijnOmgevingen, brieven en webformulieren, maar ook voor tools voor gegevensuitwisseling met derde partijen. Een voorbeeld hiervan is dat als mensen een data kluis gebruiken en zien dat er een correctie van gegevens nodig is, ze deze correctie direct bij een databron moeten aanvragen. Uitzonderingen zijn de app MijnGegevens en het Meldpunt Fouten. De app MijnGegevens biedt tot nu toe inzage in basisregistratie persoonsgegevens. Het Meldpunt Fouten biedt burgers hulp om gegevens bij verschillende databronnen te corrigeren. Over het geheel genomen bieden de instrumenten burgers inzicht in datacategorieën en creëren updates of maken het uitwisselen van gegevens mogelijk, zonder burgers meer controle te geven over hoe overheidsorganisaties de gegevens voor hun eigen dienstverlening gebruiken. Hieronder leggen we uit welke rechten kunnen worden gebruikt bij de verschillende soorten tools.

3.2 MijnOmgevingen

Ongeveer de helft van de geselecteerde overheidsorganisaties, uitvoeringsorganisaties of bestuursorganen biedt een ‘MijnOmgeving’ aan voor burgers. Voorbeelden hiervan zijn Mijn Belastingdienst, Mijn toeslagen, MijnGegevens, Mijn SVB, Mijn UWV, Mijn Werkmap of Mijn DUO. Het gaat bij dit type instrument om online omgeving waar ingelogd wordt met DigiD. We noemen deze instrumenten ‘MijnOmgevingen’.

Uitoefenen AVG rechten: nadruk op inzage en correctie
MijnOmgevingen van overheidsinstanties geven na inloggen in de meeste gevallen een overzicht op de thuispagina een overzicht van de persoonsgegevens die bekend zijn bij

de organisatie. Het gaat hierbij vaak om identiteitsgegevens, zoals naam, geslacht, geboortedatum en geboorteplaats. Tevens geven MijnOmgevingen een overzicht van voor die specifieke dienst relevante gegevens die over de burger bekend zijn. Denk aan een overzicht van werkplekken en loon bij het UWV, een overzicht van schulden bij de SVB, of een overzicht van ontvangen toeslagen in Mijn Toeslagen. Het is in de interface niet altijd duidelijk waar de gegevens in MijnOmgevingen vandaan komen of waar de bron van deze gegevens ligt. Zo staat voor de onderzoeker in de Kinderopvangtoeslagapp een wijziging, doorgevoerd door de Dienst Toeslagen over verwacht inkomen voor volgend jaar, waarvan onduidelijk is waar het op gebaseerd is. In berichten van het UWV over besluiten over toegekende uitkeringen is bijvoorbeeld in geval van de onderzoeker geen informatie te vinden over welke gegevens ten grondslag lagen aan het besluit of waar die vandaan kwamen.



Figuur 2: Schermafbeelding Mijn UWV

Correcties kunnen in mijnomgevingen gedaan worden, zolang het gegevens betreft die primair bij die overheidsinstantie liggen en het niet gaat om gegevens uit basisregisters. In Mijn UWV is het mogelijk om loongegevens en informatie over het arbeidsverleden te controleren en het door te geven als er iets niet lijkt te kloppen. Over het algemeen gaat het corrigeren van gegevens in MijnOmgevingen middels een melding van iets wat niet lijkt te kloppen of een verzoek tot 'wijzigen' van gegevens.

Via interfaceonderzoek van MijnOmgevingen zijn de onderzoekers weinig tot geen mogelijkheden tegengekomen om gegevens te verwijderen, gegevensverwerking te beperken (vragen om minder gegevens te verzamelen) of bezwaar te maken tegen gebruik van bepaalde gegevens. De verwerking van persoonsgegevens door deze overheidsorganisaties is in veel gevallen gelegitimeerd bij wet. Dat verklaart waarom

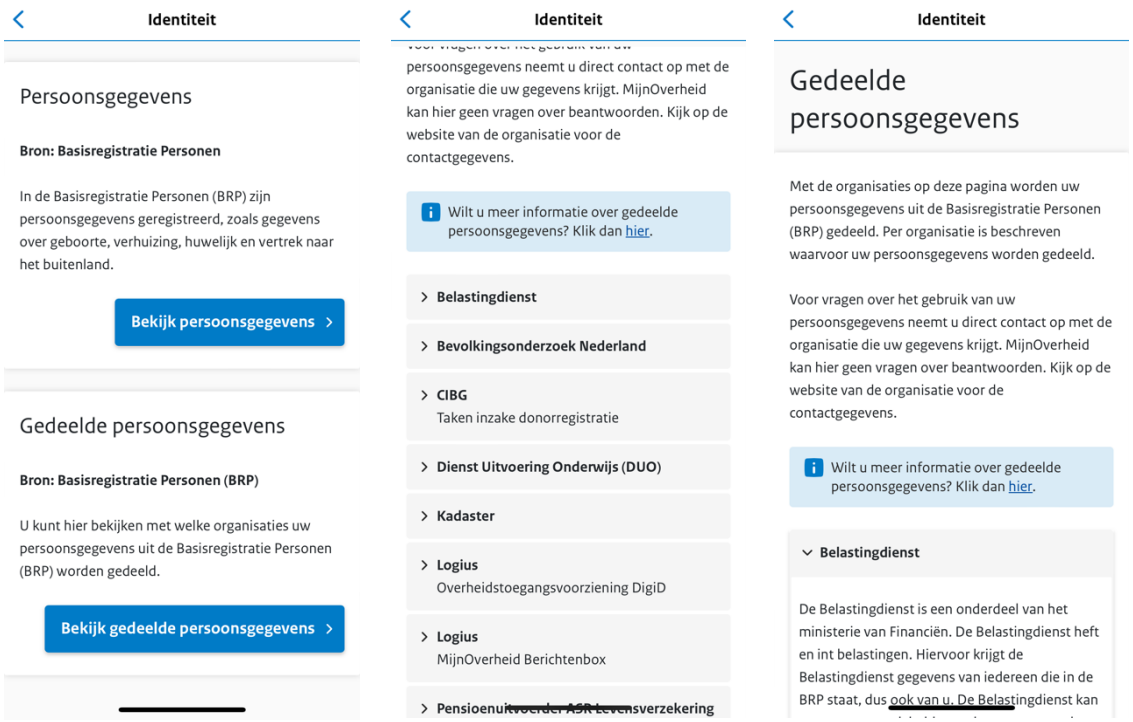
deze rechten via deze instrumenten niet uitgeoefend kunnen worden. In sommige MijnOmgevingen kunnen burgers gegevens overdragen tussen organisaties. Dit is bij de onderzochte instrumenten bijvoorbeeld het geval wanneer een burger een dienst geleverd krijgt of aanvraagt. Zo plaatst een burger in Mijn Werkmap een CV en identiteitsgegevens die gedeeld worden met organisaties wanneer deze persoon solliciteert op vacatures.

Figuur 3: Schermafbeelding werk.nl

In de meeste MijnOmgevingen kan een burger niet expliciet toestemming geven voor het overdragen van gegevens, maar is overdracht van de gegevens gelegitimeerd bij wet en regelgeving, zoals bijvoorbeeld de Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi), de loonaangifteketen[10] of samenwerkingsconvenanten zoals die tussen de Belastingdienst, het UWV en het CBS[11]. In zulke wetgeving wordt geregeld dat gegevens mogen worden uitgewisseld tussen bijvoorbeeld de gemeentelijke sociale diensten en het UWV. Het is vaak niet zichtbaar voor burgers in MijnOmgevingen wanneer gegevens worden uitgewisseld en tussen welke organisaties precies.

De app MijnGegevens biedt voor de gegevens uit de BRP een overzicht van overheidsorganisaties die het register mogen raadplegen, maar de burger heeft geen mogelijkheden zelf invloed uit te oefenen op deze overdracht van gegevens (zie figuur 4). Op de middelste afbeelding van figuur 4 is de lijst te zien van organisaties die de gegevens uit de BRP krijgen, in geval van de onderzoeker een lijst van 17 overheidsorganisaties. In de afbeelding rechts is te zien dat voor elke organisatie bekeken kan worden met welk doel die organisatie de gegevens uit het BRP ontvangt. Voor andere basisregistraties, zoals Inkomen, is een dergelijk overzicht niet opgenomen in de MijnGegevens app.

[10] Zie hier over de (juridische) herkomst van de loonaangifteketen: https://www.loonaangifteketen.nl/de-ketensamenwerking/onstaansgeschiedenis
[11] Zie https://download.belastingdienst.nl/belastingdienst/docs/convenant_belastingdienst_cbs_uwv_al11771z2ed.pdf

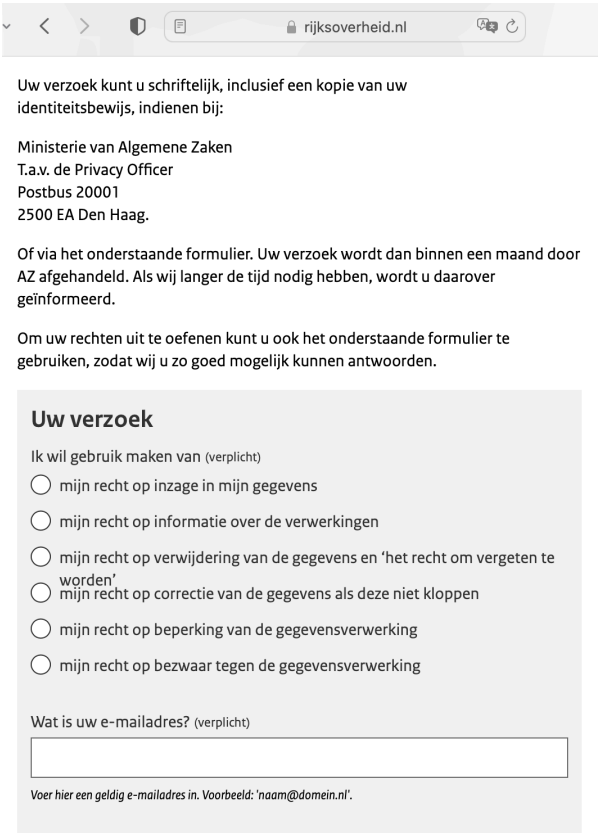


Figuur 4: Drie schermafbeeldingen uit de app MijnGegevens, 'Gedeelde persoonsgegevens'.

Het verschilt van MijnOmgevingen in zoverre ze informatie geven over het doel van de gegevensverzameling of verwerking. Sommige interfaces in de MijnOmgevingen geven expliciet informatie over waar de gegevens voor worden gebruikt (zie figuur 4). Voor andere gegevens die beschikbaar zijn via Mijnomgevingen ontbreekt informatie over het doel van gegevensverzameling, uitwisseling of verwerking. Een voorbeeld hiervan is een brief in MijnUWV over een besluit waarin niet beschreven wordt op welke informatie het besluit is gebaseerd of van welke organisatie die informatie afkomstig is. In het geval van dit onderzoek ging het om een besluit over een zwangerschapsuitkering en de hoogte daarvan. MijnGegevens brengt inzage van verschillende basisregisters bij elkaar. Daarmee is het een atypische versie van een MijnOmgeving.

3.3 Brief schrijven of webformulier invullen

Een tweede categorie van instrumenten die overheidsorganisaties aanbieden aan burgers om hun AVG-rechten uit te oefenen is het schrijven van een brief of een email. Dit is door sommige organisaties toegankelijker gemaakt door een webformulier aan te bieden. Dit type instrument maakt het mogelijk voor burgers om een beroep te doen op hun AVG-rechten. Echter, het gaat hier niet om instrumenten die in hun ontwerp al direct mogelijk maken voor burgers om hun gegevens in te zien, te corrigeren of te verwijderen.

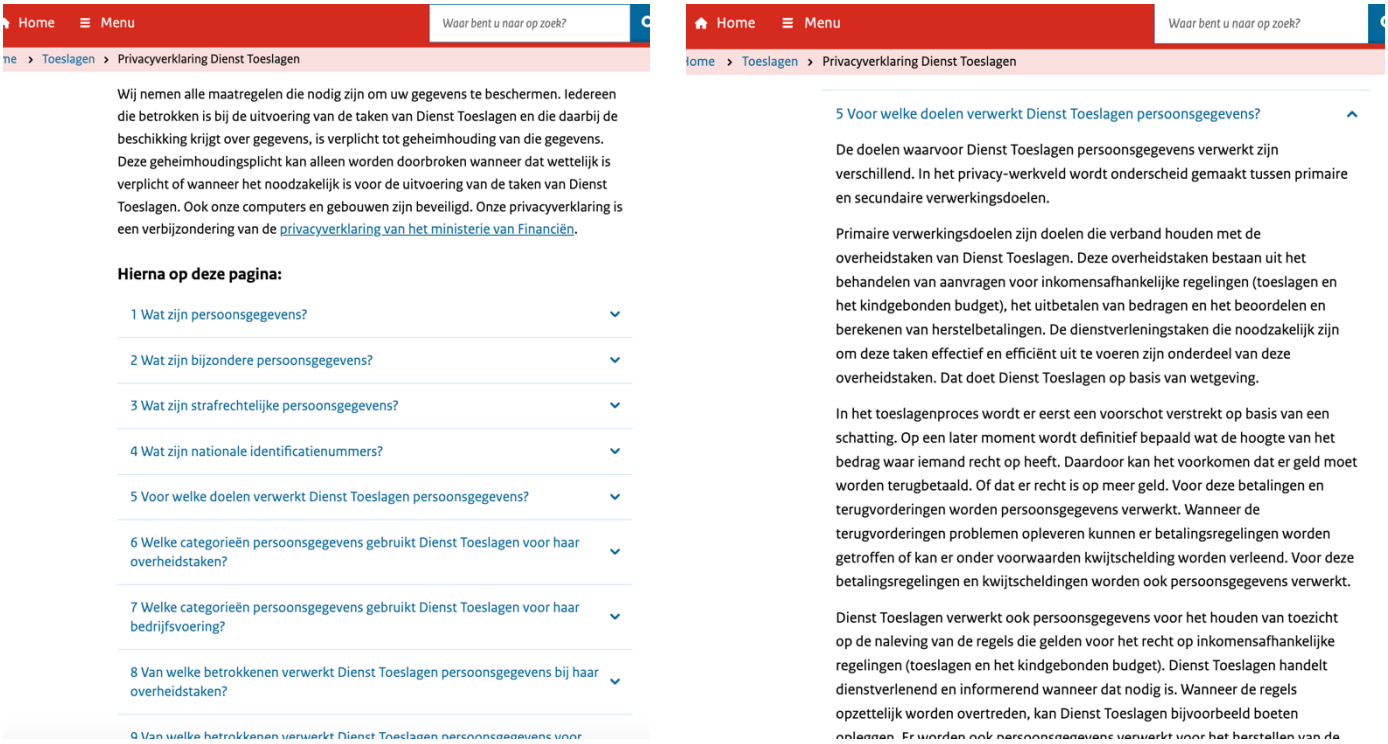


Figuur 5. Schermafbeelding privacyverklaring Ministerie van Algemene Zaken

Burgers die van dit type instrument gebruik maken, moeten al een heel precies idee hebben over de gegevens waar ze naar op zoek zijn of waarvan ze de verwerking willen beperken. Het is waarschijnlijk dat dit instrument wordt gebruikt door burgers die vanwege hun specifieke situatie wensen hebben over gegevensverwerking, of door burgers die problemen ervaren gerelateerd aan een overheid die hun persoonsgegevens verwerkt.

3.4 Privacyverklaringen

Alle overheidsorganisaties hebben privacyverklaringen op hun website. Daarin is voor sommige overheidsorganisaties te vinden welke gegevens ze over burgers mogen verzamelen en verwerken en op basis van welke wettelijke gronden ze dat doen. Privacyverklaringen zijn geen instrument waarmee burgers AVG-rechten kunnen uitoefenen voor hun persoonlijke situatie, maar ze bevatten in een aantal gevallen algemene informatie over het doel voor gegevensverwerking en informatie over ontvangende organisaties. Het recht op deze informatie is vastgelegd in de AVG. Figuur 5 illustreert hoe dit eruit kan zien.



Figuur 6. Schermafbeeldingen privacyverklaring Dienst Toeslagen

Tevens is de privacyverklaring vaak de plek waar vermeld staat *hoe* burgers hun AVG-rechten kunnen uitoefenen - zoals middels het schrijven van een brief, invullen webformulier of indienen klacht, bij de overheidsorganisatie of de Autoriteit Persoonsgegevens.

3.5 Datasluizen en datakluizen

Een derde categorie instrumenten waarmee burgers grip kunnen krijgen en houden op de persoonsgegevens die overheden van hun verzamelen en verwerken, bestaat uit applicaties die soms als sluizen en kluizen worden genoemd. De applicaties bieden aan burgers de mogelijkheid om data van verschillende bronnen op te halen om die met andere organisaties te delen. Deze applicaties zijn in de meeste gevallen door derde partijen (niet overheden zelf) ontwikkeld, maar soms wel in opdracht van overheden. Voorbeelden van deze instrumenten zijn apps zoals Yivi, Qii, Ockto, identiteitsapp IGS Wallet, en Schluss. Qii is een app waarmee burgers gegevens van bijvoorbeeld de belastingdienst en hun bank kunnen ophalen en doorgeven aan een aanbieder van sociale huurwoningen wanneer ze in aanmerking willen komen om een huis te huren. IGS Wallet is ontwikkeld voor een aantal pilots bij verschillende gemeentes, onder andere in Enschede, om het voor burgers met een bijstandsuitkering gemakkelijker te maken om hun maandelijkse inkomsten door te geven aan de gemeente en hun aanvullende bijstand

te berekenen.[12] Deze instrumenten voorzien dus in het doorgeven van data, wanneer dat nodig is om een dienst te ontvangen of aan te vragen.

Datakluizen en datasluizen maken gebruik van het recht dat burgers hebben om data over te laten dragen van een organisatie aan de burger. Daarvoor maken ze veelal gebruik van identificatiemethodes van de overheid, zoals DigiD. Na identificatie kunnen burgers met deze instrumenten een door software leesbare versie van hun gegevens over te dragen aan hen.

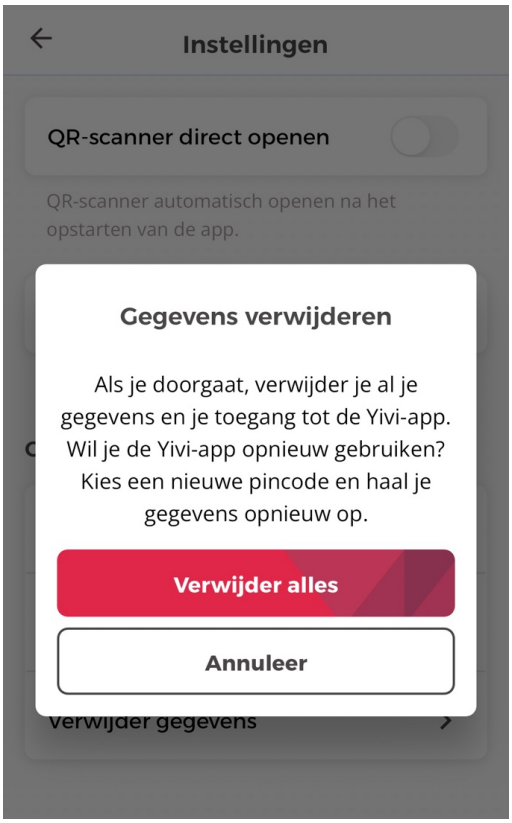
Een belangrijk verschil tussen datakluizen en sluizen is de manier waarop ze data overdragen en opslaan. Een datakluis slaagt gegevens op de telefoon of computer van een gebruiker) op, of in een persoonlijke digitale omgeving. Het principe van een kluis is om gegevens van anderen bronnen opnieuw te verzamelen en op te slaan in een eigen database. In tegenstelling draagt een sluis gegevens over van een databron naar een datagebruiker (of van een server naar een ander server), zonder te gegevens in een tussenstap op te slaan. Sluizen regelen dus de gebruikersidentificatie, toestemming, en het overdragen van gegevens, soms ook het actieve filteren van gegevens om aan eisen van data minimalisatie te voldoen. Er zijn ook belangrijke verschillen hoe kluizen en sluizen naar gegevens toegang krijgen en hoe ze gegevens doorgeven. De app Ockto gebruikt bijvoorbeeld een mix van *screenscrapers* en data filters om gegevens in een sluis te verzamelen, terwijl de app Yivi data door een data interface van de gemeente Nijmegen verzamelt. In de Yivi app kan een burger bijvoorbeeld identiteitsgegevens en adresgegevens ophalen bij diens gemeente (zie figuur 6).

[12] https://ovrhd.nl/portfolio/enschede

Figuur 7. Schermafbeeldingen Yivi app, wanneer een burger persoonsgegevens ophaalt bij Gemeente.

Omdat de burger via deze instrumenten alleen gegevens kan ophalen bij organisaties die de brondata beheren, is het niet mogelijk om gegevens te corrigeren of verwijderen bij de bron. Het is wel mogelijk om de data te verwijderen uit de app, of uit het persoonlijke account bij de app-aanbieder (zie figuur 7).

S ommige van deze instrumenten zijn ontwikkeld om gegevensverwerking te beperken tot enkel wat nodig is voor het verlenen van een dienst. Echter, instrumenten in deze categorie bieden burgers niet de mogelijkheid om specifieke overheidsorganisaties te verzoeken om minder gegevens over hen te verwerken. Datasluizen en kluizen bieden burgers geen mogelijkheid om bezwaar maken tegen verwerking van hun gegevens door overheidsorganisaties. Wel kunnen gebruikers van de instrumenten zich beroepen op dit AVG-recht om de aanbieders van datasluizen en kluizen te vragen om hun gegevens niet meer te verwerken. Op basis van de interface-studie is het niet mogelijk om na te gaan of deze apps informatie geven over het doel van gegevensverwerking. De onderzoekers hebben geen casus lopen waarin ze van deze instrumenten gebruik kunnen maken.



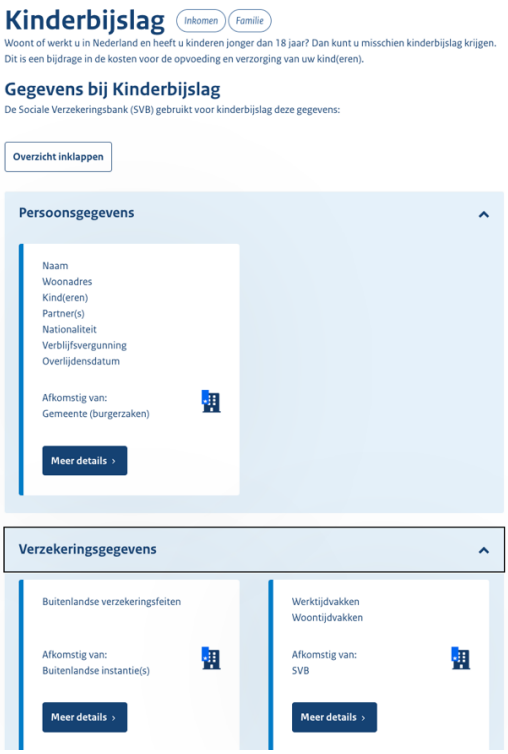
Figuur 8. Schermafbeelding Yivi app, wanneer burger klikt op optie 'Verwijder gegevens'

3.6 Instrumenten voor één doel

In de zoektocht naar instrumenten kwamen we ook instrumenten tegen die niet in bovengenoemde categorieën passen. Zo is er bijvoorbeeld het Meldpunt Fouten in Overheidsregistraties (MFO). Hier kunnen burgers terecht als er gegevens over hen bij een overheidsorganisatie niet kloppen. Het MFO helpt om de fout te corrigeren en ondersteunt ook bij de gevolgen die mensen ondervinden van de fout geregistreerde gegevens, zoals onterechte aanmaningen of boetes. Dit instrument is specifiek ingericht om gegevens te corrigeren en maakt het daarom mogelijk voor burgers om het recht op correctie uit te oefenen. Het MFO werkt samen met o.a. de Belastingdienst, CAK, DUO, Gemeenten, het Kadaster, de Kamer van Koophandel, RDW, SVB, TNO, en UWV.

3.7 Niet gepersonaliseerde instrumenten

Bovenstaande instrumenten geven de mogelijkheid aan specifieke personen om AVG-rechten uit te oefen rond data die over hen verzameld of verwerkt wordt. Er zijn ook instrumenten ingericht die mensen wel in het algemeen informatie geven over de (categorieën) van gegevens die door overheidsorganisaties verzameld en/of verwerkt worden, maar geen informatie geven die is gepersonaliseerd. Een ander instrument dat buiten de bovengenoemde categorieën valt is de website 'gegevensbijbesluiten.overheid.nl'. Deze website geeft op niet-gepersonaliseerde wijze weer welke gegevens worden gebruikt door overheden om besluiten te nemen. Bijvoorbeeld over de toekenning van huurtoeslag, de hoogte van pensioen of het toekennen van kinderbijslag. Er is per besluit te zien welke organisatie het besluit neemt, op basis van welke categorieën gegevens en welke organisaties deze verstrekken. Voor kinderbijslag ziet de informatie die de website verstrekt er zo uit:



Figuur 10: Overzicht van gegevenscategorieën voor kinderbijslag

Een vergelijkbaar instrument vinden de onderzoekers in AVG Verwerkingsregisters. Elke organisatie die persoonsgegevens verwerkt moet een verwerkingsregister maken om aan te tonen dat de organisatie gegevens verwerkt volgens de privacywetgeving. In de verwerkingsregisters van overheden is dus te zien in welke processen ze persoonlijke gegevens van burgers gebruiken en waarvoor. Dit is, wederom, geen gepersonaliseerd instrument om grip op gegevens te houden.

4 Casestudies

Eén van de doelen van dit onderzoek was om te begrijpen welke mogelijkheden en uitdagingen belanghebbenden ervaren bij de ontwikkeling van instrumenten. Dit is van belang om te begrijpen welke infrastructurele, organisatie- en wettelijke factoren de functionaliteiten van instrumenten beïnvloeden en daarmee de mogelijkheden voor 'grip' op persoonsgegevens beïnvloeden. Op basis van interviews en documentenanalyse hebben we casestudies uitgevoerd naar drie instrumenten waarmee burgers grip kunnen houden of krijgen op gegevens die de overheid over hen verwerkt: de MijnGegevens-app van MijnOverheid, de app Yivi en de app Ockto. We zullen eerst de individuele instrumenten bespreken en vervolgens ingaan op de overkoepelende thematiek en onze conclusies.

Ockto: datasluis voor overheidsdatabronnen
Ockto is een app van het type 'datasluis', ontwikkeld door Ockto B.V., opgericht in 2015 in Nederland. Burgers kunnen via de app toestemming verlenen om persoonlijke gegevens bij overheidsbronnen op te halen en door te geven aan financiële dienstverleners zoals woningverhuurders of hypotheekverstrekkers. Die bronnen zijn bijvoorbeeld de Belastingdienst, MijnOverheid of het UWV. Ockto heeft jaarlijks zo'n vijfhonderdduizend tot een miljoen gebruikers die de app gemiddeld eens per jaar gebruiken.

Ockto is ontwikkeld omdat de oprichters een behoefte zagen in de vastgoed- en huursector: er moeten veel gegevens aangeleverd worden door burgers bij toewijzing van een huurwoning of uitgifte van een hypotheek. Denk aan inkomensgegevens, gegevens over schulden of pensioengegevens. Ockto is ontworpen om het aandeel mensen dat direct de juiste informatie aanlevert te verhogen, de gegevenskwaliteit te verbeteren en het proces voor zowel burgers als financiële dienstverleners te versoepelen en versnellen. De primaire klanten van Ockto zijn hypotheekverstrekkers, financieel adviseurs en partijen in de vastgoed- of huursector. Ockto heeft zo'n 70 tot 80 klanten. Deze partijen zijn de 'data afnemers' en betalen voor Ockto. Denk aan ING, Aegon en De Hypotheker. Adviesbureau BS&F adviseert en ondersteunt gemeentes over uitvoeringsprocessen om mensen met een laag inkomen eenvoudig toegang te geven tot zorgverzekeringen, energie en tegemoetkomingen via bijvoorbeeld de 'gemeentepolis' en stadspassen. Het adviesbureau zet Ockto in voor rechtmatigheidstoetsing.

Ockto maakt het mogelijk het AVG-recht op dataportabiliteit uit te oefenen. Data van de overheid kan naar andere organisaties overgedragen worden met toestemming van de burger. Het is niet mogelijk om via Ockto brongegevens te wijzigen. Ook kunnen gegevens niet gewijzigd worden wanneer die worden doorgestuurd naar bijvoorbeeld een hypotheekadviseur. Keuzes over informatievoorziening betreffende de doelen van gegevensverwerking liggen bij de organisaties die een burger om gegevens vraagt.

Om gegevens op te halen, logt de gebruiker binnen de Ockto-omgeving in bij de overheidsorganisaties, waar de app via 'screenscraping' gegevens verzamelt. Vervolgens wordt in Ockto op een rij gezet welke gegevens zijn opgehaald. De gebruiker kan de gegevens bekijken en toestemming verlenen om de gegevens te versturen naar de dienstverlener. De gegevens kunnen door hypotheekverstrekkers voor een periode van negentig dagen geraadpleegd worden, tenzij gebruikers hun toestemming eerder intrekken. De gegevens blijven niet opgeslagen of beschikbaar op de telefoon van de gebruiker. Dit is een keuze van Ockto om de actualiteit van gegevens te garanderen.

De komende periode richt Ockto zich op het veranderende speelveld rond wallets als gevolg van aankomende wetgeving en wallet-ontwikkelingen. Ze zien dat een competitiestrijd gaande is in de Nederlandse markt van wallets om één van de voorkeursoplossingen te zijn voor Nederlandse burgers.

Yivi: datakluis met toegang naar gecertificeerde overheidsdata

Yivi is een smartphone-applicatie voor authenticatie en gegevensuitwisseling, ontworpen als 'datakluis'. Gebruikers kunnen gegevens ophalen uit de basisregistratie persoonsgegevens en het handelsregister. Deze slaan ze op in hun Yivi-app op hun eigen telefoon en worden vervolgens gebruikt voor authenticatie. Zo kunnen inwoners van de gemeente Nijmegen inloggen met Yivi bij MijnNijmegen en een online product of dienst aanvragen met Yivi. De gemeente Amsterdam had een pilot opgezet waarin burgers Yivi kunnen gebruiken om hun meldingen over de publieke ruimte te volgen. De gebruikersaantallen voor Yivi bij dit soort situaties zijn nog kleinschalig. Bij de gemeente Nijmegen loggen maandelijks ongeveer vijfentwintig mensen in op MijnNijmegen met Yivi, tegenover drieduizend via DigiD.

Yivi is oorspronkelijk ontwikkeld onder de naam IRMA – *I Reveal My Attributes* – vanuit onderzoeksactiviteiten binnen de Radboud Universiteit op het gebied van attribuut-gebaseerde authenticatie (zie bijvoorbeeld Alpár en Jacobs 2013). Aanleiding voor ontwikkeling van Yivi was de behoefte aan privacy vriendelijke authenticatie en gegevensuitwisseling met als doel individuen het gevoel te geven meer grip te hebben op het online delen van eigen gegevens. Yivi is ontworpen rond het principe van dataminimalisatie: slechts de attributen van iemands persoonsgegevens worden gedeeld die op dat moment nodig zijn voor de dienstverlening. De app werd verder ontwikkeld vanuit de stichting Privacy by Design en Stichting Internet Domeinregistratie Nederland (SIDN). Vanaf januari 2024 werd Yivi overgedragen aan Stichting Privacy by Design. Het beheer van de app wordt momenteel gedaan door SIDN totdat een andere partij dit overneemt.

Yivi maakt het mogelijk om verwerking van gegevens voor authenticatie zoveel mogelijk te beperken en biedt ook de mogelijkheid om toestemming te verlenen voor gegevensuitwisseling. De app maakt het mogelijk de opgehaalde gegevens uit de BRP in

te zien, maar het is niet mogelijk deze te wijzigen of correcties door te geven bij de bron. De gegevens in Yivi zijn voorzien van een 'echtheidscertificaat', omdat ze via een API worden verstrekt. Omdat er geen directe koppelingen zijn met het BRP of het Handelsregister, worden deze gegevens uitgegeven via de gemeente Nijmegen. De data van de Kamer van Koophandel worden via de identitybroker Signicat in Yivi geupload. De burger is zelf verantwoordelijk voor het up-to-date houden van zijn eigen gegevens.

De gemeente Nijmegen werkt aan het aanpassen van al hun dienstverleningsprocessen op Yivi en hanteert daarbij de principes van dataminimalisatie. Ook door Yivi wordt gewerkt aan meer toepassingen, bijvoorbeeld voor e-herkenning van artsen en vergunningsaanvragen van bedrijven bij de gemeente. SIDN ziet graag dat er meer koppelingen met overheidsdatabronnen komen om meer toepassingen voor Yivi te kunnen ontwikkelen. Dat laat volgens de ontwikkelaars lang op zich wachten.

MijnGegevens: knooppunt voor inzage in basisregistraties
De app MijnGegevens kan als de smartphone versie van de MijnOverheid omgeving gezien worden, zonder de Berichtenbox. Het is in MijnGegevens mogelijk om in te zien welke gegevens over jou als inwoner geregistreerd staan in verschillende basisregisters. Voor de gegevens uit het basisregister persoonsgegevens is het ook mogelijk om te zien welke organisaties deze gegevens mogen raadplegen. De app werd op 30 maart 2022 gelanceerd in appstores en is ontwikkeld door Logius, in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Momenteel ligt de focus in MijnGegevens op inzage van gegevens die bij de overheid over burgers geregistreerd staan. De gegevens die gebruikers kunnen inzien in de MijnGegevens app worden bij gebruik opgehaald via een API. De gegevens worden niet opgeslagen op de telefoon maar alleen getoond. Burgers zijn de voornaamste doelgroep van de app. De overheid heeft de ambitie om MijnGegevens in de toekomst verder te ontwikkelen tot "een plek waar burgers hun persoonlijke gegevens kunnen inzien, via welke zij een onjuist gegeven kunnen laten herstellen, en waar zij regie kunnen voeren over hun gegevens" (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2019). Daarvoor zou een voorziening als het Meldpunt Fouten in Overheidsregistraties geïntegreerd kunnen worden in de app. Het voornemen is dat via MijnGegevens in de toekomst 'brondata' toegankelijk gemaakt kan worden voor wallets, bij wijze van een knooppunt.

4.1 Grip op gegevens: welke noties van grip vinden ontwikkelaars en dienstverleners belangrijk, en welke problemen willen ze ermee oplossen?

Als we overkoepelend naar de casestudies kijken komen inzichten naar voren over de belangen en doelen die centraal staan voor de ontwikkelaars van de instrumenten, met betrekking tot de definitie van 'grip' en de problemen die betrokkenen ervaren bij het

ontwikkelen van deze instrumenten. In onze analyse vestigen we aandacht op de probleemstellingen die ontwikkelaars belangrijk vonden. De probleemstellingen bieden de mogelijkheid voor dialoog over de ontwikkeling van de instrumenten en hoe ze kunnen bijdragen aan meer 'grip op gegevens' voor burgers.

In onze gesprekken met de respondenten vroegen we wat ze verstaan onder 'grip op gegevens'. Uit de interviews blijkt dat de respondenten afwegingen maken tussen een verhoging van het gemak van gegevensuitwisseling en het verkrijgen van meer inzicht voor burgers in hun gegevens. De respondenten zien problemen rond 'datakwaliteit' en dienstverlening, die op basis van 'juiste' gegevens moet worden uitgevoerd. Burgers worden hierbij hoofdzakelijk als bron van mogelijke foutgegevens gezien. Om fouten te voorkomen, en om de efficiëntie van diensten te verhogen noemden meerdere respondenten de overdracht van brondata aan dienstverleners met toestemming van de burger als doel. Uit de interviews komt naar voren dat ontwikkelaars en organisaties die gegevens ontvangen, van mening zijn dat grip op gegevens voor burgers tot uiting komt in oplossingen die:

- zicht bieden op de gegevens die geregistreerd staan, het liefst op één plek;
- zicht bieden op de gegevens die gebruikt worden, en door wie;
- de mogelijkheid bieden om gegevens te delen, en alleen de noodzakelijke, om aan de principes van data minimalisatie te voldoen.

Opvallend is dat respondenten grip op gegevens koppelen aan het verbeteren van datakwaliteit, het versoepelen van diensten, en verhogen van efficiëntie. Hieraan ten grondslag liggen verschillende problemen die de ontwikkelaars zien als belangrijk om op te verhelpen.

Probleem 1: de hoeveelheid organisaties en processen waarmee burgers te maken hebben wordt gezien als bron van stress, radeloosheid en wantrouwen voor burgers. Een oplossing is het centraliseren en versoepelen van gegevensuitwisseling.

Verschillende respondenten zagen als probleem dat burgers vaak dingen moeten regelen op basis van hun gegevens uit basisregisters. Als voorbeelden noemden ze het verkrijgen van een woning, een verhuizing of het aanvragen van kinderopvangtoeslag. Een medewerker van Logius beschreef dat burgers 'radeloos' worden van hoe ze dingen moeten regelen met de overheid en dat dat het vertrouwen negatief kan beïnvloeden:

> *"De burger wordt daar radeloos van. […] Als je al niet eens goed aan de telefoon geholpen kan worden hoe gaat jouw vertrouwen dan groeien? Ja. Dus dat hangt allemaal met elkaar samen. Hoe beter de burger controle kan geven over zijn eigen gegevens, en zijn eigen proces, hoe beter hij snapt waar hij in die processen zit, hoe minder werk er omheen zit voor allerlei partijen. Maar ook hoe meer dat vertrouwen stijgt." – respondent in casestudie MijnGegevens*

Uit de casestudie-interviews komt naar voren dat burgers zouden verdwalen in de hoeveelheid overheidsorganisaties waar ze mee te maken hebben, dat ze niet weten waar ze dingen moeten regelen en dat ze het overzicht verliezen op de gegevens waar overheden hun besluiten en dienstverlening op baseren. Een oplossing hiervoor is overzicht te bieden over gegevens op één plek: één loket waar een burger kan zien welke gegevens geregistreerd staan, waar iemand eventuele fouten kan melden en waar iemand gegevens 'op kan halen' om diensten van zowel overheden als private partijen geleverd kan krijgen. Een toekomstvisie die hierbij aansluit is dat MijnGegevens geïntegreerd wordt met Mijn Berichtenbox en het MFO, en dat dit een koppelpunt wordt waar burgers gegevens kunnen ophalen om die in wallets van derde partijen te laden, zoals Yivi of Ockto.

Probleem 2: er worden te veel gegevens gedeeld die er niet toe doen voor het maken van beslissingen.

Een belangrijk onderwerp voor Yivi en Ockto is het principe van dataminimalisatie waardoor niet méér gegevens zullen worden gedeeld dan nodig voor een bepaald doel. De respondenten van SIDN (Yivi) en Ockto benadrukten dat er geen standaard voor dataportabiliteit bestaat voor het delen van gegevens tussen overheden en derde partijen. Een publieke interface voor derde partijen, zoals een API, ontbreekt, terwijl deze gestandaardiseerde dataportabiliteit mogelijk kunnen maken. Daarom definiëren beide apps dataminimalisatie normen en -technologieën op hun eigen manier.

Als data sluizen en kluizen bieden Ockto en Yivi allebei verschillende oplossingen voor dataminimalisatie. In het geval van processen met Ockto, kunnen burgers gegevens laten ophalen door in te loggen bij overheidsorganisaties waar Ockto de gegevens via screenscraping verzamelt. Vervolgens kunnen burgers de opgehaalde gegevens bekijken en 'toestemming' of 'geen toestemming' verlenen om de gegevens te delen. Belangrijk is dat gebruikers Ockto toegang geven naar hun MijnOmgeving en dat Ockto de gegevens zelf moet afhalen. Ockto gebruikt een filter nadat het gegevens uit de overheidsomgevingen van de gebruikers ophaalt, voordat die gegevens naar de klanten van Ockto gaan. Voor burgers bestaat dus een risico dat Ockto gegevens scrapet en deelt die burgers niet willen delen. Voor Ockto bestaat het probleem dat ze geen standaard interface hebben om gegevens af te halen, wat precies definiërt op welke gegevens het bedrijf toestemming heeft gekregen.

Yivi optimaliseert voor privacy door dataminimalisatie als uitgangspunt te nemen in de app. De gegevens worden opgeslagen in de kluis zodat de burger die Yivi gebruikt ervoor kan kiezen alleen specifieke attributen te delen met dienstverleners of overheden. Denk aan 'ja, ik ben ouder dan 21 jaar' of 'ik ben een geregistreerd arts'. Dit is alleen mogelijk als ook de dienstverlenende partijen hun processen ingericht hebben om met dit soort attributen om te kunnen gaan.

Uit ander onderzoek blijkt dat private data intermediairs een toenemend belangrijke rol spelen om standaarden voor dataportabiliteit te ontwikkelen (Nebbiai 2022). Het probleem is dus niet alleen maar het gebrek aan door de overheid ontwikkelde technologieën die voldoen aan dataportabiliteitsnormen. Het is ook problematisch dat overheden en maatschappelijke organisaties momenteel een kleine of geen rol lijken te spelen in het bepalen van een standaard voor gegevensuitwisseling.

Probleem 3: Burgers worden als probleem voor gegevensuitwisseling gezien omdat ze onbetrouwbare of incorrecte gegevens kunnen produceren.
De instrumenten zijn ontwikkeld om gegevens direct uit betrouwbare (overheids-) bronnen te halen om fouten bij het aanleveren van gegevens door burgers te vermijden. In alle cases brengen respondenten naar voren dat het burgers vaak niet lukt om de juiste gegevens aan te leveren die dienstverleners nodig hebben, met als oorzaak dat het te ingewikkeld is voor hen. Respondenten van Logius, MijnGegevens en Ockto noemen bovendien dat fraude met deze aanleiding een probleem zou kunnen zijn:

> "*Voor het ministerie van Binnenlandse Zaken, directie Wonen was* ook het voorkomen van fraude en bijdragen aan een rechtvaardiger toewijzing van huurwoningen een belangrijk onderwerp. Er werd bijvoorbeeld geknoeid met de pdf's voor inkomensgegevens. *Er waren zelfs bureautjes voor... die dat deden voor woningzoekenden. En ja,* met deze methodiek van gegevensdeling is dat niet mogelijk." – *respondent van Logius*.

De casestudies brengen twee perspectieven op burgers naar voren die kunnen botsen met institutionele belangen. Namelijk de burger als fraudeur en de burger als 'onkundig'.

Incorrecte of verkeerde gegevens leveren een probleem op voor partijen die op basis van die gegevens op rechtmatige en rechtvaardige manier diensten willen leveren aan burgers. Een respondent van Adviesbureau BS&F legt dit verder uit. Het adviesbureau biedt een 'rechtmatigheidsmodule' aan waarin ze Ockto gebruiken om na te gaan of burgers recht hebben op de diensten/producten die ze aanvragen op basis van hun financiële situatie. Volgens de respondent wil een hypotheekverstrekker zeker weten dat hij een hypotheek verleent aan een klant die deze kan afbetalen en moet deze dit ook tegenover toezichthouders kunnen verantwoorden. Een respondent bij Logius vertelde ons dat het Ministerie voor Binnenlandse Zaken en Koninkrijksrelaties hoopt dat de pilot 'digitale inkomenstoets' bijdraagt aan rechtvaardige verdeling van sociale huurwoningen. Hiervoor zal de app MijnGegevens worden gebruikt. Tot slot, gemeentes willen zeker weten dat ze toeslagen of tegemoetkomingen voor zorgverzekeringen of energie verstrekken aan de mensen die daar recht op hebben. Ze willen kunnen verantwoorden dat ze publieke gelden rechtmatig hebben verstrekt.

Betrouwbare bronnen worden als oplossing gezien, gefaciliteerd door toestemming van de burger, om fouten en mogelijke fraude te vermijden. Meerdere respondenten vertelden dat dienstverleners vanwege de datakwaliteit voorkeur geven aan 'brondata' van de overheid,

omdat die meestal als 'correct' worden beschouwd. De term brondata suggereert dat overheden de autoriteit zijn die persoonsgegevens verzamelen en controleren of ze juist en geüpdatet zijn. Gegevensuitwisseling van brondata met toestemming van burgers onderbouwt deze autoriteit omdat burgers de gegevens niet kunnen aanpassen en omdat de data ontvanger erop kan vertrouwen dat ze door de overheid gevalideerd zijn. Als mensen bijvoorbeeld vanuit de basisregistraties op een automatische manier data door een sluis delen, worden de gegevens van een bron direct naar een ontvanger verzonden.

Uit onze interviews blijkt dat de mening verschilt over wie er uiteindelijk verantwoordelijk is voor juiste gegevens. De respondent van Ockto ziet het als verantwoordelijkheid van de overheid om te zorgen dat deze gegevens kloppen, maar is ook ervan op de hoogte dat de gegevens uit de basisregistraties niet voor iedere inwoner 'kloppen'. In het geval van inkomensgegevens, wijst één van de respondenten uiteindelijk de burger aan als verantwoordelijke voor de juistheid ervan: die vult zelf zijn belastingaangifte in.

Probleem 4: Het aanleveren van gegevens in dienstverleningsprocessen vereist kennis, capaciteiten en arbeid wat ervoor kan zorgen dat burgers uitgesloten worden van (overheids)dienstverlening. De oplossing is om een soepele gebruikersroute te ontwikkelen die voor iedereen werkt.
Gerelateerd aan probleem 3, maar met een subtiel verschil: volgens de respondenten vinden burgers het erg lastig om uitgebreide gegevensprocessen te doorlopen. Dit levert vervolgens een probleem op voor overheden en bedrijven die mensen diensten willen leveren op basis van deze gegevens. Volgens onze respondenten willen zij die diensten aan *iedereen* kunnen leveren en dit het liefst op laagdrempelige en toegankelijke wijze. Voor private partijen speelt er een omzetmaximalisatiebelang bij het bedienen van veel klanten. Voor overheden speelt het belang om voor iedereen bereikbaar te zijn.

Een oplossing voor het probleem is optimaliseren voor gebruiksgemak. In alle interviews komt naar voren dat een soepele gebruikersroute belangrijk is voor de ontwikkelaars en belanghebbenden. Deze soepele gebruikersroute bestaat uit heldere stappen, liever niet meermaals moeten hoeven inloggen en wanneer er moet worden ingelogd, vinden ontwikkelaars dat het meest toegankelijkst met het gebruik van inlogmiddelen die de gebruikers kennen en vertrouwen, zoals DigiD.

De soepele gebruikersroute staat in dienst van het zo snel en compleet mogelijk doorgeven van gegevens die overheidsorganisaties of bedrijven nodig hebben om de burgers producten of diensten te leveren. De private partijen benoemen dit als het 'belang van conversie'. Ze willen gebruikers informeren over wat ze aan het doen zijn, maar wegen dat af tegen hoeveel mensen het hele proces doorkomen. Zo wordt in Ockto de keuze gemaakt om informatie over wat iemand precies doet en waarom, alleen beschikbaar te maken met extra klikken voor mensen die daar specifiek naar op zoek zijn.

Grip op data: welke oplossingen voor welke problemen?
Wat kunnen we opmaken uit deze vier probleemstellingen en de manier waarop Ockto, Yivi en MijnGegevens daar oplossingen voor proberen te bieden? De instrumenten dragen in de ogen van dienstverlenende organisaties bij aan gebruiksgemak voor burgers terwijl ze de betrouwbaarheid van data en efficiëntie in bureaucratische processen verbeteren. Dat is voor overheden belangrijk omdat ze graag op rechtvaardige, rechtmatige en kosteneffectieve wijze woningen, toeslagen en tegemoetkomingen willen toekennen aan burgers. Voor marktpartijen is het belangrijk omdat ze sturen op lage kosten per product en omdat ze moeten kunnen verantwoorden dat ze passende diensten leveren aan klanten en daarbij aanvaardbare risico's nemen, zoals bij hypotheekverstrekking. Voor alle geïnterviewden draagt automatische gegevensuitwisseling op basis van principes als dataminimalisatie bij aan privacy en het voorkomen van 'onnodige gegevensdeling'.

De voornaamste reden voor gebruik van de onderzochte instrumenten is gebruiksgemak en versoepeling van gegevens-gebaseerde beslissingen over het toekennen van diensten of producten: van woningtoewijzing tot energietoeslag en hypotheekverstrekking. Respondenten geven aan dat burgers gemakkelijker benodigde gegevens delen door MijnOverheid MijnGegevens of Ockto te gebruiken, dan volgens 'de ouderwetse manier', door het aanleveren van documenten als loonstrookjes, uitdraaien van de belastingdienst et cetera. Dit wordt voor zowel de gegevens-ontvangers als burgers gepresenteerd als een verbetering ten opzichte van de huidige situatie.

De ontwikkelaars van MijnGegevens hebben gebruikersonderzoek uitgevoerd rond de pilot digitale inkomenstoets waarin getest is hoe de app wordt gebruikt voor het uitwisselen van inkomensgegevens met woningcorporaties en voor een digitale inkomenstoets. Het gebruikersonderzoek beargumenteert dat de respondenten (n=25) de gebruikers route via MijnGegevens positief ervaren. Deelnemers omschrijven het als gemakkelijk en snel, en vertrouwen DigiD. Ze ervaren het proces als stress verlagend omdat ze minder kans hebben op het maken van een fout. Een ander onderzoek naar de data kluis Qii, een app wiens functionaliteiten vergelijkbaar zijn met Ockto, beargumenteert dat vertrouwen in woningcorporaties en het toezicht op deze organisaties een belangrijke rol speelt in het vertrouwen van gebruikers in het proces van het delen van gegevens (Mare Research 2021). Hieruit blijkt dat vertrouwen een belangrijke factor is voor gegevensuitwisseling en dat vertrouwen afhankelijk is van het ontwerp van technologieën, maar ook van de ontvangende organisatie, het gegevensgebruik en de specifieke gegevens die worden gedeeld. Uit onderzoek in opdracht van Regie op Gegevens blijkt dat verschillende groepen burgers bereid zijn hun gegevens te delen en in verschillende mate gebruik willen maken van geautomatiseerde gegevensdeling via een intermediair. In plaats van het automatisch delen van gegevens, geven sommige burgers er de voorkeur aan om gegevens persoonlijk door te geven in plaats van digitaal (MarketResponse n.d.). Een intern onderzoek van Logius, gedeeld met

het auteursteam, stelt dat burgers de communicatie en het delen van gegevens willen aanpassen aan hun eigen situatie (Logius 2023).

Uit deze onderzoeken volgt dat burgers de keuze willen hebben in welke communicatiemanieren zij hiervoor geschikt achten. Dit is ook afhankelijk van de mate van vertrouwen die mensen in digitale technologieën hebben. Wanneer er wordt geoptimaliseerd voor bepaalde problemen ontstaat het risico dat vergaande automatisering van gegevensuitwisseling plaatsvindt tussen organisaties over burgers zonder dat deze *zelfbeschikking* hebben om persoonlijke keuzes te maken over de gegevensuitwisseling en de voor- en nadelen van gegevensdeling af te wegen.

4.2. Grip op levenssituaties door gegevensgebruik: relaties tussen burgers en overheden zullen versoepeld worden

De onderzochte instrumenten bieden volgens respondenten 'grip' omdat ze mensen meer controle geven over bepaalde situaties in hun leven. Een soepele, voorspelbare gebruikersroute voor toestemmingsbeheer draagt volgens de geïnterviewden bij aan de grip die mensen ervaren wanneer ze dingen met de overheid of private dienstverleners moeten regelen. Hieronder omschrijven we hoe volgens respondenten de dienstverlening verandert op basis van meer grip op gegevens.

Machstrelaties van dienstverlening blijven ongelijk: gegevensuitwisseling blijft noodzakelijk, maar kan begrensd worden op bepaalde gegevens

Meermaals in de interviews komt naar voren dat de machtsrelatie tussen burgers, de overheid, en dienstverlenende bedrijven ongelijk is. Bepaalde gegevens moeten simpelweg aangeleverd worden als burgers een dienst aanvragen. Welke gegevens voor welke diensten noodzakelijk zijn wordt bepaald door de data-ontvanger die op basis van de gegevens een dienst verleent. Ontwikkelaars van Yivi en Ockto benoemen om die reden dat hun instrumenten met name inzicht geven in welke data wordt gedeeld en met wie, en dat ze daarmee mogelijk willen maken dat gegevensdeling op een soepele manier gebeurt.

> *"Als jij nu gevraagd wordt... je moet je salarisstrook, dit en dit aanleveren... voor je hypotheek aanvragen. En je zegt, die [gegevens] krijg je niet. Dan krijg je je hypotheek niet. Dus je krijgt wel eens die vraag... er is geen keuze voor de burger. Want die burger wil dat product hebben. Of die wil die huurwoning hebben [...]. Waar we wel voor zorgen natuurlijk is dat de hoeveelheid gegevens die of de gegevens die hij aanlevert dat dat gewoon de minimale set is." – respondent in casestudie rond Ockto*

Dit citaat laat zien dat data intermediairs zoals Ockto zich niet als partijen zien die de dienstverlening direct kunnen beïnvloeden, maar wel kunnen zorgen dat dienstverleners enkel toegang krijgen tot de gegevens die voor de dienstverlening nodig zijn.

Geautomatiseerde gegevensuitwisseling kan arbeidsprocessen van gegevenscontroles versnellen en de werkdeling binnen dienstverleners veranderen

Uit de interviews komt naar voren dat zowel overheden, bedrijven als burgers belang hebben bij het minimaliseren van tijd die besteed wordt aan bureaucratische taken als inkomenstoetsen en controle van financiële gegevens. Dit benoemen respondenten in meerdere interviews als een belang van efficiëntie. Bij hun klanten als hypothekenmakelaars zitten hier belangen achter die van doen hebben met de kostprijs van hun product. Bovendien vinden belanghebbenden dat publieksgelden zo efficiënt mogelijk besteed moeten worden.

Burgers, en dan met name de "kwetsbare doelgroep" waar BS&F mee werkt, hebben baat bij snelle afhandeling van aanvragen door de gemeente. Automatisering in hun processen draagt bij aan die snelle afhandeling:

> *"Nou kijk wat ik het mooie vind is dat als ik even vanuit de inwoner perspectief kijk naar hoe je een gemeentelijke regeling moest aanvragen duurde het vaak heel lang. Dus had je soms wel doorlooptijd van vier tot acht weken omdat het formulier nog onderweg moest gecontroleerd worden. En vanuit het inwoner perspectief en helemaal ons doelgroep heb je soms gewoon erg snel belang bij. [...] Ik vind het mooie van Ockto dat we dat proces enorm versneld en geautomatiseerd hebben. Vanuit gewoon het inwoner perspectief, kwetsbare doelgroep waar wij van zijn." – respondent BS&F*

De oplossing die naar voren komt uit de interviews is om processen te automatiseren met instrumenten als Ockto of Yivi. Zo maakt Ockto het mogelijk dat adviesbureau BS&F voor minstens tachtig gemeentes in Nederland geautomatiseerd verschillende eisen kan nagaan waaraan mensen moeten voldoen voor bijvoorbeeld financiële tegemoetkomingen voor zorgverzekeringen, energielevering en stadspassen. Volgens BS&F kunnen databemiddelaars dat voor lage kosten uitvoeren dan in het geval dat gemeentes dat zelf zouden doen.

> *"En je ziet ook gewoon dat je heel veel processen automatiseert. Dus ook gewoon echt heel veel uitvoeringswerkzaamheden gewoon verdwijnen in gemeenten waar we Ockto hebben kunnen installeren. Vooral bij de grotere gemeenten waar je gewoon echt afdelingen had die deze aanvragen voor zorgverzekering deden. [...] Ik weet nog, ik liep een keer bij de gemeente Amsterdam. Daar zijn 80 tot 100 mensen werden aangenomen om de energietoeslag uit te voeren. Ja, dat is uiteindelijk ook samenlevingsgeld. Dus vind ik het op zich mooi dat je dat ook op een andere manier kan doen. Waardoor dat gewoon veel goedkoper kan."* – respondent BS&F

Tools voor de geautomatiseerde uitwisseling van persoonsgegevens worden onderdeel van de werkdeling van publieke dienstverleners. Dienstverlening verandert door de

geautomatiseerde gegevensuitwisseling doordat bureaucratische taken van gegevensverwerking worden vervangen of opgeteld bij functies van data intermediairs als overheden zelf niet genoeg uitvoeringscapaciteit hebben. Het doel is om de bureaucratie bij het aanvragen van diensten te verminderen. Echter, het is onduidelijk of mensen ook betere toegang zullen krijgen tot diensten en of verschillende groepen mensen deze automatisering positief zullen ervaren.

Inzicht in gegevens kan nieuwe interacties tussen burger en overheid in gang brengen, maar inzicht in de gegevens zorgt ook voor problemen voor dienstverleners

Een respondent van Logius denkt dat inzicht in gegevens burgers in staat brengt om diensten en processen in gang te brengen. De respondent benoemt de mogelijkheid of hoop dat huurders in hun MijnGegevens app informatie over de energielabel van hun huis zien, of dat ze zien dat die informatie ontbreekt. Daardoor kan de huurder inzicht in zijn eigen situatie krijgen een bij de huurbaas te informeren over maatregelen die genomen worden om de situatie te verbeteren.

> *"Maar bijvoorbeeld je energielabel. Ja, ik heb echt wel een flinke discussie met mijn huisbaas gehad over het energielabel, die ik nu eindelijk in de app kon zien. Het feit dat het er nu was... dat geeft huurders nu een heleboel stof tot gesprek met hun huisbaas. Van, 'hé, geen energielabel. Ga er eens aan werken. Want ja, dat is een plicht. Waarom heb je geen energielabel?' Dus het geeft mensen een hoop inzicht in hun eigen situatie. Zodat ze daar vervolgens bij de juiste locatie invloed op kunnen uitoefenen."* – respondent van Logius.

Inzicht in data opent op deze manier mogelijkheden om actie te ondernemen om de eigen situatie te verbeteren. Dit is ook de reden dat Logius-respondenten het toekomstideaal schetsen dat MijnGegevens en de Berichtenbox samengevoegd worden en burgers meteen dingen kunnen regelen met hun gegevens.

Aan de andere kant is de zichtbaarheid van gegevens, waar ze vandaan komen en hoe oud ze zijn, ook voor dienstverlenende organisaties belangrijk. Het sluismodel wordt – wat betreft datakwaliteit – in de interviews verkozen boven het kluismodel, omdat dit model de actualiteit van gegevens beter waarborgt dan een kluis. Bij een kluis komt de verantwoordelijkheid voor de actualiteit van gegevens bij de burger te liggen. De reden hiervoor is dat een kluis de gegevens van een burgers in een persoonlijke cloud of op een persoonlijk apparaat opslaat. Daardoor is het zichtbaar voor dienstverlenende organisaties wanneer de gegevens werden opgehaald uit de databron, maar niet of de gegevens in de tussentijd worden geüpdatet in de bron. De bovengenoemde spanning tussen betrouwbaarheid van gegevens en handelingsvermogen van burgers wordt hier weer duidelijk. Het is niet mogelijk voor dienstverlenende partijen om de data dan zelf opnieuw op te halen. Het enige wat ze kunnen doen is de burger vragen om de gegevens opnieuw op te halen, wanneer ze vinden dat de gegevens niet actueel genoeg

zijn. Tegelijkertijd geeft een respondent van de gemeente Nijmegen de voorkeur aan het kluismodel om mensen controle over gegevens te geven, omdat alleen de burger zelf kan zien met wie zijn gegevens worden gedeeld. De zichtbaarheid van gegevens is dus gekoppeld aan de bredere vraag van vertrouwen en wat er meer belang heeft: de controleerbaarheid van gegevensafkomst en inzicht in updates voor gegevensontvangers, of meer controle voor burgers over gegevens?

Wat als het misgaat voor een burger?

Tot nu toe zien we dat de instrumenten optimaliseren voor soepele gegevensuitwisseling en inzicht in de gegevens van gebruikers. Automatisering rond de basisregisters van de overheid staat centraal. Maar wat als die gegevens voor mensen niet kloppen? Of als die gegevens in mensen hun nadeel werken? In het kader van het programma Regie op Gegevens is er weinig gebruikersonderzoek gedaan naar het perspectief van mensen voor wie deze gegevens niet kloppen. Personen die over het algemeen benadeeld of gediscrimineerd worden, of die mee hebben gemaakt dat beslissingen over hen werden gemaakt waar ze het niet mee eens waren. Bestaand gebruikersonderzoek rond Ockto, Yivi en gegevensuitwisseling via MijnGegevens (MarketResponse 2021; Mare Research 2022) geeft inzicht in hoe respondenten de app gebruiken, het gegevensuitwisselingsproces doorlopen en of ze het proces vertrouwen, maar biedt geen inzicht in de situatie waarbij de gegevens van burgers niet juist zijn.

Volgens een respondent van Ockto kloppen de gegevens van hun gebruikers over het algemeen wel. Toch weet de respondent dat 'heel veel [...] uitzonderingetjes' voorkomen. De respondent noemt als voorbeeld onjuiste geboortedata in de basisregistratie van migranten die in de jaren zeventig naar Nederland zijn geëmigreerd. Een ander voorkomend probleem is dat persoonsgegevens in de ene administratie, niet overeenkomen met de persoonsgegevens in een andere administratie. De respondent ziet het als taak van de overheid om die informatie op orde te krijgen. Volgens meerdere respondenten bieden noch Yivi en Ockto noch MijnGegevens momenteel mogelijkheden aan om vanuit de app aan de bel te trekken wanneer gegevens niet kloppen.

> "*Als het niet klopt, dan zal hij [de burger] zijn gegevens niet delen. En dan moet hij inderdaad via de reguliere wegen bij de belastingdienst aankloppen. Daar hebben wij geen extra informatie in voorzien.*" – respondent van Logius.

Logius heeft wel de ambitie om burgers bij MijnGegevens te informeren over wat ze kunnen doen als gegevens niet kloppen, en daar meteen mee aan de slag kunnen.

> "*Wij [Logius] zijn alleen maar degene die het ontsluiten. De burger kan niet de gegevens wijzigen. De burger kan bijvoorbeeld wel het e-mailadres wijzigen wat in MijnOverheid staat. Waarvan je zegt daarop wil ik notificaties van MijnOverheid ontvangen. Maar dat gaat dan echt over de website of over de app. Als jouw gegevens bij de gemeente niet goed staan, daar kunnen wij niks aan veranderen. Dat moet je toch echt bij de gemeente dan oplossen. Dus je hebt dan nog steeds*

wel met al die losse diensten te maken. Alleen gaan wij wel kijken hoe kunnen wij die diensten dan zo makkelijk mogelijk voor je bereiken. Dus we hebben nu in dat ontwerp het onderzoek ook gekeken. Hoe zou je dan willen communiceren met al die partijen? Zou je dat dan via MijnOverheid website al gelijk willen doen? Dat je daar een soort chat kan opstarten. Om al met jouw gemeente te communiceren. Of ga je liever naar een aparte website van je gemeente? Log je daarin? Dus dat zijn allemaal pilots die we doen om te kijken hoe de burger geïnformeerd wil worden." – respondent van Logius

Burgers hebben momenteel met verschillende organisaties te maken als er iets misgaat of niet klopt, terwijl het creëren van één centrale plek en een versoepelde ervaring centraal staat om geautomatiseerde gegevensdeling te faciliteren. Wat hierbij ook zichtbaar wordt is het beperkte handelingsvermogen van data-intermediairs om gegevens te corrigeren of een mediatierol in te nemen als er iets misgaat met de dienstverlening. Op dit moment zien ze hun rol als partijen die de processen tussen databronnen en data afnemers kunnen versoepelen of de communicatie met verschillende diensten verder door te ontwikkelen. Uit gebruikersonderzoek van Logius en Regie op Gegevens blijkt dat mensen oplossingen willen die zijn afgestemd op hun persoonlijke situatie. Deze bevindingen zijn een belangrijke stap om bestaande instrumenten aan te passen en om ze niet alleen toegankelijk te maken voor een breed groep aan gebruikers, maar ook voor burgers die kwetsbaar zijn of problematische situaties ervaren met betrekking tot het gebruik van hun gegevens.

4.3. Grip op levenssituaties door infrastructuur: wettelijke en technologische uitdagingen en vragen

Overheden spelen als databronnen een belangrijke rol voor het waarborgen van de rechten van burgers, omdat ze voorwaarden kunnen stellen aan de manier waarop data intermediairs toegang krijgen tot de gegevens. Tot nu toe verschilt per instrument de manier waarop privacy als ontwerpwaarde dient. Privacy en veiligheid komen bij Yivi tot uiting in hun keuze om alleen gecertificeerde data op te halen via API's - en niet middels *screenscraping*, zoals Ockto doet. Op dit moment zijn er nog niet veel bronnen opengesteld door De Rijksoverheid, waardoor de gebruikscases voor Yivi nog beperkt zijn. De reden hiervoor is dat gebruikers van Yivi alleen maar toegang hebben tot gegevens uit de Basisregistratie Personen via de gemeente Nijmegen en tot gegevens uit het Handelsregister via een derde partij. Ockto, aan de andere kant, heeft een duidelijke waarde propositie kunnen opbouwen voor klanten en beschikt over grote gebruikersaantallen.

Ontbreken van API's

Gegevens uit de basisregistraties worden in het algemeen niet aan marktpartijen ontsloten via API's. Er bestaan wel koppelingen tussen overheidsorganisaties, zoals tussen het BRP, de Belastingdienst, Kadaster en DUO naar de MijnGegevens app, maar

niet naar externen. Ockto geeft aan dat ze graag met API's zouden werken, maar bij gebrek daaraan *screenscraping* toepassen om data te verzamelen.

> *"Maar nog steeds hangt er rondom wat wij als Ockto doen... hangt er bij een deel van de overheid iets van... Hé, dat is screenscraping, dus dat vinden wij maar niks. Terwijl wij ook zeggen, het is prima secure... want het is maar net hoe je er mee omgaat. Maar goed, even los daarvan, wij zouden ook het liefst... via APIs met de overheid werken."* – Respondent Ockto

Bij screenscraping logt een burger in bij persoonlijke overheidsomgevingen en vergaart Ockto gegevens door de HTML-code van de weergegeven schermen te scannen op relevante data. Het probleem hierbij is dat Ockto door screenscraping de gegevens uit de MijnOmgevingen van burgers haalt zonder dat burgers en overheden kunnen controleren welke gegevens worden opgehaald. Onafhankelijk van de manier waarop gegevens worden gedeeld, is het volgens de respondent van Ockto belangrijk dat de partijen die gegevens willen uitwisselen betrouwbaar zijn en onder toezicht staan.

In het algemeen is dit soort gegevensverzameling niet gestructureerd en ook niet door servicevoorwaarden vanuit de overheid geregeld. Deskundigen van de universiteit Utrecht hebben hier tegenover een concept van een 'wettelijke compliance API' (Goanta, Bertaglia, Iamnitchi 2022) ontwikkeld waardoor de rechten van burgers in de context van data-uitwisseling kunnen worden gedefinieerd en gewaarborgd. Vanuit het perspectief van privacyberscherming maar ook compliance hebben verbindingen via API's de voorkeur in plaats van screenscraping. Ontwikkelaars geven aan dat apps zoals Ockto zich nu in een grijs gebied begeven. Respondenten van Logius benoemen dat zulke werkwijzen nu worden gedoogd, omdat het duidelijk is dat ze in een specifieke behoefte voorzien. Ook geeft een respondent van Ockto aan dat ze graag willen dat gebruikers kunnen inloggen met behulp van de DigiD-app, maar zorgt de wisselende positie vanuit overheidsinstellingen ervoor dat er nog geen DigiD-aansluiting beschikbaar is.

Er lijkt momenteel onduidelijkheid te zijn bij de respondenten over wat er wel en niet is toegestaan. Volgens respondenten van SIDN en Ockto neemt de overheid hier tot nu geen definitieve positie over in. De respondenten en hun klanten zijn afhankelijk van de gegevens die worden opgehaald uit overheidsbronnen. In het geval van Ockto heeft dit te doen met het gebrek van gestructureerd toegang tot de gegevens door een API. Ockto is voor de betrouwbaarheid van hun processen afhankelijk van de beschikbaarheid van overheidsdiensten waarvan de app de gegevens tot nu afhaalt door scraping. Meer werk is nodig om gemeenschappelijke standaarden te ontwikkelen op basis van de concrete behoeften van personen, hun mening over de gevoeligheid van gegevens en uiteenlopende gebruikscontexten. Experts op het gebied van gegevensbescherming, rechtsdeskundigen en ethici zijn het nog steeds niet eens welke varianten van gegevensdeling de voorkeur krijgt. Een recent discussies rond data altruïsme organisaties en data donaties door het gebruik van sluizen en kluizen laat zien dat

onafhankelijke kennisinstellingen en maatschapelijke organisaties een belangrijk rol kunnen spelen om standaarden voor gegevensuitwisseling te ontwikkelen (Veil 2021). Zo leidde het delen van gezondheidsgegevens in Duitsland tijdens de COVID-19-pandemie tot een publieke discussie over het acceptabele delen van gegevens voor datadonaties via de Corona-datadonatie-app. De betrokkenheid van de Chaos Computer Club zorgde ervoor dat diverse veiligheidslekken vroegtijdig konden worden gedicht en dat er een debat over dataminimalisatie plaatsvond (Tschirsich, Jäger, and Zilch 2020).

Wetgeving belemmert geautomatiseerde gegevensuitwisseling

Wetgeving maakt de ontwikkeling van data-intermediairs mogelijk. De AVG-wet bijvoorbeeld, legitimeert de ontwikkeling van apps als Ockto en Yivi omdat ze rechten op inzage, portabiliteit en andere rechten definieert. Tegelijkertijd belemmert andere wetgeving de ontwikkeling van apps zoals Ockto, Yivi en MijnGegevens. De uitdagingen die wetgeving biedt voor de ontwikkeling van instrumenten hebben onder andere betrekking op de juridische mogelijkheden voor gegevensverwerking en –deling vanuit de basisregistraties.

Alle burgers in Nederland die Yivi gebruiken, integreren hun BRP-gegevens in de app via de gemeente Nijmegen. Gemeentes zijn de enige partij die BRP-gegevens mogen uitgeven aan burgers. Volgens een respondent van de gemeente Nijmegen kan de gemeente de gegevens alleen maar verstrekken aan mensen die Yivi gebruiken, omdat Yivi een persoonlijke kluis is, in eigendom van de burger. Gemeente Nijmegen verstrekt de BRP-gegevens dus technisch gezien aan de burger, en niet aan een organisatie. Gebruikers van Yivi kunnen gegevens uit het handelsregister ophalen via een identiteitsbroker.

Een andere vraag ging over het uitwisselen van identiteitsgegevens. Een respondent noemde als voorbeeld een functie om BSN-nummers te delen via een API bij MijnOverheid. Hier liepen ontwikkelaars tegen juridische mogelijkheden voor gegevensuitwisseling aan als ze de app wilden gebruiken voor een pilot met woningcorporaties. Het doel van de pilot was om de inkomenstoets voor sociale huurwoningen bij toewijzing van een woning uit te voeren met gegevens uit het Basisregister Inkomen, welke in beheer staat van de Belastingdienst. Om de inkomenstoets uit te voeren loggen burgers bij toewijzing van een woning in via DigiD en worden de inkomensgegevens opgehaald vanuit het Basisregister Inkomen vanuit MijnGegevens en wordt deze informatie vervolgens doorgegeven naar de woningcorporaties. De woningcorporaties controleren vervolgens of het inkomen binnen bepaalde grenswaarden valt. Om de controle uit te voeren hadden de woningcorporaties ook identificerende gegevens, zoals naam en geboortedatum, nodig om de inkomensgegevens mee te matchen.

Hier ontstond een probleem. Het Ministerie van Binnenlandse Zaken, onderdeel van de pilot en verantwoordelijk voor de Rijksdienst voor Identiteitsgegevens (RvIG), mag geen

gegevens uit de BRP verstrekken aan burgers omdat dat alleen toegestaan is voor gemeentes. Daarnaast is op basis van een tussentijdse evaluatie van de pilot de richting uitgezet om gebruik te maken van het BSN in plaats van de eerdergenoemde identificerende gegevens om eenduidige identificatie mogelijk te maken. Ook dat leverde een probleem op, omdat het voor woningcorporaties niet toegestaan was het BSN te verwerken. Dit heeft geleid tot een voorstel voor het aanpassen van de Woningwet die het mogelijk maakt voor corporaties om voor dit doeleinde het BSN te gebruiken. Dit voorstel is per 1 februari 2024 in effect getreden. Tegenwoordig mogen corporatie die daartoe op eigen verzoek aangewezen zijn door de minmister BZK het BSN verwerken om eenduidig vast te stellen dat het inkomen bij de woningzoekende hoort die zich heeft ingeschreven. Deze nieuwe procedure wordt vanaf april landelijk ingevoerd. Zo kan elke toepassing voor gegevensuitwisseling via MijnGegevens lopen tegen andere, domeinspecifieke, wetgeving over het delen en verwerken van gegevens uit de basisregistraties.

5 Conclusies en aanbevelingen

In dit onderzoek onderzochten we welke instrumenten er bestaan om burgers meer grip te geven op hun gegevens. We vroegen ons af hoe de AVG-rechten worden vertaald in technologieën, hoe deze technologieën zijn ingebed in organisatorische praktijken en netwerken van overheden en voor welke doelen burgers hun rechten kunnen uitoefenen. Om deze vragen te beantwoorden stelden we de volgende onderzoeksvragen:

1. Welke initiatieven en technologieën bestaan er in Nederland om mensen controle te geven over de gegevens die overheden van hen verwerken?
2. Welke AVG-rechten kunnen worden uitgeoefend en over welke gegevens?
3. Welke mogelijkheden en uitdagingen zien belanghebbenden bij de ontwikkeling van instrumenten en hoe kan dat van invloed zijn op wie de controle heeft over bepaalde persoonsgegevens.

Deze vragen zijn om verschillende redenen belangrijk: AVG-rechten spelen een centrale rol voor burgers om grip op data uit te oefenen. Daarnaast zijn ze van belang om grip over levensomstandigheden te krijgen en om de relaties tussen burgers, overheden, dienstverleners een maatschappelijke organisaties opnieuw vorm te geven.

Bij de interacties tussen samenleving en overheid, maar ook bij de uitvoering van publieke diensten, zijn steeds vaker algoritmische technologieën en digitale data betrokken. Verschillende partijen willen toegang en controle over deze gegevens en er zijn uiteenlopende belangen verbonden aan het gebruik ervan. Inzicht in bestaande instrumenten laat zien voor welke AVG-rechten en binnen welke contexten instrumenten worden ontwikkeld. Daarnaast werpt het licht op welke rechten bij de verschillende instrumenten een rol spelen, en welke momenteel nog achterblijven.

5.1 Conclusies

Op basis van ons empirisch onderzoek van 109 instrumentinterfaces, expertinterviews en documentanalyse, concluderen wij het volgende:

Het is een positieve ontwikkeling dat overheden steeds meer instrumenten ontwikkelen die verder reiken dan de gebruikelijke ‘instrumenten’ zoals verklaringen of brieven over gegevensbescherming. Hieruit blijkt dat de overheid steeds meer uitvoering geeft aan de doelstellingen van het programma Regie op Gegevens om de rechten op inzage, correctie en dataportabiliteit te bevorderen. Daarnaast draagt het bij aan een verbetering van grip dat partijen als Regie op Gegevens en Logius naast de ontwikkeling van instrumenten ook gebruikersstudies uitvoeren. Wat uit deze onderzoeken naar voren komt, is een genuanceerd beeld van de eisen en behoeften die mensen hebben bij de interactie met overheden en openbare dienstverlening via digitale diensten. Hieruit blijkt

dat de overheid de problematiek serieus neemt en actief investeert in de ontwikkeling van instrumenten.

Het onderzoek biedt inzicht in beperkende factoren over hoe deze tools de uitvoering van AVG-rechten vertalen in technologieën, welke problemen de tools moeten oplossen en wie verantwoordelijkheid draagt is voor de implementatie van uiteenlopende functionaliteiten.

Burgers worden geconfronteerd met veel individuele oplossingen: we zien ook dat instrumenten door veel verschillende partijen worden ontwikkeld en geïmplementeerd worden. Er zijn weinig overkoepelende instrumenten aan de kant van de overheid. In plaats daarvan implementeren ministeries, gemeenten en uitvoeringsorganisaties individuele instrumenten, wat resulteert in een reeks van meer dan 100 individuele instrumenten. Commerciële bedrijven bouwen vooral instrumenten voor dataportabiliteit. Het ministerie van Binnenlandse Zaken is met prototypen begonnen om MijnGegevens als een knooppunt voor andere databemiddelaars te gebruiken. Uit de casestudies komt naar voren dat de ontwikkelaars en organisaties die met persoonlijke gegevens van burgers werken van mening zijn dat controle over gegevens nog steeds verbeterd kan worden door oplossingen te bieden die burgers inzicht geven op de gegevens die geregistreerd staan – bij voorkeur, op één centrale plek. Daarnaast zou het bevorderlijk zijn als een centrale omgeving men zelf in staat stelt om toestemmingen te verlenen voor het gebruik, delen en bekijken van (noodzakelijke) persoonlijke data. Echter, tot nu is het onduidelijk voor de betrokken partijen hoe instrumenten voor dataportabiliteit zullen gaan samenwerken.

Instrumenten besteden selectief aandacht aan sommige AVG-rechten (niet aan alle): via interface-analyse van 109 instrumenten constateren we dat instrumenten selectief worden ontwikkeld voor AVG-rechten en dat burgers vaak beperkte functionaliteiten hebben om gegevens te controleren. Uit ons onderzoek blijkt dat burgers in de meeste gevallen hun rechten op inzage, correctie, en dataportabiliteit kunnen uitoefenen. Het sturen van een brief blijkt het meest gebruikelijke instrument om gegevens te verwijderen, het delen van gegevens tussen overheidsinstanties te beïnvloeden of om klachten in te dienen over hoe gegeven verzameld en gebruikt worden. Burgers kunnen altijd een klacht indienen bij de Autoriteit Persoonsgegevens. Over het algemeen bieden de instrumenten burgers inzicht in datacategorieën en maken ze het doorvoeren van correcties op gegevens mogelijk. Op welke manier deze gegevens gebruikt worden voor dienstverlening door overheidsorganisates, blijft voor de burger vaak nog onduidelijk. De bevindingen uit gebruikersonderzoeken lijken nog niet te zijn geïmplementeerd. Deze suggereren dat burgers vormen van interactie met de overheid (digitaal en analoog) willen die geschikt zijn voor hun persoonlijke situatie.

Bureaucratische processen zullen efficiënter worden ingericht, maar hoe burgers publieke diensten ervaren is nog onduidelijk: instrumenten stellen als doel om de

bureaucratie van het gegevensproces te verminderen, maar het is onduidelijk hoe dit de ervaringen van publieke diensten beïnvloed: Uit onze casestudies blijkt dat de drie onderzochte instrumenten bedoeld zijn om specifieke problemen met publieke dienstverlening op te lossen. Op basis van onze interviews blijkt dat overheidsbelangen hierbij vaak een rol spelen. De voornaamste reden voor gebruik van de onderzochte instrumenten is gebruiksgemak en een versoepeling van gegevens-gebaseerde beslissingen over het toekennen van diensten of producten. Ook valt het op dat de mate van grip op gegevens aan datakwaliteit en efficiëntie wordt gekoppeld om bureaucratische processen en werk te verminderen. Dat is voor overheden belangrijk omdat ze graag op een rechtvaardige, rechtmatige en kosteneffectieve wijze woningen, toeslagen en tegemoetkomingen willen toekennen aan burgers. Voor marktpartijen is het belangrijk omdat ze sturen op lage kosten per product en omdat ze moeten kunnen verantwoorden dat ze passende diensten leveren aan klanten en daarbij aanvaardbare risico's nemen, zoals bij hypotheekverstrekking. Volgens de respondenten zouden data sluizen en kluizen voor de burgers de lasten verminderen bij bureaucratische processen. Of mensen hierdoor de dienstverlening beter ervaren, of dat ze daadwerkelijk betere toegang krijgen tot bepaalde diensten, is onduidelijk op basis van onze resultaten uit de interviews.

Onduidelijke technische en juridische randvoorwaarden beperken de implementatie van instrumenten voor dataportabiliteit: er bestaat tot op heden geen gestructureerde toegang tot gegevens uit de basisregisters voor data bemiddelaars. Sommige instrumenten gebruiken screenscraping om gegevens uit accounts van burgers te halen in plaats van een Application Programming Interface (API). Daardoor hebben burgers en eventuele andere databronnen minder invloed op het delen van gegevens. Een andere app maakt gebruik van toegangsrechten van individuele steden om gegevens uit basisregisters op te vragen. Daarom ontbreekt het nog aan een gestandaardiseerde aanpak om de ontwikkeling van instrumenten voor gegevensuitwisseling te ondersteunen en rechten en plichten duidelijk vast te leggen.

5.2 Aanbevelingen

Voor de verdere ontwikkeling van instrumenten is het van belang samenwerkingen tussen beleidsmakers, uitvoeringsorganisaties, betrokkenen burgers, maatschappelijke organisaties, onderzoeksinstellingen en commerciële partijen te bevorderen. Op basis van ons onderzoek doen we de volgende aanbevelingen.

We roepen beleidsmakers binnen de overheid op om:

Technische standaarden voor gegevensuitwisseling (bijvoorbeeld APIs) te ontwikkelen waarbij de rechten van burgers centraal staan. API's spelen een cruciale rol in de machtsverhouding tussen burgers en de overheid, omdat ze verschillende rechten kunnen verankeren. Deze rechten omvatten het recht op

inzage in waar persoonlijke data zich bevindt, welke overheidsinstanties data delen, wat er met die data gebeurt, en wie hierop controle mag uitoefenen. Het zou in lijn zijn met de AVG om open standaarden te gebruiken en te zorgen dat verschillende organisaties met toestemming van burgers gegevens kunnen opvragen.

Nog beter zou het zijn om een brede maatschappelijke discussie te voeren over welke normen ten grondslag moeten liggen aan de ontwikkeling van API's. Naast burgers zouden ook maatschappelijke organisaties en onderzoeksinstellingen die zich met deze vraagstukken bezighouden, aan deze discussie moeten deelnemen.

- **Toezichtkaders op een uniforme manier binnen overheidsorganisaties te implementeren:** de rollen, rechten en plichten van overheden en commerciële data bemiddelaars moeten duidelijk worden gedefinieerd en actief worden gecontroleerd door de overheid. Het is van cruciaal belang om transparant te zijn over dit beleid richting de samenleving. Bovendien is het belangrijk om input te krijgen vanuit maatschappelijke hoeken bij de ontwikkeling van deze toezichtskaders en bij de implementatie ervan.
- **Eigenaarschap van gegevens in de handen van burgers te leggen:** Overheden kunnen ook het beheer van data overdragen aan de burgers zelf. Een voorbeeld hiervan is België, waar de Vlaamse overheid streeft naar de ontwikkeling van individuele 'solid pods', een soort datakluisjes waarmee burgers hun eigen data kunnen beheren. In dit systeem moet de overheid toestemming vragen aan burgers om de data te delen die zij nodig heeft. Hierdoor keert de machtsdynamiek om en wordt de burger daadwerkelijk de primaire beheerder van gegevens.

We roepen ontwikkelaars van instrumenten op om:

- **Burgers meer inzicht te geven** in welke persoonlijke gegevens op welke manier worden gebruikt bij de totstandkoming van voor hen relevante besluitvorming.
- **Aandacht te geven aan de rechten van burgers en hen meer controle te geven wanneer er iets misgaat in de verwerking van persoonsgegevens.** Tot nu toe zijn er geen diensten beschikbaar die burgers de kans geven om fouten in de omgang met hun data door overheden te herstellen, waardoor ze mogelijk toeslagen, sociale bijstand of andere zaken mislopen terwijl ze daar wel recht op hebben.
- **Rekening te houden met de digitale kloof**. Een deel van de burgers (20% in Amsterdam) heeft geen toegang tot digitale technologieën, door weinig financiële middelen of een gebrek aan digitale vaardigheden. Als overheidsinstellingen hun diensten digitaal aanbieden, dan kan dat deze groep mensen benadelen. Daarom is het belangrijk om een analoog aanbod te creëren, bestaande uit toegankelijke

contactpersonen en processen, zodat burgers ook zonder digitale technologie controle kunnen uitoefenen op hun gegevens.

- **Maatschappelijke organisaties te betrekken** in de ontwikkeling en het gebruik van instrumenten om de ervaringen van kwetsbare groepen in kaart te brengen.

We roepen overheden, uitvoeringsorganisaties en andere publieke dienstverleners op om:

- **De instrumenten te ontwikkelen waarmee burgers grip krijgen op hun gegevens als onderdeel van de totale dienstverlening aan burgers.** Dit betekent dat de ervaring van de burger centraal moet staan bij de ontwikkeling. Dit vereist het in kaart brengen van verschillende situaties en behoeften van burgers, en op basis daarvan het ontwikkelen van een verscheidenheid aan technische hulpmiddelen, diensten en processen die burgers helpen hun rechten tegenover de overheid uit te oefenen.
- **Aandacht te geven aan kwaliteitseisen van data-gebaseerde dienstverlening.** Met het toenemende gebruik van gegevens binnen de digitale welvaartsstaat is het essentieel dat de overheid de kwaliteit van haar diensten op het gebied van gegevensbeheer voortdurend controleert. Het is belangrijk dat burgers niet de dupe worden van geautomatiseerde processen voor gegevensverwerking. Burgers moeten erop kunnen vertrouwen dat de diensten in hun belang worden geleverd, wat betekent dat de overheid de verantwoordelijkheid draagt om ervoor te zorgen dat automatisering geen extra problemen voor hen oplevert.

We roepen maatschappelijke organisaties op om:

- **AVG-rechten en instrumenten voor het verkrijgen van 'grip' in te zetten als methode** in hun werk; bijvoorbeeld door voor groepen burgers het recht op inzage uit te oefenen om, indien nodig, bezwaar te kunnen maken tegen gegevensverwerkingsprocessen in publieke en private dienstverlening.
- **Met overheden en ontwikkelaars in contact te komen** om de belangen van kwetsbaren groepen binnen het ontwerpproces te vertegenwoordigen**.**

We roepen onderzoeksinstellingen op om

- **Inzicht te bieden** in de wettelijke en sociale implicaties van verschillende typen instrumenten op basis van actuele discussies over het delen van gegevens.

Literatuur

Algemene Rekenkamer, 2014. https://www.rekenkamer.nl/publicaties/rapporten/2014/10/29/basisregistraties

Algemene Rekenkamer, 2019. Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven. Den Haag.

Alpár, Gergely, and Bart Jacobs. 2013. "Towards Practical Attribute-Based Identity Management: The IRMA Trajectory." In *Policies and Research in Identity Management*, edited by Simone Fischer-Hübner, Elisabeth De Leeuw, and Chris Mitchell, 396:1–3. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37282-7_1.

Bernholz, Lucy. 2021. *3. Purpose- Built Digital Associations*. *Digital Technology and Democratic Theory*. University of Chicago Press. https://www.degruyter.com/document/doi/10.7208/9780226748603-004/pdf.

Enthoven, Guido, Amber van Bergeijk, and Serv Wiemers. 2023. "Over Schone Dromen En Verbroken Beloften. 25 Jaar ICT, Overheid En Samenleving." Instituut Maatschappelijke Innovatie.

Fiske, Amelia, Alexander Degelsegger-Márquez, Brigitte Marsteurer, and Barbara Prainsack. 2022. "Value-Creation in the Health Data Domain: A Typology of What Health Data Help Us Do." *BioSocieties*, April. https://doi.org/10.1057/s41292-022-00276-6.

Gray, Jonathan, Carolin Gerlitz, and Liliana Bounegru. 2018. "Data Infrastructure Literacy." *Big Data & Society* 5 (2): https://doi.org/10.1177/2053951718786316

Hummel, Patrik, Matthias Braun, and Peter Dabrock. 2020. "Own Data? Ethical Reflections on Data Ownership." *Philosophy & Technology*, June. https://doi.org/10.1007/s13347-020-00404-9.

Janssen, Heleen, and Jatinder Singh. 2022. "Data Intermediary." *Internet Policy Review* 11 (1). https://policyreview.info/glossary/data-intermediary.

Light, Ben, Jean Burgess, and Stefanie Duguay. 2018. "The Walkthrough Method: An Approach to the Study of Apps." *New Media & Society* 20 (3): 881–900. https://doi.org/10.1177/1461444816675438.

Mare Research. 2022. "Welke Factoren of Aspecten Belemmeren Om Gegevens Uit Overheidsbronnen Te Delen Met Derden?"

MarketResponse. 2021. "Digitaal Delen Persoonsgegevens van Burgers."

Micheli, Marina, Marisa Ponti, Max Craglia, and Anna Berti Suman. 2020. "Emerging Models of Data Governance in the Age of Datafication." *Big Data & Society* 7 (2): 2053951720948087. https://doi.org/10.1177/2053951720948087.

Milne, Richard, Annie Sorbie, and Mary Dixon-Woods. 2021. "What Can Data Trusts for Health Research Learn from Participatory Governance in Biobanks?" *Journal of Medical Ethics*, March. https://doi.org/10.1136/medethics-2020-107020

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2019. "Beleidsbrief Regie op Gegevens." Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.digitaleoverheid.nl/document/doc-beleidsbrief-regie-op-gegevens/

Nebbiai, Matteo. 2022. "Intermediaries Do Matter: Voluntary Standards and the Right to Data Portability." *Internet Policy Review* 11 (2).

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79 (1): 119.

Peeters, Rik, and Arjan Widlak. 2018. "The Digital Cage: Administrative Exclusion through Information Architecture – The Case of the Dutch Civil Registry's Master Data Management System." *Government Information Quarterly*, Agile Government and Adaptive Governance in the Public Sector, 35 (2): 175–83. https://doi.org/10.1016/j.giq.2018.02.003.

Solove, Daniel J. 2024. "Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data." SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.4322198

Vitak, J, Y Liao, A Mols, D Trottier, M Zimmer, PC Kumar, and J Pridmore. 2023. "When Do Data Collection and Use Become a Matter of Concern? A CrossCultural Comparison of US and Dutch Privacy Attitudes." *INTERNATIONAL JOURNAL OF COMMUNICATION* 17: 471–98.

Tschirsich, Martin, Patrick Jäger, and André Zilch. 2020. "Blackbox-Sicherheitsbetrachtung Corona-Datenspende-App Des RKI." Chaos Computer Club.

Veil, Winfried. 2021. "Data Altruism: How the EU Is Screwing up a Good Idea." AlgorithWatch. https://algorithmwatch.org/en/eu-and-data-donations/

Wieringa, Maranke. 2023. "'Hey SyRI, Tell Me about Algorithmic Accountability': Lessons from a Landmark Case." *Data & Policy* 5 (January): e2. https://doi.org/10.1017/dap.2022.39

Zoonen, Liesbet van. 2016. "Privacy Concerns in Smart Cities." *Government Information Quarterly*, Open and Smart Governments: Strategies, Tools, and Experiences, 33 (3): 472–80. https://doi.org/10.1016/j.giq.2016.06.004

Bijlage: Methodologie

Lijst van experts die we om advies hebben gevraagd:

- Bits of Freedom
- Democratic Society
- IPO (Interprovinciaal overleg)
- VNG (Vereniging van Nederlandse Gemeenten)
- Provincie Zuid-Holland
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Maatschappelijke Coalitie “Over Informatie Gesproken”
- Datactivist (France)
- MyData Global (Finland)

Gestructureerde Google zoek:
In het geval van appstores hebben we met de zoektermen “Rijksoverheid” en “overheid” gezocht naar apps die door de Nederlandse overheid zijn ontwikkeld. Voor Web of Science hebben we gekozen voor zoektermen in het Engels om hiermee artikelen te identificeren die over Nederland zijn gepubliceerd met betrekking tot onderwerpen die relevant zijn voor gegevensbescherming. Voor Google Search hebben we Nederlandse zoektermen gebruikt om webpagina’s te vinden die relevante initiatieven en instrumenten onthouden. We hebben de volgende zoektermen onderzocht:

Source type	Trefwoorden
Google Search (rekening houdend met de eerste 30 zoekresultaten))	“controle" AND “gegevens”; “bescherming” AND “gegevens; “controle” AND “data”; “regie houden” AND “gegevens”; “grip houden” AND “gegevens”; “grip op” AND “gegevens”; "delen” AND “gegevens"; [gegevens aanlever app]; Each of these terms was also paired with overheid (e.g. “controle" AND “gegevens” AND “overheid”) and “burger” (e.g. [“controle” AND “data” AND “burger”]
Web of Science (alle jaren, zoeken op auteurs, titel, abstract)	[Dutch AND data protection AND government]; [Dutch AND data AND citizen AND government]; [Dutch AND “personal data” AND “government”]; [Netherlands AND data protection AND government]; [Netherlands AND data AND citizen AND government]; [Netherlands AND “personal data” AND “government”];
App stores (zoeken naar app-naam, uitgever, app-beschrijving)	Rijksoverheid; Overheid; “controle" AND “gegevens”; “bescherming” AND “gegevens; “controle” AND “data”; “regie houden” AND “gegevens”; “grip houden” AND “gegevens”; “grip op” AND “gegevens”; "delen” AND “gegevens"; [gegevens aanlever app];