Panteia
Research to Progress

Research voor Beleid | EIM | NEA | IOO | Stratus | IPM

Burgers tussen wal en schip

Het voorkomen en oplossen van knelpunten bij de (digitale) overheid

Marieke Hollander; Henri Faun; Jos Jooren; Sophie Doove

Zoetermeer, 12 maart 2015

Inhoudsopgave

Samenvatting

In het regeerakkoord is afgesproken dat burgers en bedrijven in 2017 digitaal zaken kunnen doen met de overheid. Dienstverlening van overheidsinstanties wordt ook steeds meer digitaal door burgers afgenomen. Bij digitale dienstverlening worden burgers echter ook geconfronteerd met (persoons)gegevens die verkeerd in overheidssystemen kunnen staan. Panteia heeft onderzocht welke fouten, knelpunten en vormen van fraude bij de verwerking en registratie van gegevens voorkomen, wat de oorzaken zijn en hoe deze knelpunten beter voorkomen en opgelost kunnen worden.

Voor dit onderzoek zijn 23 expertinterviews gehouden met personen van uiteenlopende overheidsinstanties, is een online vragenlijst onder een aselecte steekproef van 1500 burgers afgenomen en zijn 15 burgers over hun ervaringen met knalpunten bij de (digitale) dienstverlening door de overheid geïnterviewd.

Verschillende soorten fouten

Voordat processen gedigitaliseerd werden en voordat bestanden werden gekoppeld en er een systeem van basisregistraties was, werden er ook al fouten gemaakt bij de gegevensinvoer en bewerking. Sterker nog: de digitalisering voorkomt juist een hoop fouten, doordat er minder menselijke handelingen nodig zijn (zo zijn er veel minder handgeschreven formulieren). Wanneer er echter een fout gegeven in basisregistraties terecht komt, kan dit veel grotere gevolgen hebben, doordat systemen direct met elkaar verbonden zijn.

Naast het onderscheid tussen de fouten die in het verleden ook al voorkwamen en de fouten die direct gerelateerd aan de digitalisering zijn, kan er ook een onderscheid gemaakt worden tussen informatiefouten (over de inhoud van de gegevens) en ICT-fouten (over de hardware en software waarmee de gegevens beheerd, uitgewisseld en bewerkt worden). Deze twee dimensies leveren het volgende raamwerk aan fouten in de gegevensinvoer en –verwerking op:

	Bestaande fouten	Door digitalisering
Informatiefouten	• Invoer door overheid • Invoer door burgers • Fraude	• Voorgeschreven invoervelden • Overnemen gegevens in andere bestanden • Fraude
ICT-fouten		• Fout in berichtenverkeer • Beheersbaarheid van applicaties • Interdependenties • Beveiliging en autorisatie • Fraude

➢ *Informatiefouten*

In Nederland worden gegevens over personen, bedrijven, gebouwen etc. verwerkt in het stelsel van basisregistraties. De gegevens die overheidsorganisaties hanteren, kunnen fout in de registraties komen doordat:

- burgers verkeerde gegevens invoeren, vergeten wijzigingen door te geven of vergeten bewijsstukken voor registraties aan te leveren;
- overheden fouten maken bij de gegevensinvoer (menselijke fouten) of verkeerde beslissingen maken bij de gegevensinvoer (zowel te snel als juist niet iemand als 'vertrokken onbekend waarheen' registreren);
- verschillende landen een andere wijze van registratie van gegevens hebben (structuren van voor- en achternamen kunnen anders zijn of gegevens ontbreken doordat bepaalde zaken in andere landen niet geregistreerd worden);
- gegevens verkeerd overgenomen worden uit (basis)registraties. Organisaties krijgen informatie binnen uit (basis)registraties, die zij vervolgens bewerken en/of verrijken met hun eigen gegevens. Hierbij kunnen er discrepanties optreden tussen de gegevens zoals ze door de afnemer gehanteerd worden en hoe ze in de basisregistraties staan. Ook kan er een andere interpretatie van gegevens gehanteerd worden (bijvoorbeeld wanneer een gemeente een gegeven als 'in onderzoek' markeert) of worden correcties niet correct of niet tijdig doorgevoerd.

➢ ICT-fouten

Van ICT-fouten is sprake als er inhoudelijk correcte informatie wordt verstuurd, maar er technisch iets misgaat. Te onderscheiden fouten hierbij zijn:

- Berichtenverkeer loopt niet goed: berichten worden wel goed verstuurd, maar komen niet goed aan.
- Applicaties zijn niet optimaal beheersbaar: door slecht geschreven software kan voor problemen zorgen.
- Een overvloed aan afhankelijkheden tussen systemen: veel gegevensinput en gegevensoutput kan tot verkeerde mutaties leiden.
- Beveiliging en/of autorisatie van systemen schiet tekort: wanneer websites niet goed beveiligd zijn kunnen gegevens lekken of kan er gehackt worden. Dit werkt fraude in de hand.

➢ *Bewuste fouten: fraude*

Fraude is het bewust fout registreren van gegevens: een informatiefout. Om de informatie te vervalsen kan gebruik gemaakt worden van bestaande ICT-fouten. Fraude begeeft zich daarom op het snijvlak van informatiefouten en ICT-fouten. De meest verregaande vorm van fraude is identiteitsdiefstal, waarbij misbruik wordt gemaakt van gestolen persoonsgegevens.

Fraude is geen nieuw fenomeen, maar de digitalisering biedt wel nieuwe mogelijkheden om fraude te plegen:

- Bij gebrek aan persoonlijk contact is het gemakkelijker voor kwaadwillenden om foutieve informatie in registratiesystemen te zetten.

- Het feit dat veel data online verstuurd en opgeslagen wordt, biedt in potentie meer mogelijkheden om gegevens te onderscheppen of te wijzigen.
- Slecht beveiligde persoonsgegevens (door organisaties of door de burgers zelf) kunnen gebruikt worden voor identiteitsdiefstal. persoonsgegevens kunnen zowel digitaal verkregen worden (bijvoorbeeld via phising) als in een offline context (uit poststukken).

Herstellen van fouten

Als er eenmaal foute informatie in gegevensbestanden terecht is gekomen, is het herstellen hiervan vaak lastig. Wanneer de foute informatie bij slechts één instelling of in één basisregistratie bekend is, is herstellen over het algemeen geen probleem. Moeilijker wordt het wanneer de foute informatie in een informatieketen terecht is gekomen en de onjuiste gegevens verspreid zijn. Het herstellen komt vaak op het bord van de burger terecht, waarbij deze veelal geen goed beeld heeft van de bron van de fout, hoe en waar de fout kan worden hersteld en welke (voor hem niet-zichtbare) kanten de foutieve informatie op is verspreid.

Een complicerende factor is dat niet alle gegevens met terugwerkende kracht hersteld kunnen worden. Zo kunnen de gevolgen van verkeerde registraties nog jaren doorwerken.

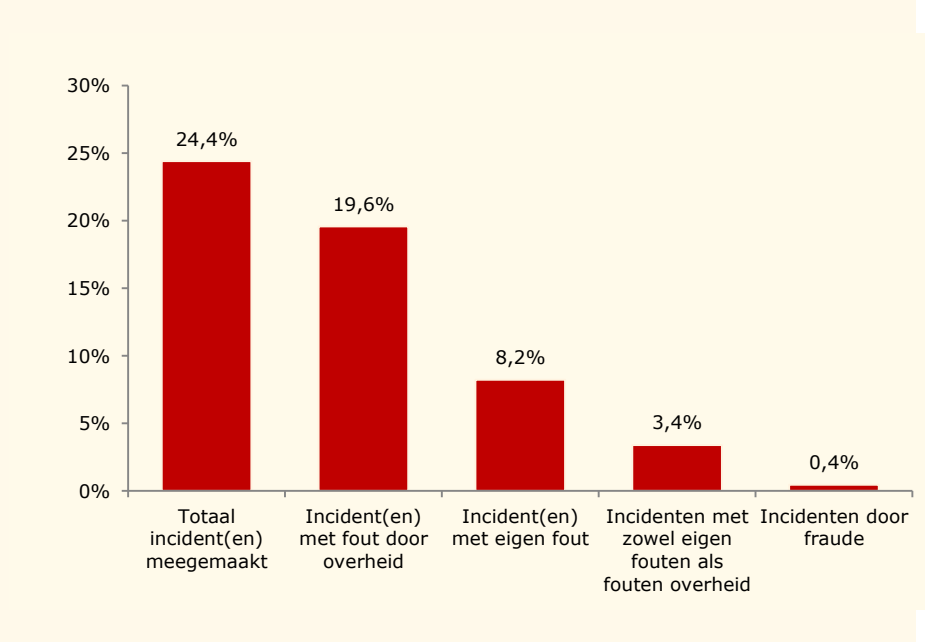
Ervaringen van burgers

Structurele fouten lijken vrijwel niet voor te komen. Structurele fouten vallen namelijk op en kunnen adequaat aangepakt worden. De fouten die voorkomen kunnen als incidenten worden bestempeld, zijn uiteenlopend van aard en worden ook vaak als individuele gevallen behandeld. Al met al komen fouten in relatieve zien weinig voor, de gevolgen voor een individu kunnen echter groot zijn.

Er is een duidelijk verschil tussen feiten en perceptie van fouten in de (digitale) dienstverlening door de overheid. Een burger doorziet niet alle processen die zich afspelen om tot bepaalde gegevens te komen. Vaak is hij in de veronderstelling dat de overheid meer weet dan in de praktijk het geval is, bijvoorbeeld op het gebied van inkomensveranderingen. Doordat de burger niet alle processen doorziet hoe de gegevens tot stand komen, interpreteert deze het als fouten van de overheid terwijl het voor de overheid juist een logisch gevolg is van de beschikbare input.

Figuur 1 geeft enkele uitkomsten uit de enquête onder burgers weer. Van de ondervraagde burgers geeft 24 procent aan de afgelopen twee jaar één of meer keer geconfronteerd te zijn met een foutieve registratie van gegevens bij de overheid. Twintig procent van de respondenten geeft aan gevallen meegemaakt te hebben waar (volgens hen) de fout bij de overheid lag. Acht procent van hen erkent dat het voorgekomen is dat er door hun eigen schuld een fout in de gegevens stond.

figuur 1 Ervaren verkeerde gegevensregistratie en oorzaken (n=1.557)



Bron: Panteia, 2015

Ook wordt uit de resultaten van de enquête duidelijk dat de materie voor burgers complex is en vaak onoverzichtelijk, zeker als het aankomt of verkeerd geregistreerde gegevens. Men heeft niet altijd een goed beeld van de oorzaak, de bron en de gevolgen van een fout. Sommige fouten die burgers noemen, worden niet als zodanig herkend door overheidsinstanties. Dat is bijvoorbeeld het geval wanneer mensen vergeten actie te ondernemen en gegevens niet gecorrigeerd worden, situaties die bijvoorbeeld in het geval van de Belastingdienst, het UWV of het SVB regelmatig voorkomen.

Het corrigeren verloopt procentueel gezien voor een groot deel van de burgers goed. Het kan echter ook een moeizaam proces zijn, juist in de gevallen dat de gevolgen groot zijn. Hierbij wordt dan vaak ontevredenheid geuit over de dienstverlening van een overheidsinstantie.

Handreikingen: De burger centraal en handelen als één overheid

Om de (digitale) dienstverlening te optimaliseren moet de overheid de burger centraal stellen en handelen als één overheid. Dit is een veelgehoord motto, maar vereist nog immer een cultuuromslag binnen de overheid. De burger ziet de overheid als een geheel en de overheid zou diezelfde burger ook meer op deze manier moeten benaderen in de dienstverlening. Dit betekent:

- Eén overheid die de burger helpt, ongeacht wat het eerste aanspreekpunt voor de burger is.
- Realiseren dat de overheid maar een klein deel van het dagelijkse leven van de burger is: zakendoen met de overheid is lastig als een burger niet alle achterliggende processen ziet.

- Concurrentie lokt betere dienstverlening uit. De overheid heeft geen concurrenten, maar kan wel de dienstverlening zodanig inrichten dat eenzelfde kwaliteit van dienstverlening wordt geboden als in een concurrerende omgeving.
- Transparantie in processen betekent meer begrip van de burger en meer grip van de burger op wat er met zijn gegevens gebeurt. Neem een voorbeeld aan track-and-trace systemen van webshops.

Bij het oplossen van fouten en knelpunten in de (digitale) dienstverlening dient een balans te worden gevonden, waarbij zowel het belang van de burger als de mogelijkheden die overheidsinstellingen hebben, worden afgewogen. Daarin vormen de uitgangspunten van de burger centraal en één overheid als basis bij de uitwerking.

Incidenten voorkomen

Incidenten bij de (digitale) dienstverlening door de overheid kunnen op de volgende manier voorkomen worden.

- *Bewustwording van burgers*

Burgers zijn nog weinig bekend met het bestaan en de werking van diverse basisregistraties. Zij zien niet altijd hoe ze zelf het systeem beïnvloeden door verkeerde gegevens door te geven of wijzigingen niet tijdig te communiceren. De burger is zich er ook vaak niet van bewust dat foutieve persoonsgegevens afkomstig zijn uit een centraal beheerde basisadministratie en dat zij zelf deze gegevens kunnen controleren en inzien. Meer bewustzijn creëren bij de burger over het bestaan en de werking van de basisadministraties, wat de voordelen zijn van een dergelijk systeem en waarom ze in het leven zijn geroepen, is belangrijke voor de algemene kennis van de burger. Hierbij is een belangrijke communicatietaak weggelegd voor de overheid. Als dit bewustzijn verhoogd is, kan gewerkt worden aan het informeren van burgers over meer praktische zaken als het inzien en corrigeren van persoonsgegevens.

- *Snellere doorlooptijd onderzoek van adressen of personen 'in onderzoek' bij de gemeente.*

Meerdere knelpunten zijn ontstaan doordat mensen te snel, of juist niet als 'vertrokken, onbekend waarheen' (VOW) geregistreerd komen te staan. Door risicopatronen in beeld te brengen en meer fysieke controles kunnen onderzoeken sneller afgerond worden en tot betere resultaten leiden. Daarbij moeten er altijd twee bronnen zijn: de input van de burger en een verificatie door bevoegde personen en/of op basis van documenten. Ook kan een gemeente meer actie ondernemen als er nog belangrijke bewijsstukken bij voorlopige registraties ontbreken.

- *Afspraken over status van data in bronbestanden*

Er kunnen betere afspraken gemaakt worden, meer eenduidigheid worden gecreëerd, over de waarde en betekenis van bepaalde data in bronbestanden, vooral wanneer een gemeente de data "in onderzoek" heeft

geplaatst. De Stelselcatalogus is nog weinig bekend en schrijft geen wijze van gebruik voor.

- *Synchroniseren van bestanden en bestanden die met gebruik van brongegevens zijn bewerkt.*

Bronbestanden en afgeleide, verrijkte bestanden zouden vaker gesynchroniseerd moeten worden. Door de huidige manier van werken met berichten, kunnen bestanden verschillende gegevens bevatten. Meer checks op deze gegevens kunnen (het verspreiden van) fouten voorkomen.

- *Kwaliteitscontroles op data*

Er kunnen meer kwaliteitscontroles voor data worden ingebouwd, waarbij de factor 'plausibiliteit' meegenomen wordt. Systemen verwerken informatie, die intuïtief zeer onwaarschijnlijk is, zonder hierbij vragen te stellen. Er zijn vrijwel geen controles in systemen ingebouwd die als het ware een alarmsignaal doen afgaan, als over een burger zeer onwaarschijnlijke gegevens worden geregistreerd (bijvoorbeeld 99 kinderen registreren of 1700 auto's op naam hebben staan).

- *Beheer informatie in handen van de burger*

Een verregaande vorm van 'de burger centraal stellen' zou zijn om het beheer van informatie in handen van de burger geven. Hier worden al stappen mee gezet, met het oprichten van 'datakluisjes' voor de burger.

Incidenten oplossen

Het oplossen van knelpunten kan verbeterd worden met de volgende maatregelen:

- *Nemen van verantwoordelijkheid door verschillende instanties, zoals het doorgeleiden van klachten naar de juiste persoon of instantie.*

Bij het oplossen van knelpunten waar verschillende overheidsorganisaties bij betrokken zijn, zou de overheidsinstelling waar een burger bij aanklopt nadrukkelijker verantwoordelijkheid kunnen nemen. Ook als er 'achter de schermen' meerdere afdelingen/organen/instanties betrokken zijn. De burger ziet zijn knelpunt als één zaak bij één grote overheid en wil dat zijn probleem/klacht ook als zodanig behandeld wordt.

Het is niet gezegd dat elke instelling elke burger bij de hand zou moeten nemen om samen zaken op te lossen. Maar er kan wel een stap verder worden gegaan dan aangeven dat 'dit de gegevens zijn die bekend zijn en dat daar verder weinig aan gedaan kan worden'.

Hieraan kan bijvoorbeeld invulling worden gegeven door geformaliseerde (informatie)paden bekend maken bij instellingen, die door medewerkers als een soort handleiding gebruikt kunnen worden om de burger op weg te helpen. Klopt een burger aan met een bepaalde informatiefout,

dan zou hem duidelijk moeten kunnen worden gemaakt waar de bron van deze fout is, op welke manier hij dit kan verifiëren en waar hij het eventueel kan herstellen en welke andere instellingen dezelfde informatie ook foutief overgenomen kunnen hebben.

- *Casemanager met overkoepelende blik*

Bij specifieke knelpunten is er behoefte aan een partij die een breder overzicht heeft en zowel de burger als een overheidsinstelling kan bijstaan. Oplossingen voor verkeerde gegevens in databestanden zijn namelijk niet altijd voor de hand liggend. Overheidsinstellingen overzien slechts een deel van de dataketen en zijn vaak beperkt in de wijzigingen die ze kunnen doorvoeren. Een casemanager voor de lastig te corrigeren gegevens, die los van de partijen staat, kan ondersteuning bieden aan zowel burgers als overheidsinstellingen. Idealiter wordt het casemanagement belegd bij een organisatie die nu ook al op het gebied van ondersteuning bij datafouten en/of fraude actief is.

- *Structureler omgaan met incidenten, zoals het beschrijven van problemen en de oplossingen en dit ter beschikking stellen aan anderen*

De knelpunten waar burgers mee te maken hebben zijn niet structureel, maar komen wel vaker voor. Doordat de knelpunten ook worden behandeld als incidenten (en dus elk geval als een uniek en uitzonderlijk geval) wordt er ook weinig gedaan met hetgeen dat door een individuele ambtenaar geleerd wordt van het oplossen van het probleem.

Een medewerker van een gemeente of andere instelling die te maken krijgt met een burger, die een bepaald knelpunt ervaart, kan dit knelpunt oplossen als er een flinke tijdinspanning wordt geleverd. Als vervolgens een vergelijkbaar incident zich bij een andere burger voordoet, zal een andere ambtenaar die dit voor hem tracht op te lossen een vergelijkbare tijdinspanning moeten leveren, omdat de oplossing hem niet bekend is en hij hier zelf naar op zoek moet.

In de praktijk zijn er verschillende manieren om vorm te geven aan het structureler omgaan met incidenten. Een laagdrempelige (niet kostbare en praktisch goed realiseerbare) manier om hier op in te spelen is een online verzamelpunt in de vorm van een forum of kennisbank, waar ambtenaren hun knelpunten en gevonden oplossingsmogelijkheden kunnen delen. Een categorisatie op basis van de basisregistratie waar het knelpunt mee te maken heeft, zou voor de gebruikers de vindbaarheid van oplossingen binnen deze verzamelbak.

Een alternatief van of een aanvulling op een forum of kennisbank is door een persoon aanspreekpunt te maken of als expert te benoemen inzake knelpunten met betrekking tot een bepaalde basisadministratie. Op dit moment is het namelijk zo dat een medewerker van bijvoorbeeld een gemeente, bij wie een burger met een probleem aanklopt, niet weet waar of bij wie hij terecht kan voor een oplossing.

De kennisbank en/of het aanspreekpunt kan ondergebracht worden bij dezelfde organisatie als de hiervoor beschreven casemanager. Zodoende is alle kennis en ondersteuning aan zowel burgers als de overheid zelf belegd bij één organisatie.

Fraude voorkomen en oplossen

Fraude en identiteitsdiefstal kan (deels) voorkomen worden door het goed beveiligen van persoonsgegevens en een goede controle van gegevens op plausibiliteit. Door gegevens (binnen de grenzen van de Wet bescherming persoonsgegevens) aan elkaar te koppelen, kunnen niet-plausibele gegevens herkend worden (bijvoorbeeld 12 kinderen in een tweekamerappartement).

Bij het oplossen van fraudegevallen komt er vaak veel kijken en moet de burger ondersteund worden. Deze taak is reeds belegd bij het Centraal Meldpunt Identiteitsfraude en –fouten. Deze instantie moet dan wel grotere bekendheid onder de bevolking krijgen.

1 Aanleiding en aanpak

1.1 Knelpunten in contact met de digitale overheid

In de jaren '90 van de vorige eeuw startte de overheid met digitale dienstverlening en communicatie via internet. Sindsdien heeft de 'e-overheid' veel en snelle ontwikkelingen doorgemaakt. In 1998 werd in het Actieprogramma Elektronische Overheid de komst aangekondigd van '*een site op Internet (www.overheid.nl) die het met behulp van een zoekmechanisme mogelijk maakt op een gebruiksvriendelijke manier snel overheidsinformatie op te zoeken*'. Inmiddels is communicatie met en informatieverstrekking door de overheid via internet steeds meer de norm geworden. Dat geldt zowel voor de Rijksoverheid (bijvoorbeeld via mijnoverheid.nl en belastingdienst.nl) als voor gemeenten.

De overheid streeft ernaar, uit het oogpunt van gemak voor de burger én kostenbesparing, dat het elektronische kanaal meer gebruikt wordt in de communicatie tussen overheid en burgers. Tegelijk worden er in diverse publicaties belemmeringen geconstateerd die dit in de weg kunnen staan. Zaken als gebruiksvriendelijkheid, betrouwbaarheid en veiligheid van overheidswebsites blijken niet altijd optimaal.

Zo rapporteerde de Nationale Ombudsman[1] in de afgelopen jaren klachten te hebben ontvangen van burgers die met de gevolgen van verkeerde gegevens in overheidssystemen geconfronteerd werden. Uit een enquête onder burgers bleek dat 17% van de respondenten wel eens heeft meegemaakt dat zijn gegevens verkeerd in een overheidssysteem stonden. Het probleem doet zich vooral voor indien meerdere instanties elkaars gegevens gebruiken ('ketenproblematiek'). Een voorbeeld is de registratie in de Basisregistratie Personen (BRP, voorheen bekend als de Gemeentelijke Basisregistratie, GBA) dat iemand is geëmigreerd terwijl dit niet het geval is, met het gevolg dat diverse toeslagen worden stopgezet.

Bij dit soort zaken blijkt het voor burgers zeer moeilijk de fout te herstellen. Zowel omdat onvoldoende transparant is wat en waar de bron van de fout is, als omdat met alle instanties afzonderlijk contact nodig is om de gegevens te herstellen. Ook was herstel vaak moeizaam omdat er bewijs werd gevraagd dat de burger niet kon leveren. Geopperd wordt dan ook dat inzage- en correctierecht van burgers bij overheidssystemen beter moet worden geregeld. Momenteel zijn er via mijnoverheid.nl mogelijkheden voor inzage- en correctierecht, echter deze zouden niet optimaal zijn. Daarbij zou de verantwoordelijkheid voor fouten en fraude te eenzijdig bij de burger worden gelegd, die niet altijd over de benodigde vaardigheden beschikt om assertief en adequaat voor het eigen belang op te komen.

Kortom: de digitalisering brengt veel voordelen voor zowel de burgers als de overheid, maar het kan ook voor knelpunten zorgen. Soms is er sprake van een dermate groot knelpunt, dat moeilijk op te lossen is, dat

[1] De burger gaat digitaal. De Nationale Ombudsman, 2013.

burgers 'tussen wal en schip' dreigen te vallen. Het is zaak om deze burgers middels goede dienstverlening weer in veilige haven te brengen.

1.2 Doelstelling, onderzoeksvragen en analysekader

Doelstelling

Zoals hiervoor beschreven is er sprake van een toenemende digitalisering van de overheidsdienstverlening, die ook als wenselijk wordt gezien vanuit het oogpunt van vermindering van (administratieve) lasten en kostenbeheersing, maar er mede toe kan leiden dat burgers in de knel komen. De gesignaleerde knelpunten in het eerder genoemde rapport ´De burger gaat digitaal´ van de Nationale Ombudsman, alsmede meldingen bij het Centraal Meldpunt Identiteitsfraude (CMI), dat mensen problemen hebben om hun digitale gegevens bij verschillende overheidsorganisaties gewijzigd te krijgen, zijn aanleiding voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) om onderzoek te laten uitvoeren.

De centrale doelstelling van het onderzoek is als volgt:
Inzichtelijk maken hoe kan worden voorkomen dat burgers vastlopen (door eigen fout, systeemfout of criminaliteit) in de digitale wereld van de overheidsdienstverlening, en hoe fouten kunnen worden hersteld.

Onderzoeksvragen

Het onderzoek richt zich op het beantwoorden van de volgende vragen:

Fouten en fraude

- Wat zijn veelgemaakt fouten van burgers bij het gebruik van digitale overheidsdiensten? Hoe vaak komen zij voor en bij welke websites/diensten?
- Welke knelpunten ondervindt men bij digitale transacties met de overheid?
- Welke fouten worden gemaakt door de overheden zelf, en in hoeverre gaat het dan om fouten in digitale systemen en/of om menselijke fouten?
- Welke vormen van fraude komen voor in het contact met de digitale overheid?

Oorzaken en herstelmogelijkheden

- Wat zijn de oorzaken/achtergronden van deze fouten/fraude, waar ontstaan ze in het systeem?
- Hoe kunnen deze fouten en deze vormen van fraude worden voorkomen in een digitaal dienstverleningsproces? Hierbij gaat specifieke aandacht uit naar ketenproblematiek.
- Hoe zouden (gevolgen van) fouten/fraude beter kunnen worden gesignaleerd?
- Hoe kunnen ze (bij voorkeur snel en eenmalig) worden hersteld?

Concrete oplossingen en input voor toekomstig beleid

- Wat zijn concrete, pragmatische, efficiënte en effectieve oplossingen om fouten zoveel mogelijk te voorkomen dan wel te kunnen herstellen?

- Wat zijn hierbij de taken en verantwoordelijkheden van de verschillende betrokken partijen (waaronder overheden en burgers)?
- Hoe kan bij het ontwerpen van nieuwe dienstverleningssystemen (bijvoorbeeld ontwerpregels) rekening worden gehouden met snel en eenmalig herstel van fouten in de keten?
- Hoe kan worden gezorgd dat mensen hun gegevens adequaat kunnen (laten) beheren (met het oog op de uitvoering van een nieuwe wet op de e-overheid)?
- Welke bouwstenen leveren deze bevindingen op voor een eventuele stelselwet Basisregistraties (waaronder mogelijke voorzieningen voor borging en verbetering van digitale dienstverlening, zoals bijvoorbeeld een "correctiepunt")?

1.3 Onderzoeksaanpak

Het onderzoek richtte zich op het in beeld brengen welke knelpunten (fouten, vormen van fraude) voorkomen in het contact tussen de burger en de digitale overheid, wat de aard, achtergrond en oorzaken van die fouten zijn, en welke oplossingen mogelijk zijn om deze te voorkomen dan wel te herstellen.

In overleg met de opdrachtgever is afgesproken dat de focus hierbij ligt op ***knelpunten bij de invoer van gegevens en gegevensverwerking***, waar burgers het slachtoffer van worden. Dat betekent dat we bijvoorbeeld knelpunten omtrent gebruiksvriendelijkheid van websites buiten beschouwing laten.

Het onderzoek bestond uit diepte-interviews met experts/betrokken partijen. Daarnaast is een enquête uitgevoerd onder 1.557 burgers, gevolgd door verdiepende interviews met 15 burgers over de precieze aard en oorzaak van het probleem. Hierna zijn oplossingen in kaart gebracht, door analyse van de verzamelde gegevens en aanvullende interviews met experts. In bijlage 1 staat een overzicht van de organisaties die in de eerste en de afsluitende fase geïnterviewd zijn.

1.4 Leeswijzer

Dit rapport bestaat uit vier hoofstukken. Naast de aanleiding en aanpak in het eerste hoofdstuk, wordt in hoofdstuk 2 feitelijk weergegeven welke knelpunten, fouten en vormen van fraude er uit de interviews naar voren zijn gekomen. Er wordt ingegaan op zowel het ontstaan als de correctie van fouten. Hoofdstuk 3 behandelt de ervaringen van burgers met fouten en het corrigeren van fouten. Hoofdstuk 4 tot slot gaat in op mogelijkheden voor het voorkomen en oplossen van fouten.

2 Potentiële knelpunten, fouten en fraude

2.1 Inleiding

Uit zowel de interviews met de betrokken actoren, de experts en de burgers, als uit de enquête onder burgers, blijken erop twee fronten knelpunten te zijn die burgers bij de (digitale) dienstverlening door de overheid kunnen ervaren. Enerzijds kunnen er fouten in geregistreerde gegevens ontstaan, waar burgers de dupe van worden. Anderzijds ervaren burgers ook knelpunten bij de correctie van foute gegevens.

In dit hoofdstuk komen beide knelpunten aan bod. Daarvoor worden de verschillende oorzaken voor foute registraties middels een theoretisch kader in beeld gebracht (paragraaf 2.2) en worden de typen fouten nader toegelicht (2.3 en 2.4). Daarbij is ook aandacht voor een bijzonder soort 'fout', namelijk bewuste fraude (2.5). Vervolgens komen de knelpunten bij het herstellen van fouten aan bod (2.6).

2.2 Kader: soorten fouten bij (digitale) dienstverlening

De fouten in de (digitale) dienstverlening kunnen op verschillende manieren ingedeeld worden. Er kan gekeken worden naar fouten die direct samenhangen met de digitalisering en er kan gekeken worden naar de directe oorzaak van een fout: informatiefouten (over de inhoud van de gegevens) versus ICT-fouten (over de technische kant van gegevensverwerking). In de onderstaande figuur 2 zijn deze dimensies weergegeven, inclusief de fouten die in de volgende paragrafen nader toegelicht worden.

figuur 2 Theoretisch kader van typen fouten

Bron: Panteia, 2015

2.2.1 Bestaande fouten en fouten door digitalisering

Digitale dienstverlening betekent: bestaande processen digitaliseren en nieuwe processen ontwikkelen.

De digitalisering van de overheidsdiensten is tweeledig. Allereerst worden er bestaande processen gedigitaliseerd. Formulieren die voorheen handmatig werden ingevuld, worden nu digitaal ingevuld en zaken waar men vroeger persoonlijk voor aan een balie moest komen, kunnen nu van huis uit met de computer geregeld worden. Daarnaast biedt de digitalisering mogelijkheden die er voorheen nog niet waren. Systemen worden meer met elkaar verbonden, waardoor de invoer van data nog maar eenmalig hoeft te gebeuren. Door het stelsel van basisregistraties kunnen verschillende overheidsorganisaties dezelfde gegevens uit één bron gebruiken.

Voorheen kwamen er ook fouten voor in de dienstverlening. Niet alles is te wijten aan de digitalisering.

Fouten of knelpunten in de digitale dienstverlening door de overheid kunnen zich ook op twee manieren voordoen: enerzijds zijn er fouten die voorheen ook al voorkwamen in de oude werkwijzen. Deze komen nu in een digitale context voor. Voorbeelden hiervan zijn spelfouten in bestanden en het te laat of niet doorgeven van wijzigingen. Anderzijds zijn er fouten die ontstaan zijn als direct gevolg van de digitalisering, bijvoorbeeld doordat gegevens verkeerd door systemen worden overgenomen.

Het verschil tussen fouten die wel of niet het directe gevolg van de digitalisering zijn, is niet altijd evident. Ze kunnen in theorie ook met elkaar samenhangen: als een gegeven verkeerd wordt doorgegeven (iets wat voorheen ook kon gebeuren, en dus geen direct gevolg van de digitalisering) kan dit verstrekkende gevolgen hebben door de samenhang van databestanden (wel een direct gevolg van de digitalisering). Een verkeerd gegeven zal zich namelijk sneller over verschillende databestanden van verschillende organisaties verspreiden.

Digitalisering zorgt in feite voor minder fouten…

Een groot deel van de fouten in databastanden is dus niet direct toe te schrijven aan de digitalisering. In het verleden kwamen deze naar verwachting zelfs vaker, toen er meer handmatig ingevoerd werd, of toen men nog per instantie apart gegevens moest doorgeven. Een deel van de ‘fouten’ die door burgers in gegevensbestanden gesignaleerd wordt, zijn ook inherent aan de wijze waarop de verschillende overheidsinstanties werken (bijvoorbeeld de belastingdienst die zich baseert op gegevens van een jaar eerder). Burgers ervaren dit soms als een fout, terwijl hier in werkelijkheid geen sprake van is.

…maar fouten hebben wel verstrekkende gevolgen

Doordat er veel minder handmatig wordt ingevoerd, er minder dubbel ingevoerd hoeft te worden en meer gebruik wordt gemaakt van gedeelde gegevens, is de kans op foute invoer kleiner. Het gevolg van de digitalisering en de koppeling van bestanden is wel dat áls er sprake is van verkeerde gegevens, dat deze in veel meer bestanden terecht kunnen komen en de effecten voor een burger groter zijn. Het corrigeren van een fout is dan niet altijd even gemakkelijk.

De digitalisering heeft ervoor gezorgd dat er minder menselijke controle op de invoer van gegevens is. Voorheen werden meer zaken persoonlijk afgehandeld. Wanneer er gegevens ogenschijnlijk niet klopten of verdacht leken, kon dit door ervaren ambtenaren gesignaleerd worden.

Deze controle ontbreekt vaak bij digitale invoer en verwerking. Zo kan het gebeuren dat foute of niet-plausibele gegevens in bestanden komen.

2.2.2 Informatiefouten en ICT-fouten

Een informatiefout is een inhoudelijk probleem met data.

Onder informatiefouten verstaan we het fenomeen dat bepaalde gegevens inhoudelijk niet correct zijn. Dit kan verschillende oorzaken hebben waar zowel de burger zelf als de overheid verantwoordelijk voor kunnen zijn. Het is daarbij belangrijk om een onderscheid te maken tussen de oorspronkelijke invoer en de verdere verspreiding naar afgeleide bestanden en verrijkte bestanden.

Informatiefouten komen door verkeerde invoer of overname van gegevens

In Nederland is er een stelsel van basisregistraties, dat de komende jaren nog verder wordt uitgebreid. Hierin zijn gegevens over (onder andere) personen, bedrijven, gebouwen en voertuigen vastgelegd. In deze bestanden worden gegevens zo veel mogelijk éénmalig vastgelegd. Door de verschillende basisregistraties aan elkaar te koppelen kunnen complete overzichten van een persoon of een bedrijf gegenereerd worden. Het systeem valt of staat bij de correcte invoer van gegevens en de correcte koppeling en het correct gebruik van de gegevens uit de basisregistraties.

Informatiefouten kunnen voortkomen uit:

- Fouten bij de invoer door de overheid
- Fouten bij de invoer door burgers
- Fouten door registratieverschillen tussen landen
- Fouten bij het overnemen van gegevens uit (basis)registraties

Deze vier worden in paragraaf 2.3 nader toegelicht

ICT-fouten zijn toe te schrijven aan hardware en software.

Bij ICT-fouten is de informatie die verstuurd wordt inhoudelijk correct, maar gaat er technisch iets mis. Dit kan aan software of hardware liggen. Het gaat dus niet zo zeer over menselijke fouten, maar de techniek waar iets niet in klopt. Daarin worden vier soorten fouten onderscheiden:

- Fout in berichtenverkeer
- Beheersbaarheid van applicaties
- Interdependenties
- Beveiliging en autorisatie

Deze vier worden in paragraaf 2.4 nader toegelicht.

2.3 Informatiefouten

2.3.1 Fouten bij invoer door overheid

De invoer van gegevens door de overheid is deels handwerk en dus foutgevoelig

Het invoeren en wijzigen van gegevens gebeurt voor een deel handmatig en is dus mensenwerk. Dit betekent dat er ook fouten gemaakt kunnen worden. Sommige fouten zijn relatief onschuldig en zorgen niet voor veel last (bijvoorbeeld een spelfout in een naam), andere fouten kunnen grotere gevolgen hebben (bijvoorbeeld de verkeerde persoon als 'overleden' markeren).

Een fenomeen dat zich vaker voordoet is dat burgers onterecht door de gemeente uitgeschreven worden uit de BRP. Wanneer een burger niet meer blijkt te wonen op het adres waar hij is ingeschreven, kan de ge-

meente hem uitschrijven onder vermelding van 'vertrokken, onbekend waarheen' (VOW). Hier gaan gemeenten verschillend mee om. Sommige gemeenten doen dit relatief vaak (bijvoorbeeld Rotterdam[2] en Amsterdam[3]), in andere gemeenten blijken er juist te vaak ten onrechte burgers ingeschreven te staan[4].

Zoals eerder aangegeven kwam dit type fout ook al in het verleden voor, toen er nog geen sprake van digitalisering was. Vanwege de digitalisering worden dit soort fouten tegenwoordig wel in de digitale (basis)bestanden geregistreerd.

2.3.2 *Fouten bij invoer door burgers*

Fouten door burgers komen veelal doordat ze nalaten een wijziging door te geven

Burgers hebben weinig mogelijkheden om direct zelf aanpassingen in bestanden te maken. Vaak loopt de invoer via overheidsinstanties die toezien op de juistheid en de kwaliteit van gegevensinvoer. Toch kan de fout ook bij burgers liggen. Veelal treden er fouten op doordat burgers *nalaten* iets door te geven.

Voorbeelden die vaker voorkomen zijn het vergeten door te geven van een verhuizing of een wijziging van inkomen. Het niet doorgeven van een verhuizing kan ertoe leiden dat nieuwe bewoners van de leeggekomen woning in fiscaal opzicht samenwonen met de vertrokken oudbewoner, met alle gevolgen voor belastingen, rioolheffingen, afvalstoffenheffingen en toeslagen van dien. Het niet doorgeven van wijzigingen in het inkomen kan ook gevolgen hebben voor belastingen, toeslagen en uitkeringen.

Zonder bewijsstukken is een registratie niet compleet

Naast het niet-doorgeven van wijzigingen, komt het ook voor dat een invoer of wijziging niet compleet is, doordat de burger de relevante (bewijs)stukken nog niet heeft overlegd. Dit komt met name voor bij immigranten en expats. Zij kunnen zichzelf wel al inschrijven bij de gemeente en kunnen daarbij ook opgeven dat ze getrouwd zijn en kinderen hebben. Maar als ze niet de relevante stukken, zoals trouwakte en geboorteaktes overleggen, is de inschrijving nog niet compleet, en heeft men bijvoorbeeld ook geen recht op kinderopvangtoeslag.

Overlijden in het buitenland

Een bijzonder geval waar de benodigde formele documenten soms ontbreken is wanneer een Nederlandse burger tijdens verblijf in het buitenland overlijdt. Niet alle landen geven de in Nederland noodzakelijke papieren uit bij overlijden. Hierdoor is het lastig om iemand in Nederland als overleden te registreren[5]. Dit is niet zo zeer een 'fout' van de burger te noemen, maar is vergelijkbaar met de categorie 'fouten door incompatibiliteit van systemen op de werkelijkheid' hieronder.

[2] Zie: Jaap van Hal, Mathilde van den Hoogen, Marieke Vreugdenhil-Tempelman & Anne Mieke Zwaneveld (2014) Opsporing verzocht! Een onderzoek naar de gang van zaken voor, tijdens en na een adresonderzoek en de uitschrijving uit de GBA.Rotterdam: Gemeentelijke Ombudsman Rotterdam
[3] Aldus de Gemeentelijke Ombudsman van Amsterdam in een interview.
[4] Zo bleek ook in enkele cases in de door Panteia uitgevoerde enquête.
[5] Deze casus is tweemaal tijdens afzonderlijke interviews met gemeenten gemeld. Eenmaal betrof het een sterfgeval in Ierland en een andere keer in Iran.

Burgers overzien de gevolgen van bepaalde handelingen niet

Ten slotte komt het ook voor dat burgers bewuste aanpassingen in hun registraties (laten) maken, zonder dat ze de consequenties overzien. Zo zijn er cases bekend waarbij personen zich laten uitschrijven bij de gemeente, om zo niet meer door schuldeisers gevonden te kunnen worden. Ze komen dan als 'vertrokken, onbekend waarheen' (VOW) geregistreerd te staan. Doordat ze zich uitschrijven hebben ze ook geen zorgverzekering meer en bouwen ze geen AOW op. Hier komen ze soms te laat achter. Overigens is er feitelijk sprake van fraude wanneer iemand zich ten onrechte laat uitschrijven bij de gemeente (zie paragraaf 2.5).

Evenals de verkeerde invoer door de overheid, kwamen fouten door de burger ook in het verleden voor, toen er nog geen sprake van digitalisering was. Vanwege de digitalisering worden dit soort fouten tegenwoordig wel in de digitale (basis)bestanden geregistreerd.

2.3.3 Fouten door registratieverschillen tussen landen

Persoonsgegevens van migranten passen niet altijd in de Nederlandse systemen

De opbouw van databestanden en de bijbehorende invoersystemen zijn ontwikkeld met Nederlanders en Nederlandse gebruiken en historische registratiesystemen voor ogen. In de praktijk werkt deze systematiek ook voor een grote meerderheid van de personen die geregistreerd worden.

Er blijkt echter ook een groep te zijn voor wie de Nederlandse registratiesystemen niet werkbaar zijn. Immigranten uit andere delen van de wereld kunnen namelijk niet uit de voeten met systemen waarin voor- en achternamen geregistreerd worden, of geboortedata met dag, maand en jaar. In sommige landen en culturen komt het namelijk voor dat mensen geen voornaam hebben of alleen een geboortejaar. Ook blijkt het dat bepaalde diakritische tekens niet gebruikt kunnen worden bij bepaalde digitale invulformulieren.

De Basisregistratie Personen (BRP) houdt op basis van het namenrecht wel rekening met afwijkende gebruiken. Dit geldt echter niet voor alle registratiesystemen die binnen de overheid gehanteerd worden. Ook zijn er cases bekend waar men wel correct ingeschreven kan worden, maar er op basis van de inschrijving persoonsverwisselingen kunnen plaatsvinden, zoals het voorbeeld hieronder illustreert.

Namen internationaal

Er kan verwarring ontstaan doordat namen in andere landen of culturen anders zijn opgebouwd. Een voorbeeld hiervan is het Chinese systeem met familienaam, generatienaam en persoonsnaam. Daarbij staat de persoonsnaam als laatste. Wanneer een Chinees zich zou inschrijven zonder zijn persoonsnaam (bijvoorbeeld omdat deze moeilijk uit te spreken is) en zijn tweelingbroer zou hetzelfde doen, zouden ze precies dezelfde naam en geboortedatum hebben, met het risico van persoonsverwisseling van dien[6].

[6] Dit voorbeeld werd door een van de respondenten van de interviews genoemd. In die casus woonde echter maar één van de tweelingbroers in Nederland en waren de risico's op persoonsverwiseling nog hypothetisch.

2.3.4 *Fouten bij het overnemen van gegevens uit (basis)registraties*

Een vierde vorm van informatiefouten komt voort uit het verkeerd, onvolledig of helemaal niet overnemen van gegevens of wijzigingen vanuit basisregistraties door de afnemers.

Basisregistraties zorgen ervoor dat de burger bepaalde gegevens maar eenmalig hoeft door te geven.

Het systeem van basisregistraties voorziet erin dat gegevens eenmalig verzameld worden en door meerdere instanties gebruikt kunnen worden. In de bestanden van de afnemende organisaties worden deze gegevens verrijkt met eigen gegevens (bij de Belastingdienst worden de persoonsgegevens bijvoorbeeld aangevuld met gegevens over het inkomen). Een wijziging hoeft door de burger slechts één keer doorgegeven te worden. Vanuit de BRP wordt er vervolgens een bericht gestuurd naar alle aangesloten instanties (zoals de Belastingdienst, SVB, UWV, et cetera). Dit maakt het gemakkelijker voor de burger (minder dubbel doen) en zorgt ervoor dat belangrijke wijzigingen sneller en met kleinere kans op fouten bij alle noodzakelijke instanties doorgevoerd worden.

Gegevens en wijzigingen uit de basisregistraties worden niet altijd goed verwerkt.

Het komt in de praktijk echter voor, dat wijzigingen wel in een bronbestand worden doorgevoerd, maar verkeerd of helemaal niet bij de afnemers geregistreerd worden. Dit wordt hieronder middels een voorbeeld toegelicht.

Adresgegevens bij de Belastingdienst
In het onderzoek kwam een aantal gevallen naar voren van verhuizingen die niet goed verwerkt werden door de Belastingdienst. Meerdere respondenten van interviews en in de enquête gaven aan op een verkeerd adres bij de Belastingdienst geregistreerd te staan (bijvoorbeeld op het adres van de ouders, ook wanneer men zelf nooit op dat adres gewoond heeft), terwijl ze in de BRP wel op hun eigen adres geregistreerd staan. Er gaat dan blijkbaar iets mis in de koppeling tussen de BRP en de Belastingdienst.

Bewerkte bestanden zijn komen soms niet meer overeen met de actuele data in de bronbestanden

Het risico op fouten in de bestanden van afnemers wordt groter wanneer zij werken met afgeleide of verrijkte bestanden. Doordat verschillende bestanden met elkaar gecombineerd worden, kunnen sommige correcte data overschreven worden met incorrecte of verouderde gegevens.

Voor de beheersbaarheid van de gegevens die dagelijks veranderen is het voor instanties vaak nuttig om met gegevens van een bepaalde peildatum te werken en dit bestand periodiek te actualiseren. Dit betekent echter dat er in de praktijk met een verouderd bestand gewerkt wordt. Dit is in veel gevallen niet erg, als actualiteit niet noodzakelijk is. Er moet echter wel zorg gedragen worden voor een correcte periodieke actualisatie van de bestanden.

Definitieverschillen kunnen tot foute interpretatie van data leiden.

Een andere vorm van inconsistentie tussen bronbestanden en afgeleide bestanden is het hanteren van een verschillende interpretatie van gegevens. Een voorbeeld dat meerdere gemeenten gaven was de status van het gegeven ‘in onderzoek’ (zie hieronder).

Bewoner op adres 'in onderzoek'
Wanneer een gemeente het signaal krijgt dat een bewoner vertrokken is, zonder dat hiervan door de bewoner melding is gemaakt, zet de gemeente de persoon op het adres 'in onderzoek'. Het is vervolgens de taak van de gemeente om uit te zoeken of die persoon er nog woont, en zo niet of deze getraceerd kan worden. Wanneer dit niet lukt, krijgt de vertrokken persoon de status VOW.
Tijdens het onderzoek wordt de status 'in onderzoek' echter niet door de Belastingdienst gebruikt. Wanneer er dus een nieuwe bewoner op het adres wordt ingeschreven, terwijl er nog een onderzoek loopt of de oude bewoner er nog woont, gaat de Belastingdienst ervan uit dat er sprake is van een gedeeld huishouden. Dit kan bijvoorbeeld gevolgen hebben voor toeslagen.

Het verwerken van correcties is essentieel voor de kwaliteit van een databestand

Hoewel er weinig concrete bewijzen zijn, vermoeden sommige gemeenten dat afwijkingen tussen bronbestanden en afgeleide bestanden kunnen ontstaan door het niet verwerken van correcties. Wanneer er een fout in een bronbestand gesignaleerd wordt, kan dit middels een correctiebericht aangepast worden. Wanneer dit correctiebericht niet herkend of gebruikt wordt, blijft de fout in de afgeleide bestanden staan, terwijl de fout wel al bij de bron gecorrigeerd is. In het verleden is het voorgekomen dat een correctie na een (foutief) overlijdensbericht niet door alle afnemers van gegevens goed verwerkt werd, of dat er sprake was van het afsluiten van dossiers na overlijden, waardoor de correctie niet verwerkt werd en het dossier afgesloten bleef[7].

2.4 ICT-fouten

Dit onderzoek is vooral vanuit het burgerperspectief opgezet. De hieronder genoemde ICT-fouten zijn technische aspecten in de backoffice van de overheid. Hoewel de burger wel geconfronteerd kan worden met de gevolgen van ICT-fouten, zijn de oorzaken vrijwel nooit zichtbaar voor het publiek. We onderscheiden vier soorten ICT-fouten.

Er zijn vier soorten ICT-fouten:
1. Het berichtenverkeer loopt niet goed
2. Applicaties zijn slecht geschreven
3. Te veel interdependenties
4. Beveiliging schiet tekort

2.4.1 Berichtenverkeer loopt niet goed

In de praktijk kan het voorkomen dat berichten worden met de correcte informatie vanuit het bronbestand worden verstuurd, maar met vertraging of helemaal niet aankomen. Het laatste komt zeer weinig voor, maar vertragingen zijn wel mogelijk (bijvoorbeeld bij een slechte verbinding). In sommige gevallen kan een te laat binnengekomen bericht leiden tot beslissingen op basis van achterhaalde gegevens.

Dit type ICT-fout kan de veroorzaker zijn van het feit dat gegevens uit bronbestanden niet goed in de afgeleide/verrijkte bestanden verwerkt worden (zoals hierboven reeds in paragraaf 2.3.4 genoemd).

2.4.2 Beheersbaarheid van applicaties

Sommige applicaties zijn instabiel en/of slecht geschreven. Updates van applicaties kunnen problemen verhelpen, maar lossen niet altijd alle kwetsbaarheden op. Geheel nieuwe versies van applicaties invoeren is

[7] Dit voorbeeld is genoemd in het rapport van de Algemene Rekenkamer (2014) Basisregistraties: vanuit het perspectief van de burger, fraudebestrijding en governance. Enkele geïnterviewde experts spraken hun zorgen uit dat dit soort cases nog steeds kunnen voorkomen.

niet altijd mogelijk, bijvoorbeeld vanwege de kosten die hiermee samenhangen.

2.4.3 Te veel interdependenties

De netwerken en applicaties voor gegevensverwerking zijn zeer complex. Er komt via meerdere kanalen data binnen, die vervolgens naar meerdere bestemmingen wordt doorgesluisd. Er kunnen soms spontane mutaties optreden, waarbij verkeerde data aan elkaar gekoppeld wordt of data muteert. Een respondent van de interviews vergeleek het als volgt: om het overzicht op een vliegveld te behouden is er één ingang (de douane) en gaat de stroom mensen naar meerdere uitgangen (de gates). Bij digitale applicaties is er soms sprake van een veelvoud aan ingangen en een veelvoud aan uitgangen. Dit biedt ruimte voor fouten.

2.4.4 Beveiliging en autorisatie schieten tekort

Veel websites en systemen vertrouwen op one-factor login, bijvoorbeeld gebruikersnaam, wachtwoord en verificatie via één kanaal, dat wil zeggen één computer of één mobiele telefoon. Dit is het geval bij DigiD laag. Bij DigiD midden, dient er verificatie plaats te vinden via een code die per sms gestuurd wordt. Dit is two-factor login en is aanmerkelijk veiliger. Slechte beveiliging geeft ruimte voor misbruik. Dit kan beveiliging door burgers zijn (wachtwoorden niet geheim houden) of door websites die DigiD niet in een veilige omgeving inbedden[8]. Hier wordt in de volgende paragraaf over fraude op ingegaan.

2.5 Bewuste fouten: fraude

Fraude is bedrog door het vervalsen van administratie van de eigen gegevens of die van een ander.

Fraude is volgens de definitie in Van Dale "bedrog, gepleegd door vervalsing van administratie". Het is dus in feite het bewust fout registreren van gegevens: een informatiefout. Om de informatie te vervalsen kan gebruik gemaakt worden van bestaande ICT-fouten (bijvoorbeeld ondeugdelijke beveiliging tegen hackers). Fraude begeeft zich daarom op het snijvlak van informatiefouten en ICT-fouten.

Meestal is het doel van fraude het behalen van (eigen) financieel gewin, maar het kan ook aangewend worden om iemand anders bewust te duperen. De gegevens die vervalst worden kunnen de eigen gegevens zijn, of die van een ander. De meest verregaande vorm van fraude is identiteitsdiefstal, waarbij misbruik wordt gemaakt van gestolen persoonsgegevens.

Door de digitalisering zijn er nieuwe mogelijkheden om fraude te plegen.

Fraude is geen nieuw fenomeen, maar de digitalisering biedt wel nieuwe mogelijkheden om fraude te plegen. Doordat interacties met de overheid vaker zonder persoonlijk contact gaan, zijn er minder mogelijkheden voor ambtenaren om onraad te vermoeden. Bij gebrek aan persoonlijk contact is het gemakkelijker voor kwaadwillenden om foutieve informatie in registratiesystemen te zetten. Ook het feit dat veel data online verstuurd en opgeslagen wordt, biedt in potentie meer mogelijkheden

[8] In het tv-programma Opgelicht werd gesignaleerd dat er gemeentelijke websites waren die gebruik maakten van DigiD voor identificatie en authenticatie van burgers. Howel het systeem van DigiD zelf wel veilig is, bleken de websites van de gemeenten niet aan de veiligheidseisen te voldoen, waardoor het gebruik van DigiD op die sites niet veilig was. Zie: http://www.opgelicht.nl/dossiers/detail/7727/8/

om gegevens te onderscheppen of te wijzigen. Grote bedrijven en overheden hebben hun beveiliging hiervoor meestal wel op orde, maar particulieren en kleine ondernemers blijven hierin vaak achter.

Identiteitsdiefstal kan een oorsprong in de offline of de online wereld hebben

Identiteitsdiefstal kan op meerdere wijzen tot stand komen. Wanneer de fraudeur bepaalde persoonskenmerken bemachtigt, is het mogelijk om een identiteit te vervalsen. Deze kenmerken kunnen gestolen worden via de fysieke wereld (inbraak, diefstal van bankpas of creditcard, stelen van post, etc.) of via de digitale wereld (hacken van computersystemen, phishing, etc.). Wanneer een identiteit via de digitale weg wordt gestolen, kan er sprake zijn van een ICT-fout, hetzij door de maker van een website, of door het beveiligingssysteem van de identificatie en authenticatie bij het inloggen. Ook kan de schuld bij een burger zelf liggen als deze onzorgvuldig met privé inloggegevens omgaat.

2.6 Herstellen van fouten

Recht van inzage en correctie volstaat niet altijd

Wanneer een fout in gegevensbestanden geconstateerd wordt, blijkt dat burgers knelpunten kunnen ervaren bij het (laten) corrigeren van de fout. Voor de basisregistraties hebben burgers het recht van inzage en correctie. Dit is bij wet geregeld en maakt het corrigeren van bijvoorbeeld gegevens in de BRP relatief eenvoudig. In veel gevallen blijkt dat één of twee telefoontjes genoeg zijn om foute gegevens te herstellen. Er zijn echter ook gevallen bekend waar correctie een stuk lastiger bleek te zijn.

De knelpunten doen zich vooral voor wanneer er fouten in afgeleide bestanden staan. Het systeem van basisregistraties is erop ingericht dat afnemers van gegevens uit de basisregistratie berichten krijgen van wijzigingen. In theorie kunnen er dus geen discrepanties tussen bronnen en afgeleide bestanden bestaan. In de praktijk blijkt dit echter toch voor te komen.

Discrepanties tussen bronbestanden en afgeleide bestanden hebben niet altijd een duidelijke oorzaak

Wanneer zich een situatie voordoet waarin gegevens in afgeleide bestanden afwijken van de bron, is dit voor zowel de burger als de betrokken overheidsinstanties lastig. De verschillende overheidsinstanties overzien namelijk maar een deel van de dataketen, en dragen ook voor slechts een deel hiervan verantwoordelijkheid. In de uitzonderingssituaties waarbij er discrepanties zijn, heeft zich ergens in de keten een incident voorgedaan. Bij gebrek aan een duidelijke oorzaak (de keten werkt immers vrijwel altijd naar behoren) verwijzen overheidsinstanties veelal naar elkaar voor een oplossing. Instanties zijn namelijk niet bij machte om gegevens elders in de keten aan te passen.

Burger heeft geen kennis van ketens, draagt wel bewijslast, en krijgt vaak weinig ondersteuning.

Bij het corrigeren van gegevens wordt de burger met het knelpunt geconfronteerd dat hij geen kennis heeft over waar het in de informatieketen fout is gegaan. Door het systeem van gekoppelde bestanden, kan een burger nauwelijks overzien waar gegevens eventueel fout geregistreerd staan. Als er op één plek met verkeerde gegevens gewerkt wordt, kan het zijn dat bij andere afnemers met dezelfde verkeerde gegevens gewerkt wordt. De bewijslast en het initiatief voor correctie liggen bij de burger, die dit niet altijd zelfstandig kan oplossen. Wanneer

het om verkeerde persoonsgegevens gaat, zijn er gemeenten die hun inwoners daar intensief in bijstaan. Dit gebeurt echter niet overal. Er bestaan wel instanties zoals het Centraal Meldpunt Identiteitsfraude en fouten (CMI). Ook kunnen burgers terecht bij de manifestpartijen, Kafkateams of ondersteuning krijgen van de Nederlandse Vereniging Voor Burgerzaken (NVVB). Deze instanties zijn echter niet bij iedereen bekend.

Identiteitsdiefstal moeilijk (volledig) te corrigeren

Zaken van identiteitsdiefstal zijn dermate complex dat een burger dit niet alleen kan oplossen. De complexiteit van gedeelde databronnen werkt in het geval van identiteitsdiefstal nog meer in het nadeel van het slachtoffer. Aangebrachte wijzigingen kunnen lastig ongedaan gemaakt worden en er is geen grip op waar de gegevens terechtgekomen zijn. Er is in Nederland een bekende casus van identiteitsfraude die veel landelijke media-aandacht gekregen heeft. Het betrof iemand wiens identiteit door een kennis was gebruikt voor criminele activiteiten. Hij heeft hier, zelfs na correctie van verschillende bestanden, nog jarenlang last van gehad.

Correctie met terugwerkende kracht niet altijd mogelijk

Een laatste knelpunt bij de correctie van gegevens, is dat correctie met terugwerkende kracht niet altijd mogelijk is. Beslissingen of maatregelen die genomen zijn op basis van verkeerde gegevens kunnen moeilijk met terugwerkende kracht ongedaan gemaakt worden. Hierdoor kan men bijvoorbeeld uitkeringen of toeslagen mislopen, ondanks dat men er wel recht op had.

3 Praktijk: ervaringen van burgers

3.1 Inleiding

In het vorige hoofdstuk is een breed scala aan (mogelijke) knelpunten aan bod gekomen, in dit hoofdstuk kijken we naar hoe deze knelpunten in de praktijk uitpakken. Daartoe is een enquête uitgezet onder ruim 1.500 Nederlanders[9], met de vraag of zij hebben meegemaakt dat er bij overheidsorganisaties verkeerde gegevens over hen bekend waren, zo ja welke, en hoe één en ander tot stand gekomen en (eventueel) opgelost is. Naast de enquête zijn er ook vijftien interviews gehouden met burgers over zaken die zij met de overheid hebben meegemaakt, waarbij er sprake was van gegevens die incorrect in bestanden stonden[10].

De resultaten van deze enquête en interviews worden besproken in paragraaf 3.4 en 3.5. Om de resultaten van de juiste context te voorzien lichten we allereerst toe in hoeverre er sprake is van structurele fouten of incidenten (paragraaf 3.2) en lichten we de feitelijke fouten in het licht van de perceptie van de burger toe (3.3).

3.2 Structurele fouten versus incidenten

Er is geen sprake van structurele fouten…

Kijkend naar de dagelijkse praktijk, lijken geen structurele fouten te zijn die uitsluitend aan de digitale dienstverlening van de overheid toegeschreven kunnen worden. Structurele fouten zouden namelijk snel gesignaleerd worden, doordat ze veelvuldig voor zouden komen. In de digitale dienstverlening geldt immers dat iets niet eenmalig gebeurt. Een proces wordt duizenden of zelfs miljoenen keren op eenzelfde wijze gedaan. Wanneer hier een structurele fout in zou sluipen kan deze vlug gesignaleerd en opgelost worden.

…maar wel van een breed scala aan incidenten…

Gezien de grote meerderheid van de online transacties en de digitale dienstverlening tussen overheid en burgers die naar behoren lopen, kunnen de gevallen waar wel iets misgaat worden gezien als incidenten. De incidenten kennen een grote variëteit in aard, oorzaken en gevolgen. Overigens zijn er wel degelijk overeenkomsten tussen de incidenten. In de praktijk blijkt echter dat per overheidsinstelling het aantal knelpunten in de digitale dienstverlening dermate beperkt en diffuus is, dat er over incidenten gesproken kan worden.

… die voor burgers zeer hinderlijk kunnen zijn.

Het feit dat het om incidenten gaat, wil niet zeggen dat er geen probleem is. Wanneer er in een zeer beperkt aandeel van transacties een fout voorkomt heeft dit landelijk alsnog voor veel mensen gevolgen. Als er bijvoorbeeld bij één op de tienduizend huishoudens iets fout zou gaan, heeft dit in Nederland betrekking op 760 huishoudens. Fouten in de digitale dienstverlening kunnen daarbij verstrekkende gevolgen hebben voor degenen die het betreft.

[9] Deze groep is representatief voor de Nederlandse bevolking tussen 16 en 65 jaar.
[10] Een aantal van deze cases zijn in dit hoofdstuk als voorbeeld opgenomen. Daarbij zijn de respondenten geanonimiseerd en voorzien van een fictieve naam.

3.3 Feiten versus perceptie

De burger percipieert 'fouten' vaak anders dan de overheid.

Bij de interpretatie van de ervaren fouten van burgers is het van belang om een onderscheid te maken tussen feiten en perceptie. In de perceptie van de burger maakt de overheid vaker 'fouten' dan in de praktijk (en zeker vanuit overheidsperspectief) het geval is. Bepaalde overheidsprocessen zijn voor burgers vaak moeilijk te doorzien of te begrijpen. Wanneer er iets in de dienstverlening gebeurt of een gegeven wordt gehanteerd wat de burger niet begrijpt, kan hij dit als een fout zien. In veel gevallen is het echter een regulier onderdeel van de door de overheid gehanteerde processen.

De wijze waarop verschillende overheidsinstanties naar bruto inkomsten kijken, kan bijvoorbeeld verwarrend zijn. Ook gaan burgers er soms van uit dat de overheid over meer gegevens beschikt dan in werkelijkheid het geval is. Hierdoor zien zij bepaalde geregistreerde gegevens als 'fout', maar zijn het in de praktijk de best mogelijke gegevens die bij de overheid bekend zijn.

De analyse van de uitkomsten uit de enquête is op de eerste plaats een weergave van de perceptie van de burgers. Het gaat om ervaren knelpunten, ook als dit vanuit overheidsperspectief geen fout of knelpunt is. Daarom spreken we in dit hoofdstuk over de *ervaren* fouten.

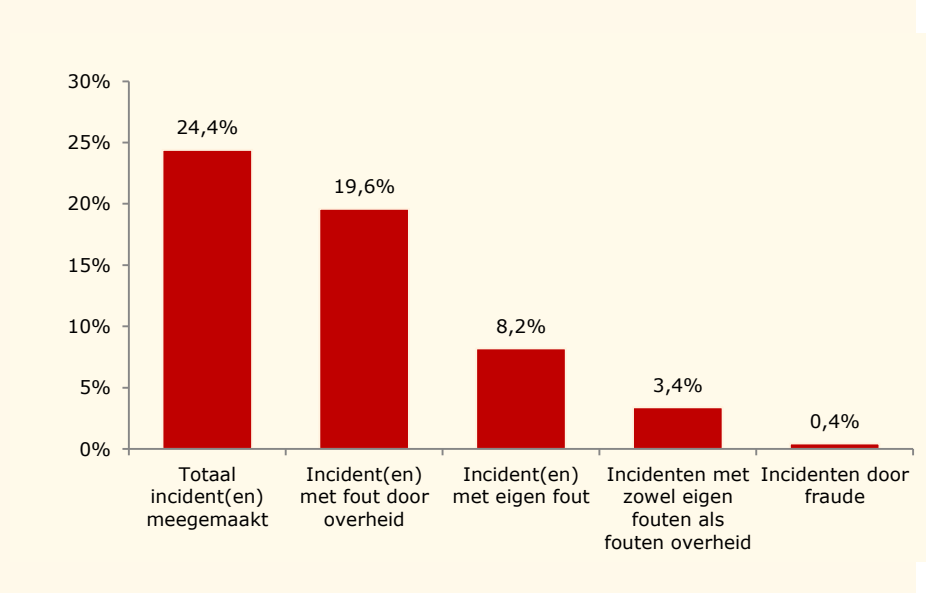
3.4 Ervaren fouten

Circa 24 procent van de burgers heeft één of meer fouten in de gegevensregistratie gesignaleerd

Van de ondervraagde burgers geeft 24 procent aan de afgelopen twee jaar één of meer keer geconfronteerd te zijn met een foutieve registratie van gegevens bij de overheid (zie figuur 3). Twintig procentpunt hiervan geeft aan gevallen meegemaakt te hebben waar (volgens hen) de fout bij de overheid lag. Acht procentpunt van hen erkent dat het voorgekomen is dat er door hun eigen schuld een fout in de gegevens stond. In minder dan één procent van de gevallen was er sprake van (vermeende) fraude.

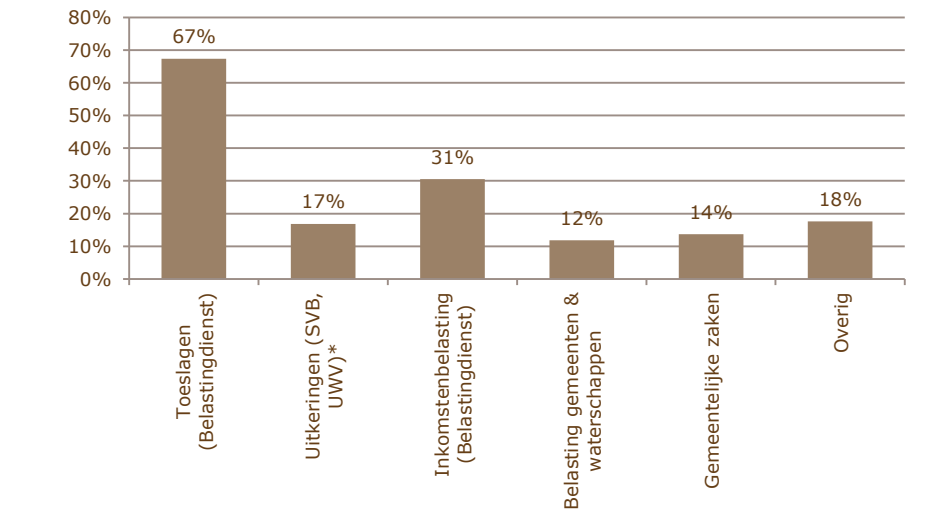
Burgers kunnen bij verschillende overheidsdiensten geconfronteerd worden met verkeerde gegevens. Vaak komen ze achter de fout als ze met een onverwachte beslissing geconfronteerd worden of merken dat er iets niet goed loopt in de dienstverlening. Van de respondenten die zich geconfronteerd zagen met verkeerde gegevens is in de onderstaande figuur 4 weergegeven bij welke overheidsdiensten dit was. Daarbij is een onderscheid gemaakt tussen de verschillende overheidsdiensten: toeslagen, uitkeringen, inkomstenbelasting, gemeentelijke belasting en waterschapsheffingen, gemeentelijke zaken (doorgeven verhuizing. aanvraag identiteitsbewijs, aanvraag vergunning) en overige zaken (bekeuringen, subsidieaanvragen, boetes, incasso's). De percentages tellen niet tot honderd op, omdat respondenten knelpunten bij meerdere diensten kunnen hebben meegemaakt.

figuur 3 Ervaren verkeerde gegevensregistratie en oorzaken (n=1.557)



Bron: Panteia, 2015

figuur 4 Overheidsdiensten waar burgers geconfronteerd werden met verkeerde gegevens (n=380)



** mogelijk sprake van dubbeltellingen met toeslagen.*

Bron: Panteia, 2015

Hieronder wordt per overheidsdienst toegelicht wat veelvoorkomende knelpunten waren. Elk van de knelpunten wordt geïllustreerd met een voorbeeld uit de interviews met burgers.

3.4.1 Belastingdienst (toeslagen en inkomstenbelasting)

Burgers kunnen het 'geschatte inkomen' als een foute registratie ervaren

Het 'knelpunt' waar men bij de belastingdienst het meeste tegenaan liep, was dat er beslissingen genomen waren (stopzetten toeslag, terugvorderen toeslag, meer belasting betalen dan verwacht) als gevolg van een verkeerd geschat inkomen en/of gegevens over de partner. Dit heeft niet zo zeer met echte fouten te maken, maar meer met de werkwijze van Belastingdienst: (voorlopige) toekenningen van toeslagen en voorlopige aanslagen gaan uit van inkomensgegevens en de huishoudsituatie van eerdere jaren. In veel gevallen was het knelpunt dat het inkomen in een opvolgend jaar hoger of lager was, waardoor men later toeslagen moest terugbetalen of in eerste instantie misliep.

Ondanks dat het tijdig doorgeven van wijzigingen in het inkomen een verantwoordelijkheid is van de burger, geeft circa driekwart van de respondenten aan dat de fout bij de Belastingdienst lag. De redenatie is veelal dat "de Belastingdienst toch wel moet weten wat mijn inkomen is." Hier is de vraag wie de fout heeft gemaakt dus vooral een kwestie van perceptie.

Naast inkomen ook adresgegevens en bankrekeningnummer vaker incorrect bij de Belastingdienst

Naast de foutieve inkomensgegevens, gaf een aantal respondenten aan problemen te ondervinden met foutieve adresgegevens of het bankrekeningnummer bij de Belastingdienst.

Verhuizing verkeerd geregistreerd
12 jaar geleden zijn de ouders van de heer Martins verhuisd. Hij is gelijktijdig uit zijn ouderlijk huis gegaan en heeft bij de gemeente zijn nieuwe adres doorgegeven. Bij de belastingdienst staat hij sindsdien echter op het (nieuwe) adres van zijn ouders geregistreerd, terwijl hij daar zelf nooit gewoond heeft. Hij kwam hier achter doordat post van de belastingdienst bij zijn ouders bezorgd werd. Bij de gemeente en alle andere instanties van de overheid kloppen zijn gegevens wel. Ook na meerdere telefoontjes en brieven aan de Belastingdienst is zijn adres nog steeds niet gewijzigd.

3.4.2 UWV & SVB (uitkeringen)[11]

Arbeidsverleden en/of inkomen meest voorkomend fout geregistreerd gegeven bij uitkeringen.

Gepercipieerde fouten bij uitkeringen hangen veelal samen met onjuiste gegevens over het inkomen of het arbeidsverleden. Dit heeft gevolgen voor het recht op de uitkering en/of de hoogte en duur van de uitkering. Evenals bij de Belastingdienst gaf circa een kwart van de respondenten aan dat zij zelf verantwoordelijk waren voor de foutieve gegevens. De overige driekwart zag het als een fout van de overheid of hun (voormalig) werkgever. Zij zouden een verkeerd inkomen of arbeidsverleden geregistreerd of doorgegeven hebben.

[11] Een deel van de respondenten kende ogenschijnlijk niet het verschil tussen een toeslag en een uitkering. Uit een aantal van de antwoorden blijkt namelijk dat men de uitkering associeert met de Belastingdienst. Waarschijnlijk gaat het in die gevallen om een toeslag, al kan dit niet met zekerheid gezegd worden. Er is dus mogelijk sprake van dat een deel van de knelpunten bij uitkeringen feitelijk bij de toeslagen gerekend kan worden. Ook is het mogelijk dat respondenten hierbij zowel knelpunten rond toeslagen als knelpunten rond belastingen hebben geselecteerd. In dat geval is er sprake van een dubbeltelling.

Te veel uitkering is te veel huurtoeslag

Mevrouw De Jong heeft een ziektewetuitkering ontvangen van het UWV. Aan het einde van het jaar bleek uit een brief van het UWV dat zij een uitkering voor een fulltimer had ontvangen, terwijl zij slechts recht had op dat van een parttimer. Ze moest toen 800 euro terug betalen aan het UWV. Nergens in de papieren is echter terug te vinden voor welk percentage ze een ziektewetuitkering ontving, hierdoor had zij zelf gedurende het jaar geen weet van de fout.

Van de belastingdienst ontving mevrouw daarnaast ook huurtoeslag omdat ze op basis van het loon dat zij voorheen verdiende daar al die jaren recht op had gehad. Doordat ze 800 euro te veel had ontvangen van het UWV had ze echter te veel inkomsten gehad en moest ze de gehele huurtoeslag terug betalen (4.000 euro). Dat ze deze 800 euro alsnog terug moest betalen, maakte voor de belastingdienst niets uit omdat de terugbetaling pas een jaar later ter sprake was gekomen en dus niet verrekend kon worden met de inkomsten van het jaar waarin ze de uitkering had ontvangen.

Mevrouw De Jong moest dus zowel de uitkering als de huurtoeslag terugbetalen, terwijl ze achteraf alsnog weer recht op de huurtoeslag zou krijgen.

3.4.3 Gemeentelijke belasting en waterschapsheffing

Burgers ervaren de door de gemeente gehanteerde WOZ-waarde als een 'fout'

Met betrekking tot de gemeentelijke belasting en de waterschapsheffing ervaren mensen de gehanteerde WOZ-waarde van het huis vaak als een verkeerd geregistreerd gegeven. Men vond het bedrag dat de gemeente hanteerde meestal te hoog. Dit is meestal niet zo zeer een fout geregistreerd gegeven, maar eerder toe te schrijven aan het feit dat burgers het niet eens zijn met de systematiek op basis waarvan de waarde bepaald wordt. Er is hier dus veelal geen sprake van een verkeerd geregistreerd gegeven mar van de perceptie van fouten. Bovendien is dit fenomeen van alle tijden en dus ook niet aan de digitalisering toe te schrijven. De meerderheid van de respondenten schreef deze 'fout' in de registratie toe aan de gemeente. Ook zagen enkele respondenten een verhoging van de jaarlijkse belasting als een 'fout' van de gemeente.

Daarnaast waren er ook enkele incidenten waarbij er echt sprake was van fout geregistreerde gegevens, zoals huishoudenssamenstelling of het feit dat een hond reeds overleden was (in verband met hondenbelasting).

Kwijtschelding gemeentebelasting

In 2014 hadden mevrouw Jansen en haar vriend een aanslag van de gemeente ontvangen voor gemeentelijke heffingen. Omdat haar vriend voor het grootste deel in de WAO zit en zijzelf flexwerker is, hebben zij niet veel inkomsten. Daarom hebben zij hiervoor kwijtschelding aangevraagd. Omdat mevrouw flexwerker is werkt ze de ene maand meer dagen dan de andere maand en wisselen haar maandelijkse inkomsten erg. Voor de kwijtschelding moest ze een loonstrook mee sturen. Op haar laatste loonstrook stond ongeveer 200 euro, deze heeft ze mee gestuurd. Op basis hiervan heeft de

gemeente het inkomen van mevrouw op 600 euro per maand geschat, veel meer dan het bedrag dat ze de afgelopen maand verdiend had.

Op basis van deze berekening van de gemeente is besloten dat de kwijtschelding niet toegekend werd. De gemeente kon geen bevredigend antwoord geven op hoe de berekening tot stand kwam. Dit was nou eenmaal hoe het berekend werd en kwijtschelding was niet mogelijk. Achteraf bleek de inschatting van 600 euro per maand inderdaad te hoog en is de reeds betaalde belasting alsnog terugbetaald en kwijtgescholden.

3.4.4 Gemeentelijke zaken en overige knelpunten

Breed scala aan incidenten met gemeenten. Vorige bewoner niet uitgeschreven komt meermaals voor.

De zaken die (in de ogen van de burger) bij de gemeente fout gingen zijn zeer diffuus. Het kwam een aantal keer voor dat een vorige bewoner zich niet op het adres had uitgeschreven. Verder is er geen duidelijke lijn in de fouten te vinden. Vanwege de kleine aantallen zijn er geen significante uitkomsten te vinden. Het betreft dus vooral incidenten die niet altijd met de digitalisering samenhangen. Hetzelfde geldt voor de overige zaken, die verschillende knelpunten adresseerden.

3.5 Ervaringen met oplossingen en correcties

Burger schrijft fout meestal toe aan de overheid (77 procent).

In de meeste gevallen (ongeveer 77 procent) schrijven de burgers de fout in de gegevens toe aan de overheid. Dit is deels correct en deels niet. Er zijn inderdaad verschillende incidenten waar er buiten de schuld van de burger om zaken bij de overheid verkeerd lopen. Vaak gaat echter niet om een echte fout, maar een voorlopig gegeven, dat zonder veel moeite aangepast kan (of had kunnen) worden. Dit is bijvoorbeeld het geval bij geschat inkomen of de WOZ-waarde.

Gegevens vaak naar tevredenheid gecorrigeerd…

Met het corrigeren van gegevens lopen de ervaringen uiteen. Van de respondenten die geconfronteerd zijn met verkeerde gegevens, geeft 89 procent aan dat de gegevens reeds gecorrigeerd zijn, of dat dit op korte termijn zal gebeuren. De meerderheid (79 procent) van de respondenten is tevreden over hoe een situatie (uiteindelijk) is opgelost. Ook uit de interviews blijkt dat in veel gevallen de verkeerde gegevens relatief eenvoudig hersteld konden worden.

…maar niet altijd.

In 8 procent van de gevallen verwacht de respondent echter dat de gegevens helemaal niet meer gecorrigeerd zullen worden. Redenen hiervoor lopen uiteen, zoals afgewezen bezwaarschriften (vooral bij WOZ-gegevens) of het feit dat gegevens niet met terugwerkende kracht kunnen worden aangepast. Voor de meeste respondenten van wie de gegevens niet veranderd konden worden, is het echter niet duidelijk waarom dit niet kon. In totaal is in 21 procent van de zaken waarbij verkeerde gegevens stonden geregistreerd, de respondent niet tevreden over de afhandeling. Dit aandeel is groter dan de genoemde acht procent, bijvoorbeeld omdat de zaak nog loopt of omdat ze het niet eens zijn met een uiteindelijke beslissing rond de toekenning van toeslagen of uitkeringen.

Corrigeren gegevens kan een moeizaam proces zijn.

Uit de interviews blijkt dat het corrigeren van gegevens soms een moeizaam proces kan zijn. Het meest stoort men zich aan slechte service vanuit de overheidsinstelling. Men moet vaker hetzelfde verhaal vertellen aan verschillende contactpersonen binnen een organisatie. Ook komt het voor dat een wijziging meermaals doorgegeven wordt, maar alsnog niet doorgevoerd wordt. In die gevallen is het voor zowel de burger als de instantie vaak een raadsel waarom de wijziging niet lukt.

Hoewel dit in slechts een kleine minderheid van de gevallen is, gaat het om aanzienlijke absolute aantallen.

Procentueel gezien is er een beperkt aantal cases waarin er verkeerde gegevens over een burger geregistreerd komen te staan en waarbij de correctie zeer moeizaam is. Binnen de steekproef van de enquête gaat het om minder dan 2 procent van alle respondenten voor wie er geen oplossing gevonden lijkt te worden. Daarbij zijn de knelpunten uiteenlopend van aard en slechts ten dele aan de digitalisering toe te schrijven.

Kleine percentages zijn op schaal van een grote populatie alsnog aanzienlijke aantallen. Zonder de gegevens uit de enquête één-op-één naar de Nederlandse bevolking door te willen vertalen, kan wel geconcludeerd worden dat er potentieel honderden of duizenden mensen zijn bij wie zich flinke knelpunten voordoen, inclusief eventuele verstrekkende gevolgen.

4 Voorkomen en oplossen

4.1 Inleiding

Gezien de grote hoeveelheid digitale transacties met de overheid en het kleine percentage fouten in de digitale dienstverlening dat tot moeilijk oplosbare knelpunten leidt, kan gesproken worden van incidenten. Vanwege hun uiteenlopende aard, valt te verwachten dat er zich altijd incidenten zullen blijven voordoen. Er kan altijd wel iets mis gaan en niets is voor honderd procent uit te sluiten.

In absolute termen kan een klein percentage alsnog om een aanzienlijk aantal gaan. Naast de fouten in gegevensinvoer en –bewerking zijn er ook gevallen van identiteitsfraude. Hiervan verwacht een aantal experts dat deze in aantallen zullen toenemen. Daarom is het van belang dat er twee zaken aangepakt worden:

1. incidenten moeten zo veel mogelijk voorkomen worden en
2. wanneer zich een incident voordoet moet er adequaat op gereageerd worden, zodat het zo goed mogelijk afgehandeld wordt.

In dit hoofdstuk staan we daarom stil bij de vragen hoe fouten bij informatiefouten en ICT-fouten voorkomen kunnen worden (paragraaf 4.2) en hoe ze beter opgelost kunnen worden (paragraaf 4.3). Ten slotte is er ook aandacht voor fraude en identiteitsdiefstal (paragraaf 4.4).

Voorkomen en oplossen door de burger centraal te stellen en te handelen als één overheid. Dit betekent: als één overheid op de juiste manier positioneren met optimale dienstverlening.

Cultuuromslag: de burger centraal en handelen als één overheid

Bij het voorkomen en oplossen van knelpunten met betrekking tot de digitale dienstverlening door de overheid, is het belangrijk om de gebruiker (de burger) centraal te stellen. Dit is een vaak gehoorde uitdrukking als het gaat om overheidsdienstverlening. Het werd in 2011 reeds als een van de uitgangspunten genoemd in de overheidsbrede implementatieagenda voor dienstverlening en e-overheid (i-NUP). Het is echter zaak om dit motto ook nader in te vullen. Daartoe hebben wij de volgende uitgangspunten geformuleerd die als basis voor de handreikingen in dit hoofdstuk dienen:

- ***De burger ziet de overheid als één geheel*** en doorziet niet hoe de structuur van verschillende overheidsorganen en –instanties met elkaar samenhangt. Dit zou ook niet nodig moeten zijn. Het is de strategie van de overheid om ook als geheel richting de burger te communiceren, maar in de praktijk komt hier vaak nog te weinig van terecht. De burger centraal stellen betekent ook meer uitgaan vanuit de beleving van de burger en meer acteren als één geheel.
- ***Voor de meeste burgers vormt de overheid maar een zeer beperkt deel van het dagelijks leven***. Voor veel mensen strekt het niet verder dan eenmaal per jaar belastingaangifte doen, eenmaal per tien jaar een paspoort en rijbewijs vernieuwen en een paar belangrijke levensgebeurtenissen zoals verhuizingen, geboortes en overlijden doorgeven. De overheid moet daarom haar plaats weten in het leven van de burger en hier rekening mee houden bij alle dienstverlening. Dit betekent dat de overheid er begrip voor moet hebben

dat burgers de werkwijze van de overheid niet kent. Ook betekent het dat de overheid zich zou moeten positioneren als één van de vele (digitale) instanties waar de burger contact mee heeft en zich niet moet positioneren als een uitzonderlijke instantie waar de burger een bijzondere binding mee heeft.

- ***De burger heeft geen keuze bij wie hij overheidsdiensten afneemt***. Overstappen naar een andere aanbieder is onmogelijk. Dit vraagt om goede service om frustratie te voorkomen en vooral om bewuste aandacht voor het centraal stellen van de burger. Doordat de burger geen keuze heeft wordt het vaak als gegeven gezien dat de burger bij een bepaalde organisatie aanklopt om diensten af te nemen. Hierdoor is de organisatie vaak intern gefocust, met vooral aandacht voor processen. Een goede dienstverlening vereist zodoende extra aandacht.
- ***Bij de klantgerichtheid van de digitale overheidsdienstverlening is transparantie van belang***. De burger heeft reeds het recht van inzage en correctie van de eigen gegevens. Ook is het mogelijk om op te vragen welke instanties gegevens vanuit de basisregistraties gebruiken. De overheid kan hierin nog een stap verder gaan, door bijvoorbeeld te leren van webshops die voor alle transacties een vorm van 'track & trace' hanteren. Zodoende blijft de consument op de hoogte wat de status van zijn bestelling is en wanneer hij een bepaalde uitkomst kan verwachten. Elke transactie met de overheid zou op eenzelfde manier vormgegeven kunnen worden, via mijnoverheid.nl of een toekomstige datakluis. Wanneer een actief op de hoogte wordt gehouden van wat er met zijn gegevens, zijn aanvragen en zijn klachten gebeurt, biedt dit meer houvast voor zowel het voorkomen als het oplossen van knelpunten.

4.2 Fouten voorkomen

Vijf handreikingen om fouten te voorkomen.

In hoofdstuk 2 zijn diverse informatiefouten omschreven, waarbij grote lijnen duidelijk zijn geworden wat betreft mogelijkheden om deze te voorkomen. Hieronder worden acties omschreven, waarmee informatiefouten voorkomen kunnen worden. Deze zijn gebaseerd op interviews met experts en gaan met name in op de informatiefouten. ICT-fouten zijn technische fouten, die ook om technische oplossingen vragen. In dit onderzoek ging het vooral om hoe de burger fouten ervaart, daarbij is de technische kant (die de burger niet ziet) buiten beschouwing gelaten. De ICT-fouten zouden in een apart traject nader onderzocht en opgelost kunnen worden.

➢ *Bewustwording van burgers en herinneringen*

Betere kennis bij burgers over procedures en gevolgen van handelingen voorkomt fouten.

Om fouten bij gegevensinvoer door burgers te voorkomen is het van belang om de burger beter te informeren hoe fouten voorkomen kunnen worden. Burgers zijn nog weinig bekend met het bestaan en de werking van diverse basisregistraties. Illustratief hierbij is bijvoorbeeld het feit dat vrijwel elke geïnterviewde medewerkers van een gemeente tijdens het interview aangaf dat burgers zelden tot nooit gebruik maken van hun inzagerecht. Op dit vlak valt nog veel winst te boeken. De burger is zich er vaak niet van bewust dat foutieve persoonsgegevens afkomstig zijn uit een centraal beheerde basisadministratie en dat zij zelf deze

gegevens kunnen controleren en inzien. Hierdoor ontstaat onbegrip en is het voor de burger onduidelijk hoe en waar zij zelf een fout kunnen voorkomen of oplossen.

Meer bewustzijn creëren bij de burger over het bestaan en de werking van de basisadministraties, wat de voordelen zijn van een dergelijk systeem en waarom ze in het leven zijn geroepen is belangrijke algemene kennis die burgers veelal niet hebben. Deze kennis is een eerste voorwaarde om burgers vervolgens te informeren over meer praktische zaken als welke gegevens waar vandaan afkomstig zijn, hoe en waar men deze gegevens kan inzien en desgewenst ook kan aanpassen. Bij het informeren van de burgers en het creëren van bewustzijn is een belangrijke communicatietaak weggelegd voor de overheid.

Wanneer wijzigingen/toevoegingen in onderzoek zijn omdat burgers de bijbehorende documenten nog niet hebben ingediend, zou er actiever achteraangegaan moeten worden. Burgers zijn wellicht vergeten dat ze nog iets moeten inleveren en zijn gebaat bij een herinnering hieraan. Daarbij kan ook beter op de consequenties van het niet inleveren van bewijsstukken gewezen worden. Dit kan veel problemen voorkomen.

- *Beheer informatie in handen van de burger*

Gegevensbeheer door burgers voorkomt fouten of klachten achteraf.

Een verregaande vorm van 'de burger centraal stellen' zou zijn om het beheer van informatie in handen van de burger geven. Hier worden al stappen mee gezet, met het oprichten van 'datakluisjes' voor de burger. De burger beheert dan zelf zijn gegevens (onder toezicht van de overheid) en kan zien welke instantie wanneer welke gegevens waarvoor gebruikt. Zodoende kan de burger actief voorkomen dat er met verkeerde gegevens wordt gewerkt. In Tilburg heeft men dit principe al toegepast op de WOZ-waarde. Bewoners mochten deze controleren en eventueel aanpassen. Dit voorkomt dat men het achteraf niet eens is met de gehanteerde WOZ-waarde.

- *Snellere doorlooptijd van adressen of personen 'in onderzoek' bij de gemeente.*

Kortere doorlooptijd onderzoeken leidt tot kortere doorlooptijd van onduidelijke gegevens.

Meerdere knelpunten zijn ontstaan doordat mensen te snel, of juist niet als 'vertrokken, onbekend waarheen' (VOW) geregistreerd komen te staan. Dit hangt samen met het gesignaleerde probleem van 'foute invoer door overheid'. Door risicopatronen in beeld te brengen en meer fysieke controles uit te voeren, kunnen onderzoeken sneller afgerond worden en tot betere resultaten leiden. Daarbij moeten er altijd twee bronnen zijn: de input van de burger en een verificatie door bevoegde personen en/of op basis van documenten.

- *Afspraken over status van data in bronbestanden*

Afspraken over data en definities voorkomt misverstanden.

Er kunnen betere afspraken gemaakt worden over de waarde en betekenis van bepaalde data in bronbestanden, vooral wanneer een gemeente de data "in onderzoek" heeft geplaatst. Om te voorkomen dat gegevens vanuit bronbestanden onjuist overgenomen of onjuist geïnterpreteerd worden, zouden gegevens door alle instanties op eenzelfde wijze gebruikt moeten kunnen worden. Daarvoor is onderlinge bekendheid met

elkaars definities en gebruiken nodig. Hiervoor is overigens reeds de Stelselcatalogus met begripsduidingen opgesteld. Deze is bereikbaar via www.e-overheid.nl. De Stelselcatalogus geniet echter nog (te) weinig bekendheid en schrijft geen wijze van gebruik voor.

- *Synchroniseren van bestanden en bestanden die met gebruik van brongegevens zijn bewerkt.*

Door gegevens periodiek te synchroniseren worden afwijkingen in afgeleide bestanden sneller gevonden.

Afgeleide of verrijkte bestanden zouden vaker gesynchroniseerd moeten worden met de bronbestanden. Nu wordt er vooral met berichten gewerkt. Maar het kan uiteindelijk voorkomen dat bestanden niet meer synchroon lopen. Daarvoor moeten synchronisatiechecks ingevoerd worden: kloppen de gegevens zoals ze bij de afnemer bekend zijn nog met de gegevens zoals ze in de bronbestanden geregistreerd staan? En zo niet, waarom niet? Hierbij is het ook van belang om logbestanden bij te houden van wijzigingen die zijn doorgevoerd. Zo kan achteraf altijd gecontroleerd worden waar iets is fout gegaan en kan vanaf dat punt bezien worden wat er nog meer fout gegaan kan zijn.

- *Kwaliteitscontroles op data*

Plausibiliteitschecks voorkomen verdachte, foute en fraudeleuze gegevens in bestanden.

Om de invoer van data door burgers en overheid kwalitatief beter te maken, en ook om fraude te voorkomen, kunnen er meer kwaliteitscontroles voor data worden ingebouwd. Daarbij zou de factor ‘plausibiliteit’ nadrukkelijk meegenomen moeten worden. Systemen maken het soms eenvoudig om te frauderen. Formulieren bieden door de invulvelden soms te ruime mogelijkheden. Het zou bijvoorbeeld niet mogelijk moeten zijn om 99 kinderen te laten registreren of 1700 auto’s op je naam te hebben staan (dit is in het verleden daadwerkelijk gebeurd). Er zou in ieder geval een ‘alarmbelletje’ af moeten gaan. Dit kan bijvoorbeeld ook getoetst worden door meer koppelingen. Als persoonsgegevens bijvoorbeeld aan woonlocatie gekoppeld worden, is snel te zien dat een gezin met zes kinderen in een tweekamerappartement niet plausibel is.

4.3 Fouten oplossen

Vier handreikingen om fouten (beter) op te lossen.

Zoals aan het begin van hoofdstuk 2 al werd gesteld zijn de fouten, waar dit onderzoek over gaat, geen structurele fouten maar is er sprake van incidenten. Deze incidenten zullen echter wel altijd voor blijven komen. Naast het proberen te voorkomen van deze incidenten, is het daarom ook zaak om het oplossen van incidenten te verbeteren. Gedurende het onderzoek is er een beeld ontstaan van hoe de burger beter bediend kan worden bij het oplossen van knelpunten. Deze oplossingen sluiten aan op het eerder geformuleerde uitgangspunten van de burger centraal zetten en handelen als één overheid.

- *Nemen van verantwoordelijkheid door verschillende instanties, zoals het doorgeleiden van klachten naar de juiste persoon of instantie.*

Bij het oplossen van knelpunten waar verschillende overheidsorganisaties bij betrokken zijn, zou het overheidsorgaan waar een burger in eerste instantie bij aanklopt met een melding van verkeerde gegevens na-

drukkelijker verantwoordelijkheid kunnen nemen. Ook als er 'achter de schermen' meerdere afdelingen/organen/instanties betrokken zijn. De burger ziet het als één zaak bij één grote overheid en wil dat zijn probleem/klacht ook als zodanig behandeld wordt. Het handelen als één dienstverlenende overheid moet duidelijker zijn en de verantwoordelijkheid op te treden namens die ene overheid moet meer genomen worden door de individuele overheidsorganisaties.

Burgers kunnen beter geholpen worden door eerst intern te controleren of alle gegevens kloppen en pas dan door te verwijzen naar de juiste schakel in de keten.

Het nemen van verantwoordelijkheid start met de voorbereiding op burgers die met een probleem aankloppen. Men dient zich te realiseren dat er (ogenschijnlijk) onverklaarbare fouten kunnen optreden, maar ook dat het formuleren en aankaarten van het probleem voor de burger een lastige zaak kan zijn. Dit betekent dat voordat een burger naar een andere overheidsinstelling doorverwezen wordt, er eerst geverifieerd moet worden waar de gegevens vandaan komen en of er inderdaad met de juiste gegevens gewerkt wordt en van daaruit naar de juiste organisatie door te verwijzen.

Het is niet gezegd dat elke instelling elke burger bij de hand zou moeten nemen om samen zaken op te lossen. Maar er kan wel een stap verder worden gegaan dan aangeven dat 'dit de gegevens zijn die bekend zijn en dat daar verder weinig aan gedaan kan worden'. In de praktijk betekent dit dat als een burger bij het UWV meldt dat een adres niet klopt, dat hij dan niet direct naar de gemeente verwezen wordt, maar dat er eerst gecontroleerd wordt in de BRP of het UWV wel met de juiste gegevens werkt. Is dit niet het geval, dan zal het UWV actie moeten ondernemen. Pas als met zekerheid blijkt dat het UWV wel dezelfde gegevens hanteert als die in het BRP staan, wordt de burger doorverwezen naar de gemeente om daar de gegevens te wijzigen.

De burger centraal zetten betekent in dit geval dus ook dat er meer geformaliseerde (informatie)paden bekend moeten zijn bij instanties, die door medewerkers als een soort handleiding gebruikt kunnen worden om de burger op weg te helpen. Klopt een burger aan met een bepaalde informatiefout, dan zou hem duidelijk moeten kunnen worden gemaakt waar de bron van deze fout is, op welke manier hij dit kan verifiëren en waar hij het eventueel kan herstellen en welke andere instellingen dezelfde informatie ook foutief overgenomen kunnen hebben. Voor veel burgers is het te complex om deze zaken zelf uit te zoeken en hier proactief en op adequate wijze achteraan te gaan.

Het op het juiste pad brengen van een burger, letterlijk de burger centraal zetten, kan op deze manier handen en voeten worden gegeven. Voorheen werd informatie per organisatie als afgebakend geheel beheerd. Door de opzet van basisregistraties stroomt persoonsinformatie steeds vrijer door overheidsinstanties heen. Ook richting de burger kan op deze manier begonnen worden met het verlagen van de schotten tussen de organisaties.

- *Casemanager met overkoepelende blik*

Bij specifieke knelpunten is er behoefte aan een partij die een breder overzicht heeft en zowel de burger als een overheidsinstelling kan bijstaan. Oplossingen voor verkeerde gegevens in databestanden zijn namelijk niet altijd voor de hand liggend. Overheidsinstellingen overzien

slechts een deel van de dataketen en zijn vaak beperkt in de wijzigingen die ze kunnen doorvoeren.

Bij omvangrijke knelpunten is casemanagement nodig om de burger te assisteren om data te corrigeren.

Een casemanager voor de lastig te corrigeren gegevens zou idealiter binnen een van de huidige organisaties geregeld kunnen worden. Hieraan zou dan ook meer bekendheid gegeven moeten worden, zodat de burgers ondersteuning gemakkelijker kunnen vinden. Instanties die signaleren dat een burger dreigt vast te lopen bij de (digitale) dienstverlening door verkeerd geregistreerde gegevens, zouden de burger naar een instantie kunnen doorverwijzen die het casemanagement op zich neemt.

De casemanager zou los van de partijen moeten staan, maar wel deel uitmaken van de overheid. Het is namelijk van belang dat de burger eerst hulp vindt binnen de overheid, voordat er een externe toezichthouder zoals de Ombudsman bij betrokken wordt.

Naast ondersteuning aan burgers kan een casemanager ook ondersteuning bieden aan overheidsinstellingen zelf. De ervaring die de casemanager opdoet kan gedocumenteerd worden. Toekomstige soortgelijke gevallen kunnen daardoor sneller opgelost worden. De casemanager kan op basis van zijn ervaringen gemakkelijker concrete en specifieke instructies geven aan instellingen die een wijziging moeten doorvoeren.

- *Lerende organisatie: structureler omgaan met incidenten, zoals het beschrijven van problemen en de oplossingen en dit ter beschikking stellen aan anderen*

Deels overlappend met het vorige punt is het structureler omgaan met incidenten. De knelpunten waar burgers mee te maken hebben zijn niet structureel, maar komen wel vaker voor. Doordat de knelpunten ook worden behandeld als incidenten (wat wil zeggen dat elk geval als een uniek en uitzonderlijk geval) wordt er ook weinig gedaan met hetgeen dat door een individuele ambtenaar geleerd wordt van het oplossen van het probleem.

In hoofdstuk 2 werden enkele voorbeelden gegeven van incidenten, die weliswaar niet structureel, maar wel meermaals voorkomen. De beschreven knelpunten 'overlijden in het buitenland' en 'namen internationaal' zijn voorbeelden van incidenten, die geregeld terugkeren. Een medewerker van een gemeente of andere instelling die te maken krijgt met een burger, die deze knelpunten ervaart, kan dit knelpunt oplossen als er een flinke tijdinspanning wordt geleverd. Als vervolgens een vergelijkbaar incident zich bij een andere burger voordoet, zal de ambtenaar die dit voor hem tracht op te lossen een vergelijkbare tijdinspanning moeten leveren, omdat de oplossing hem niet bekend is en hij hier zelf naar op zoek moet.

Het belang van structureler omgaan met incidenten is meerzijdig. Enerzijds kan de burger beter en klantvriendelijker behandeld worden, anderzijds valt er veel aan efficiency te winnen voor overheidsinstellingen als er structureler omgegaan wordt met incidenten. Manieren om de kennis, die wordt opgedaan bij het oplossen van een knelpunt, te formaliseren en structureren, kan het oplossen van volgende incidenten vergemakkelijken.

In de praktijk zijn er verschillende manieren om vorm te geven aan het structureler omgaan met incidenten. Een laagdrempelige (niet kostbare en praktisch goed realiseerbare) manier om hier op in te spelen is een online verzamelpunt in de vorm van een forum of kennisbank, waar ambtenaren hun knelpunten en gevonden oplossingsmogelijkheden kunnen delen. Een categorisatie op basis van de basisregistratie waar het knelpunt mee te maken heeft, zou voor de gebruikers de vindbaarheid van oplossingen binnen deze verzamelbak.

Door de wijze van oplossen van ingewikkelde knelpunten te documenteren, of door een organisatie aan te wijzen om bij knelpunten te adviseren, kunnen overheidsorganisaties van elkaar leren.

Het is mogelijk dat een dergelijk forum of kennisbank reeds online voor handen in. In dat geval is dat op dit moment weinig tot niet voldoende bekend bij de personen die te maken hebben met burgers, die knelpunten ervaren. Een forum of kennisbank speciaal opgezet voor dit doel is aan te raden. Dit zorgt voor herkenbaarheid en maakt communicatieinspanningen om de bekendheid te verhogen eenvoudiger en effectiever.

Een alternatief van of een aanvulling op een forum of kennisbank is een persoon of organisatie het aanspreekpunt maken of als expert benoemen inzake knelpunten met betrekking tot een bepaalde basisadministratie. Deze persoon dient exact op de hoogte te zijn van de werking van de basisadministraties. Op dit moment is het zo dat een medewerker van bijvoorbeeld een gemeente, bij wie een burger met een probleem aanklopt, op basis van zijn eigen netwerk of op basis van eerdere ervaringen contact gaat zoeken met andere instellingen om een oplossing te vinden. Dit is arbeidsintensief en levert vaker niet dan wel het gewenste resultaat op. Ook in dit proces kan meer structuur worden aangebracht door duidelijk te maken aan medewerkers van overheidsinstanties en gemeenten bij welke persoon zij in eerste instantie kunnen aankloppen, in het geval zij met incidenten te maken hebben en op zoek zijn naar een oplossing.

De rol van consulent en beheerder van lessen uit de praktijk zou ondergebracht kunnen worden bij dezelfde organisatie die het casemanagement voor de burger doet bij lastige fouten in databestanden. Zodoende wordt de kennis en expertise voor het oplossen van alle soorten fouten in de digitale dienstverlening door de overheid bij één organisatie belegd. Deze kan beter kennis vergaren en zowel burgers als ambtenaren bij knelpunten assisteren.

4.4 Fraude en identiteitsdiefstal

Fraude voorkomen door plausibiliteitstoetsen op data, veilig en verantwoord gebruik.

Een van de grootste uitdagingen voor de digitale overheidsdienstverlening is het bestrijden van fraude en identiteitsdiefstal. Phishing en hackers kunnen op grote schaal grote schade veroorzaken. Online bestaan namelijk geen kleine getallen: als er online gegevens gestolen worden, dan is dit meestal niet van één of enkele personen, maar kan het vele duizenden of zelfs miljoenen personen betreffen.

Voor fraude en identiteitsdiefstal hebben we enkele handreikingen geformuleerd met betrekking tot het voorkomen en het oplossen van incidenten.

Voorkomen

Fraude op basis van (bewuste) informatiefouten kan voorkomen worden door in te zetten op strengere controles en plausibiliteitstoetsen van gegevens, zoals deze al in paragraaf 4.2 aan bod kwamen.

Er ligt vooral nog een vraagstuk in hoeverre de overheid verantwoordelijk is voor hackers of andere kwaadwillende aanvallen die inbreuk maken op privacy en identiteiten kunnen stelen. De overheid biedt de mogelijkheid om zaken online te regelen en stimuleert de burger om liefst zo veel mogelijk digitaal af te handelen. Dit vraagt nogal wat van de burger, maar daarmee ook van de overheid.

De overheid heeft een zorgplicht. Systemen moeten beveiligd zijn tegen alle vormen van inbreuk. Deze eis geldt ook wanneer de burger zichzelf niet 100 procent beschermt. De overheid biedt immers de dienst en mag niet van een burger verwachten dat deze op technisch gebied van alles op de hoogte is. De overheid moet dus een stap verder gaan in de beveiliging en ook de burger tegen zichzelf in bescherming nemen.

Tegelijk kan de overheid ook eisen stellen aan de middelen die een burger gebruikt: eisen aan besturingssystemen, antivirussoftware, firewalls en browsers. Dit is vergelijkbaar met het wegverkeer: de overheid is verantwoordelijk voor deugdelijke en veilig ingerichte wegen, de burger mag deze betreden als zijn auto door de APK is gekomen.

De vraag waar de eigen verantwoordelijkheid van de burger eindigt en waar die van de overheid begint is geen gemakkelijke om te beantwoorden. De burger is in dezen geen consument die kan overstappen naar een andere aanbieder als hem de voorwaarden niet aanstaan. Het lijkt dan ook opportuun om van de overheid een stapje meer te verwachten dan van bijvoorbeeld banken in de verantwoordelijkheid voor beveiliging van digitale dienstverlening.

Oplossen

In geval van identiteitsdiefstal is casemanagement noodzakelijk.

Als er aantoonbaar identiteitsdiefstal heeft plaatsgevonden is er een casemanager nodig die alle ingangen kent en invloed heeft bij partijen om sommige zaken voor elkaar te krijgen c.q. ongedaan te maken. In Nederland is daarvoor het Centraal Meldpunt Identiteitsfouten en –fraude (CMI) opgericht. Hieraan moet meer bekendheid gegeven worden. Het is van belang dat er een link is tussen het CMI en de casemanager van een organisatie voor het oplossen van knelpunten, zoals beschreven in paragraaf 4.3. Dit kan door het casemanagement ook bij het CMI te beleggen of door een intensieve samenwerking.

Bijlagen

Bijlage 1 Geïnterviewde organisaties

Organisatie	Datum
Agentschap BPR (BZK)	28 januari 2015
Belastingdienst	27 november 2014
CMI	20 november 2014
Digicommissaris	2 februari 2015
DUO	9 december 2014
Gemeente Enschede	17 december 2014
Gemeente Maassluis	2 december 2014
Gemeente Oss	8 december 2014
Gemeente Roermond	17 december 2014
Gemeente Rotterdam	26 november 2014
ICTU	24 november 2014
ICTU[12]	9 februari 2015
KING	3 december 2014
Logius	3 december 2014
Nationale ombudsman	28 november 2014
NVVB/Gem. Molenwaard	20 januari 2015
Ombudsman Amsterdam	5 december 2014
Seniorweb	24 november 2014
SVB	8 december 2014
Taskforce BID	28 november 2014
UWV	12 december 2014
VDP	19 december 2014
Werkorganisatie Duivenvoorde (gemeenten Voorschoten & Wassenaar)	8 december 2014

[12] Met ICTU zijn twee interviews gedaan: een interview in de voorbereidende fase en een in de afsluitende fase, om de uitkomsten uit het onderzoek te klankborden.