Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 301

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 december 2013

Op 10 april 2013 had ik overleg met de vaste commissie voor Binnenlandse Zaken over de toekomstbestendigheid van de identiteitsinfrastructuur. De deelnemers aan dat overleg deelden het besef dat identiteitsfraude een serieus en groeiend probleem is. Er was steun voor de gepresenteerde maatregelen. Tegelijkertijd bestond het beeld dat de aanpak wat gefragmenteerd was. Met deze brief wil ik namens het kabinet een integrale visie op de aanpak van identiteitsfraude delen met uw Kamer. Deze visie hangt samen met de Rijksbrede aanpak van fraude, waarover u door de Minister van V&J wordt geïnformeerd. Het kabinet biedt u deze visie op de aanpak van identiteitsfraude samen aan met de eerste monitor «Identiteit in Cijfers»[1]. Doel is om die monitor jaarlijks op te stellen, om een altijd actueel en met de jaren steeds scherper inzicht te hebben in ontwikkelingen op het gebied van identiteit en identiteitsfraude.

Visie in het kort – slim voorkomen, vlot herstellen

Het kabinet heeft een toekomst voor ogen waarin alerte en goed geïnformeerde burgers en organisaties zich uitstekend weten te weren tegen pogingen tot identiteitsfraude. Identiteitsfraudeurs stuiten op een hecht web van actuele kennis en slimme technologische toepassingen. En áls ergens een identiteitsfraudeur toeslaat, dan wordt dit vroeg ontdekt en met vereende krachten vlot verholpen.

Voorkomen en herstellen van identiteitsfraude vraagt om een integrale, informatie gestuurde aanpak waarin partners in publieke en private sector de krachten samenballen[2]. Grote organisaties en zware ketens zijn kwetsbaar tegenover de kleine, creatieve, wendbare dadergroepen die hen bestoken en makkelijk van aanvalsstrategie kunnen veranderen. Het

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

[2] Europol pleit in haar Threat Assessment Internet Facilitate Organised Crime iOCTA, File nr: 2530–264 (pag 8) uit 2011 nadrukkelijk voor publiek en private samenwerking.

kst-26643-301
ISSN 0921 - 7371
's-Gravenhage 2013

antwoord op identiteitsfraude komt van moderne netwerken die snel reageren en slim anticiperen op identiteitsfraude.

Preventie staat voorop. Voorkomen is beter dan genezen. Dat vraagt vooral om hogere barrières tegen de snel toenemende identiteitsfraude in de digitale wereld. Het beoogde eID-stelsel moet hier een verbetering leveren. Ook zijn betrouwbare ijkpunten van de identiteitsinfrastructuur nodig: zorgvuldige controles op cruciale momenten, in face-to-face contacten tussen overheid en burgers. Daarnaast moet met het oog op preventie én detectie de kennis over daders en hun methoden beter worden gedeeld.

Aanleiding – structurele maatschappelijke schade

Identiteit is goud waard. Wie zich op betrouwbare wijze kan identificeren, heeft toegang tot een snel groeiend aanbod van diensten en producten wereldwijd en weet zich gezekerd van de rechten die verbonden zijn aan woonstaat en nationaliteit. De meeste mensen gaan hier eerlijk mee om. Maar de stijgende waarde van identiteitsgegevens en het groeiende aantal mogelijkheden om identiteitsgegevens te bemachtigen trekt wereldwijd fraudeurs aan.

Identiteitsfraude is modus operandi bij veel verschillende vormen van illegale en criminele activiteiten, zoals illegale grenspassage, illegale arbeid, mensensmokkel[3], drugshandel, terrorisme, witwassen van geld en vele typen fraude. Identiteitsfraude maakt daders ongrijpbaar of laat verkeerde mensen opdraaien voor een sanctie. Ze brengt de overheid financiële schade toe: voorzieningen worden verleend aan mensen die daar geen recht op hebben. Ook bij fraude tussen burgers onderling of tussen burgers en bedrijfsleven speelt identiteitsfraude een grote rol: uit het recente Nationaal Dreigingsbeeld blijkt dat in 80% van alle fraudegevallen gericht tegen burgers, bedrijfsleven en financiële instellingen sprake is van enige vorm van misbruik van identiteiten. Bijna 2 miljoen Nederlanders zijn tussen 2007 en 2012 slachtoffer geweest van enige vorm van identiteitsfraude[4]. Zij hebben naar schatting 2,8 miljard euro schade geleden[5]. Ook de emotionele impact kan ingrijpend zijn voor slachtoffers, net als de reputatieschade die zij ondervinden.

Identiteitsfraude berokkent de samenleving structurele schade en zal dat bij verdere toename nog sterker gaan doen. Ze ondermijnt het vertrouwen in de financiële instellingen, tast de betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgevoel. Ingrijpende incidenten in de digitale dienstverlening kunnen wantrouwen losmaken tegenover de digitale economie en de digitale overheid. En de relatie tussen een persoonlijk profiel en geautomatiseerde handelingen van apps, robots en op termijn zelfs elektronische implantaten brengt uiteenlopende gezondheids- en veiligheidsrisico's met zich mee. Een betrouwbare en sterk beveiligde identiteit wordt in de toekomst een kwestie van levensbelang.

---

[3] Uit de Criminaliteitsbeeldanalyse Mensensmokkel 2012 bleek dat misbruik van identiteits- en verblijfsdocumenten de meest voorkomende modus operandi is van mensensmokkelaars.

[4] Bron: PWC 2013. Recenter onderzoek van het CBS bevestigt dit beeld: in 2012 waren bijna 370.000 mensen slachtoffer van fraude bij aan- of verkopen via internet. Dat komt neer op drie procent van de Nederlandse bevolking van 15 jaar en ouder.

[5] Bron: Update onderzoek «Omvang van identiteitsfraude en maatschappelijke schade in Nederland», PWC, juni 2013

Aanpak vandaag – veel initiatieven, meer samenwerking nodig

Voor het voorkomen van identiteitsfraude en het herstellen van de schade die erdoor ontstaat zijn betrouwbare identiteitsinfrastructuren nodig die het mensen mogelijk maken om hun identiteit (of aspecten daarvan) voor anderen op een verifieerbare wijze kenbaar te maken, om de door anderen geclaimde identiteit (of relevante aspecten daarvan) te verifiëren en om in het geval van misbruik vast te stellen wie erachter zit, waar en wanneer misbruik heeft plaatsgevonden, hoe de gevolgen van misbruik kunnen worden hersteld en hoe verdere gevolgen kunnen worden voorkomen.

Dergelijke identiteitsinfrastructuren worden ontwikkeld door diverse private en publieke partijen, zoals bijvoorbeeld banken die hun klanten voorzien van een rekeningnummer, bankpas en identifier en een veilige omgeving voor online bankieren, of ziekenhuizen die medische en administratieve gegevens van hun patiënten veilig bewaren en patiënten een pas met foto meegeven voor identificatie. Kenmerkend voor Nederland is dat veel van deze infrastructuren zijn gebaseerd op de identiteitsinfrastructuur die door de overheid wordt onderhouden, met als kernelementen de Gemeentelijke Basisadministratie (GBA), het Burgerservicenummer (BSN), paspoort, ID-kaart, rijbewijs en DigID en voor buitenlanders die naar Nederland komen de Basisvoorziening voor Vreemdelingen (BVV) en een verblijfsdocument.

Zowel de overheid als private partijen werken permanent aan verbeteringen van hun identiteitsinfrastructuren en het beheer en gebruik ervan[6], vanuit de soms niet eenvoudig te verenigen perspectieven van betrouwbaarheid, privacy, gebruikersgemak en efficiëntie. Tegenover hen staan fraudeurs, die met steeds geraffineerdere methoden kwetsbare plekken in de identiteitsinfrastructuren vinden. Aan beide zijden worden steeds nieuwe methoden en technieken ontwikkeld en toegepast; bedreiging en beveiliging zijn in een permanente wedloop met elkaar verwikkeld. Identiteitsfraudeurs en de «facilitators» die hen bedienen zijn doorgaans goed geïnformeerd, innovatief en technisch competent. Ze opereren als criminele organisaties over landsgrenzen heen. Daarbij hebben ze het verrassingselement aan hun zijde: de keuze waar, hoe en wanneer ze toeslaan. Als de preventie of opsporing op één plek wordt versterkt, wijzigen ze makkelijk van aanvalsstrategie.

Het aantal plekken waar identiteitsfraudeurs kunnen toeslaan neemt toe. Er is vooral een sterke toename van fraude in de digitale wereld. Het potentieel voor voorkomen en herstellen van identiteitsfraude dat daar tegenover staat, wordt nog onvoldoende ontsloten. Gelukkig komt identiteitsfraude steeds beter in beeld, nemen veel organisaties en sectoren maatregelen en is er een ontwikkeling gaande richting meer samenwerking. Dat zijn drie positieve uitgangspunten waarop het kabinet zijn visie baseert voor een integrale aanpak van identiteitsfraude.

Gezamenlijke verantwoordelijkheid – burgers, bedrijfsleven en overheid

We mogen niet verwachten dat identiteitsfraude ooit is uit te bannen. Het is net als met gezondheid. Mensen zijn door de eeuwen heen altijd en overal wel bestookt door ziektekiemen – oude bekende of nieuwe. We ontwikkelen daar generatie op generatie een steeds sterkere weerstand tegen. Maar vroeg of laat wordt iedereen wel eens getroffen. Het is dan

[6] De bijlage geeft een analyse die tot deze visie heeft geleid, met o.a. maatregelen in diverse sectoren.

belangrijk om er op tijd bij te zijn en de juiste behandeling toe te passen. Zo is het ook met identiteitsfraude. Er zijn altijd wel criminelen op zoek naar kwetsbare plekken in het systeem – met oude en nieuwe methoden. De meeste mensen en organisaties ontwikkelen er een gezonde weerstand tegen door voorzichtig om te gaan met gegevens en door steeds betere technieken en methoden te benutten. Maar iedereen kan wel eens slachtoffer worden van identiteitsfraude. Dan is het zaak om de fraude zo snel mogelijk te detecteren en adequaat te behandelen.

Burgers, overheid en bedrijfsleven hebben een gezamenlijke verantwoordelijkheid voor het voorkomen en herstellen van identiteitsfraude. Burgers moeten er zelf voor zorgen dat ze een gezonde weerstand hebben tegen pogingen tot identiteitsfraude, door voldoende waakzaam te zijn en door de beschikbare middelen – zoals beveiligingssoftware – op de juiste manier te gebruiken. Zij zijn ook de eersten die in actie moeten komen als ze slachtoffer zijn van identiteitsfraude, of een poging daartoe.

Datzelfde geldt voor organisaties, in publieke en private sector: zij zijn zelf verantwoordelijk voor een gezonde weerstand tegen identiteitsfraude. Van organisaties mag daarnaast worden verwacht dat ze hun klanten zo goed mogelijk beschermen tegen identiteitsfraude, door zorgvuldig om te gaan met het verwerven, beveiligen en gebruiken van persoonsgegevens, door verzoeken om correctie en verwijdering van gegevens adequaat te behandelen en door klanten actief te voorzien van informatie en middelen om identiteitsfraude te voorkomen.

De rol van de overheid bij het voorkomen en herstellen van identiteitsfraude: zij zorgt online en offline voor een robuuste identiteitsinfrastructuur met betrouwbare ijkpunten: contactmomenten tussen burgers en overheid waarin goed opgeleide professionals met hulp van geavanceerde apparatuur een identiteit met de grootst mogelijke zekerheid vaststellen, registreren en verifiëren. De overheid borgt een aantal elementaire identificerende gegevens voor alle Nederlanders en iedereen die in Nederland verblijft. De overheid stelt heldere richtlijnen vast voor de veiligheid en betrouwbaarheid van particuliere identiteitsinfrastructuren en identificatiemiddelen en voor de begeleiding van slachtoffers van identiteitsfraude en -fouten. De overheid werkt samen met het bedrijfsleven en maatschappelijke organisaties aan een integrale aanpak van identiteitsfraudeurs. En de overheid monitort voortdurend de ontwikkelingen in de wereld van identiteitsfraude en verkent de grenzen van de bestrijding van deze groeiende tak van misdaad, samen met experts in publieke en private sector in binnen- en buitenland.

De visie in vijf beleidslijnen – gezamenlijke aanpak van identiteitsfraude

Burgers, overheid en bedrijfsleven staan het sterkst wanneer zij samen optrekken tegen identiteitsfraude. In de eerste plaats gaat het om het beter en breder benutten van kennis, technieken en methoden. In de tweede plaats gaat het om het beter op elkaar afstemmen van nieuwe maatregelen die door diverse partijen in publieke en private sector getroffen worden. In de derde plaats gaat het om het afspreken van een gezamenlijke richting voor ontwikkelingen op de lange termijn. Het kabinet onderscheidt daarbij vijf samenhangende beleidslijnen:

1. Gezonde weerstand

Voorkomen is beter dan genezen. De preventie van identiteitsfraude moet permanent evolueren met nieuwe vormen van bedreiging. Kennis en alertheid zijn sleutelfactoren, gedragen door bewustwordingscampagnes

en fraude-alerts. Bundeling van initiatieven uit publieke en private sector moet de algehele preventie versterken, doordat kennis en informatie een bredere doelgroep bereiken en doordat geldende regels en beschikbare middelen langs verschillende wegen onder de aandacht worden gebracht.

De menselijke factor zal op termijn echter niet voldoende blijken tegenover de steeds ingrijpender impact van identiteitsfraude. Er zullen zeker veel mensen zijn die zich met de meest actuele kennis en middelen goed weten te weren tegen identiteitsfraudeurs, maar er zullen ook altijd mensen zijn die daar niet of beperkt toe in staat zijn. Daarom wil het kabinet de weerstand tegen identiteitsfraude op termijn zo goed mogelijk «hard» organiseren: zo hoog mogelijke fysieke barrières opwerpen tegen identiteitsfraude.

Dat begint bij het minimaliseren van het gebruik van identificerende gegevens en bij het veilig bewaren ervan. Op beide punten gaan het borgen van privacy en het voorkomen van identiteitsfraude hand in hand. Overheid en bedrijfsleven zijn gebonden aan het principe van dataminimalisatie[7]. Dat principe geeft aan dat persoonsgegevens slechts mogen worden verwerkt als daartoe een noodzaak bestaat. Het principe is leidend bij het registreren en bewaren van gegevens in systemen. Bij de rijksdienst bijvoorbeeld wordt met het toetsmodel privacy impact assessment beoordeeld of systemen zo worden gebouwd dat er zo min mogelijk persoonsgegevens in worden opgeslagen en bewaard. De campagne «laat je niet zomaar kopiëren» was een invulling van het dataminimalisatieprincipe voor kopietjes van identiteitsbewijzen. De ID-cover van de NVVB (Nederlandse Vereniging voor Burgerzaken) is daar een slim en praktisch hulpstuk bij. De digitalisering van de dienstverlening van overheid en bedrijfsleven en de toenemende betrouwbaarheid van digitale verificatie- en autorisatieprocessen zorgen ervoor dat kopietjes van identiteitsbewijzen en papieren correspondentie in de toekomst minder nodig zijn, waardoor criminelen minder kans maken om aan identiteitsgegevens te komen door kopietjes te bemachtigen of in brievenbussen te vissen. Voor wat betreft het veilig bewaren van gegevens is op termijn winst te boeken met het compartimenteren van identiteiten[8] en het enkelvoudig en waar nodig versleuteld opslaan van gegevens: hackers hebben minder kansen naarmate identiteitsgegevens op minder plaatsen zijn opgeslagen. Dat is technisch mogelijk door niet dezelfde gegevens in veel verschillende systemen te bewaren, maar slechts op één goed beveiligde plek, met voor verschillende partijen een beveiligde toegang tot per situatie verschillende deelverzamelingen van die gegevens. De BRP zet met de enkelvoudige opslag van gerelateerde persoonsgegevens een belangrijke stap in die richting.

Tegelijkertijd moet er rekening mee worden gehouden dat er altijd wel gegevens in handen komen van kwaadwillenden en dat niet is na te gaan hoeveel gegevens er al in het criminele circuit bekend zijn. Hackers voorspellen dat alle gegevens die in databases zijn opgeslagen op een dag gehackt kunnen worden – zij het op afstand, zij het door handlangers aan de bron. En het is een feit dat de virtuele wereld niet aan geheugenverlies lijdt: eenmaal verstrekte gegevens verspreiden zich snel en laten

---

[7] De Wbp legt het principe van dataminimalisatie neer. Persoonsgegevens mogen slechts worden verwerkt als daarvoor een noodzaak bestaat (art 8). Art. 11, lid 1 bepaalt daarnaast dat persoonsgegevens slechts mogen worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (relevantie-eis). Verder is van belang dat verwerking van gevoelige persoonsgegevens in principe verboden is (art. 16–23 Wbp), en slechts onder strikte(re) voorwaarden is toegestaan.

[8] Het principe van compartimenteren van identiteiten is vergelijkbaar met het compartimenteren van olietankers: als er midscheeps een gat ontstaat, stroomt niet meteen de hele tanker leeg.

zich moeilijk vernietigen. Daarom wil het kabinet richting een situatie waarin de combinatie van naam, adres, Burgerservicenummer en andere persoonsgegevens nergens nog voldoende is voor het plegen van identiteitsfraude. Dat kan door in de toekomst bij controles altijd te vragen om een persoonlijke «sleutel» die fraudeurs moeilijk kunnen bemachtigen. Het eID-stelsel zal daar een belangrijke bijdrage aan leveren.

Een goede persoonlijke sleutel bestaat uit slimme en voor de situatie voldoende betrouwbare toepassingen van de drie-eenheid «*wie je bent, wat je weet en wat je hebt*». Het hoogste betrouwbaarheidsniveau – online en offline – bestaat uit een combinatie van een betrouwbaar fysiek middel (*wat je hebt*; bijvoorbeeld een pas met een chip en een identifier of smart phone), tweestapsverificatie (*wat je weet;* bijvoorbeeld met een dubbel wachtwoord, pincode, sms of een persoonlijke vraag-antwoord-combinatie) en biometrische kenmerken (*wie je bent*; bijvoorbeeld stem- of gelaatsherkenning). Veel landen verkennen nieuwe technieken en concepten. Datzelfde geldt voor innovatieve trendsetters als Apple, Google en Facebook. Het kabinet wil goed luisterend naar het maatschappelijke debat over dit thema onderzoeken hoe nieuwe technologie in uiteenlopende situaties optimaal ingezet kan worden voor het voorkomen van identiteitsfraude, het beschermen van privacy, het vergroten van de mogelijkheden voor burgers om zelf gegevens te beheren en delen en het bevorderen van economische kansen voor Nederland.

2. Betrouwbare controles

Een goede en efficiënte dienstverlening in publieke en private sector is slechts mogelijk dankzij betrouwbare identiteitsgegevens. Dat betekent voor veel instanties zoveel als een paradigmawijziging – zeker in een context van vergaande digitalisering van de dienstverlening: door de identiteit van burgers op de juiste momenten zorgvuldig te controleren, leveren organisaties grote winst op voor heel het maatschappelijk en economisch verkeer, doordat die controles ruimte scheppen voor efficiënte dienstverlening en burgers beschermen tegen identiteitsfraude. Zorgvuldige controles bedienen de burgers.

Dat vraagt om een investering in de «ijkpunten» van de Nederlandse identiteitsinfrastructuur: face-to-face contacten tussen burgers en overheid waarbij goed opgeleide professionals met hulp van geavanceerde apparatuur een identiteit met de grootst mogelijke zekerheid vaststellen, registreren en verifiëren. Een belangrijk initiatief in die richting is het programma «Naar betrouwbare persoonsgegevens» van de NVVB, dat zich richt op de ontwikkeling van kennis en vaardigheden van ambtenaren burgerzaken.

Ook een regionale concentratie van kennis en apparatuur, met ondersteuning van landelijke expertisecentra, kan de ijkpunten van de identiteitsinfrastructuur naar een hoger betrouwbaarheidsniveau tillen. In Oost-Nederland is positief gereageerd op een voorstel van de burgemeesters van Enschede, Apeldoorn en Zwolle om samen te werken aan de inschrijving in de GBA.

Het kabinet wil onderzoeken op welke slimme manieren extra controles kunnen worden toegepast bij het verstrekken van overheidsmiddelen en onder welke omstandigheden de overheid bepaalde identiteitsmiddelen kan intrekken. Om fraudeurs niet in de kaart te spelen is het van belang ook aandacht te besteden aan minder voorspelbare identiteitscontroles.

Op termijn moeten partijen met actuele kennis over identificerende gegevens een betere plek krijgen in het beheer en de validatie van

gegevens die voor veel partijen van belang zijn. Dat geldt zowel voor identiteitsvaststelling bij geboorte en immigratie, als voor identiteitsverificatie bij emigratie en overlijden, als voor correctie van gegevens wanneer registraties onjuist blijken. Het gaat hier om het beter benutten van specifieke kennis en kunde van onder andere gemeenten, politie, Koninklijke Marechaussee, IND, buitenlandse posten, Belastingdienst, zorginstellingen en financiële dienstverleners.

3. Vroege diagnose

Een vroege diagnose van gevallen van identiteitsfraude is van groot belang om snelle behandeling mogelijk te maken en om verspreiding te voorkomen. Opgave voor de betrokkenen van de diverse disciplines is om als netwerk te opereren en om integrale defensiestrategieën te ontwikkelen en implementeren. Dat moet op een manier gebeuren die beantwoordt aan de creativiteit en wendbaarheid van criminele organisaties en hun internationale speelveld.

Er zijn al diverse initiatieven tot interdisciplinaire samenwerking, zoals bij het Centrum voor Informatiebeveiliging en Privacy (CIP) onder regie van het UWV, de infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de expertisegroep fraudebestrijding onder regie van de Belastingdienst en de samenwerking tussen de Nationale Politie en de Koninklijke Marechaussee in de oprichting van vreemdelingenpolitieloketten en ID-desks. Dat zijn grote stappen die de «intelligence» versterken vanwaaruit identiteitsfraude en andere vormen van fraude kunnen worden bestreden.

De crux voor een vroege diagnose is het goed registeren van identiteitsfraude, het stapelen van casussen, het herkennen van patronen en het doorrechercheren op onregelmatigheden in het gedrag van groepen of individuen. Voorwaarde daarvoor is dat gegevens of indicatoren voor mogelijke fraude die de overheid of andere organisaties beschikbaar hebben met de juiste partijen worden gedeeld, met waarborgen voor privacy en voor rechtsbeginselen als het non-discriminatiebeginsel, gelijkheidsbeginsel en verbod op willekeur en met waarborgen tegen «false positives» (de onterechte veronderstelling dat iemand fraudeert). De aanpak hiervan staat beschreven in de Rijksbrede antifraudestrategie die de Minister van V&J u zal toezenden.

4. Adequate behandeling

Voor slachtoffers is het van belang dat zij zich erkend voelen in hun probleem, dat zij beschermd worden tegen hernieuwd slachtofferschap en dat zij ondersteuning krijgen bij aangifte en bij schadeloosstelling en herstel. Van de eerste aangifte van identiteitsfraude bij de politie tot het geheel oplossen van de zaak wil het kabinet dat de slachtoffers centraal staan.

Belangrijkste is dat de schade zich niet verder verspreidt. Dat is mogelijk door het direct ontwaarden van gestolen (of verloren) identificatiemiddelen: slachtoffers moeten hun identiteitsdocumenten, pasjes en digitale identiteiten onmiddellijk kunnen blokkeren en instanties kunnen oproepen tot verhoogde alertheid op hun gegevens. Ook moet online verifieerbaar zijn welke identiteitsdocumenten geldig en welke ongeldig zijn. Repressie haakt hier in op preventie.

Iedere instantie in publieke en private sector heeft zelf de verantwoordelijkheid om slachtoffers van fraude (en fouten) te helpen door foutieve of gecorrumpeerde gegevens te verwijderen of te corrigeren. Wanneer het

probleem zich verspreidt over meerdere administraties, moet herstel vanuit het netwerk komen. Dat vraagt om maatwerk: de beste methode is dat afgevaardigden van betrokken instanties samen aan tafel zitten om een probleem op te lossen. Voor schrijnende gevallen is er hulp van het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) en de Fraudehelpdesk. Het kabinet zet in op een geïntensiveerde samenwerking tussen het CMI, Fraudehelpdesk en andere organisaties die er zijn om slachtoffers te helpen.

Voor de publieke sector geldt dat ruim 600 organisaties gebruik maken van de Gemeentelijke Basisadministratie (GBA). Cruciaal voor een adequate behandeling van identiteitsfraude is dan ook dat burgers op tijd signaleren wanneer er iets loos is met hun gegevens in de GBA en dat fouten vlot hersteld worden. Het kabinet roept burgers op om er zelf voor te zorgen dat hun gegevens in de GBA kloppen, wat in 2013 is onderstreept met de campagne «Voorkom gedoe, kijk het na».

Op de lange termijn moet het spreiden van de gevolgen van fraude en fouten voorkomen worden door de eerder genoemde enkelvoudige opslag van gegevens.

5. Effectieve repressie

Bij de bestrijding van identiteitsfraude zijn het opwerpen van barrières en een verhoogde alertheid van private en publieke partijen in het handelsverkeer van doorslaggevend belang. Een effectieve en gerichte aanpak van fraudeurs vraagt om een verbinding tussen het strafrecht en andere vormen van handhaving, toezicht en nalevingsbevordering. Op die manier is er sprake van meer afgestemde en integrale handhaving waarin het strafrecht tijdig en situationeel wordt ingezet. De Minister van V&J gaat hier in zijn antifraudebrief nader op in.

Bij een effectieve repressie van identiteitsfraude mag niet vergeten worden dat misbruik van identiteiten overwegend een faciliterende handeling is om een delict te plegen. Identiteitsfraude is geen doel op zich, maar een middel, wat ook uit de gehanteerde definitie voortvloeit. De aanpak van identiteitsfraude staat dan ook niet op zichzelf, maar maakt deel uit van de aanpak van criminaliteitsfenomenen waarbij identiteitsfraude modus operandi is.

Fraude met identiteitsdocumenten is strafbaar volgens artikel 231 van het Wetboek van Strafrecht[9]. Fraude met identificerende persoonsgegevens (bijvoorbeeld het aannemen van een valse naam of een valse hoedanigheid) vormt onderdeel van meer algemene delictsomschrijvingen als oplichting (artikel 326 Sr), flessentrekkerij (artikel 326a Sr) en bedreiging

[9] Wetboek van Strafrecht, Artikel 231: «1. Hij die een reisdocument valselijk opmaakt of vervalst, of een zodanig stuk op grond van valse gegevens doet verstrekken dan wel een aan hem of een ander verstrekt reisdocument ter beschikking stelt van een derde, met het oogmerk het door deze te doen gebruiken als ware het aan hem verstrekt, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie. 2. Met dezelfde straf wordt gestraft hij die in het bezit is van een reisdocument waarvan hij weet of redelijkerwijs moet vermoeden, dat het vals of vervalst is, dan wel opzettelijk gebruik maakt van een niet op zijn naam gesteld reisdocument.»

(artikel 284 e.v. Sr)[10]. Voorts kent het Wetboek van Strafrecht specifieke strafbaarstellingen voor de aanpak van misdrijven waartoe fraude met identificerende persoonsgegevens vaak de opstap vormt. Bij die misdrijven gaat het bijvoorbeeld om mensensmokkel, witwassen, bank- of uitkeringsfraude, terrorisme of drugs- en wapengerelateerde misdrijven.

Strenge repressiemaatregelen moeten in combinatie met stevige preventiemaatregelen een afschrikkende werking vormen: bij potentiële fraudeurs moet het verhaal rondgaan dat identiteitsfraude in Nederland een onbegonnen zaak is.

Internationale aanpak

Een integrale aanpak van identiteitsfraude op Europees niveau is nog veel complexer dan een aanpak met Nederlandse partners: de lidstaten hebben alle hun eigen historie van vaststellen, registreren en verifiëren van persoonsgegevens en daaruit zijn heel verschillende wetten, regels, systemen en middelen voortgevloeid. Het spreekt voor zich dat de aanpak op mondiaal niveau nog complexer is.

Toch is een internationale aanpak cruciaal voor preventie en bestrijding van identiteitsfraude. De georganiseerde misdaad kent geen grenzen. Hoe sterk ook de nationale aanpak, via kwetsbare plekken in andere landen blijven de gevolgen van identiteitsfraude Nederland bereiken. Daarnaast zijn internationaal opererende dadergroepen niet te bereiken met een nationale aanpak. Het grensoverschrijdende karakter van identiteitsfraude – in het bijzonder in de digitale wereld – levert grote uitdagingen op voor Europese en internationale samenwerking. Het kabinet pleit daarom voor intensiveren van de samenwerking op EU-niveau voor het voorkomen en bestrijden van identiteitsfraude.

Uitvoeringsagenda aanpak identiteitsfraude

De visie die u in deze brief is voorgelegd, zal worden uitgewerkt in een uitvoeringsagenda Aanpak Identiteitsfraude. Die agenda zal recht doen aan de vele initiatieven die al worden genomen in de aanpak van identiteitsfraude. Het gaat dan zeker om de initiatieven waarbij deskundigen van verschillende disciplines en sectoren elkaar opzoeken om samen te leren en samen zaken aan te pakken – regionaal, nationaal en internationaal. Het zijn dergelijke verbeteringen die het netwerk van fraudebestrijders het fijnmazige karakter geven dat nodig is om fraudeurs te slim af te zijn. Wanneer vanuit de visie nieuwe maatregelen voortvloeien waarvoor nog geen middelen zijn voorzien in de begroting(en), worden business cases opgesteld. De business cases worden getoetst voordat besloten wordt of de maatregelen worden getroffen.

Voor de zomer van 2014 zal het kabinet u een voorstel voor deze uitvoeringsagenda sturen. Het kabinet hecht eraan hierbij het belang van het

[10] Wetsvoorstel wijziging van het Wetboek van Strafrecht en de Wegenverkeerswet 1994 in verband met de verbetering van de aanpak van fraude met identiteitsbewijzen en wijziging van het Wetboek van Strafvordering, de Beginselenwet justitiële jeugdinrichtingen en de Wet DNA-onderzoek bij veroordeelden in verband met de verbetering van de regeling van de identiteitsvaststelling van verdachten en veroordeelden (Kamerstuk 33 352). Dit wetsvoorstel voorziet erin dat meer frauduleuze gedragingen met identiteitsbewijzen strafbaar worden gesteld. Voorts wordt hiermee misbruik van identificerende persoonsgegevens afzonderlijk strafbaar gesteld en meer op één lijn gesteld met misbruik van reisdocumenten en identiteitsbewijzen waarvoor artikel 231 van het Wetboek van Strafrecht wel een aparte strafbaarstelling kent.

verbreden van de visie en het uitwerken van een uitvoeringsagenda in publiek-private samenwerking te benadrukken, net als de hoofdrol die burgers zelf vervullen bij de aanpak van identiteitsfraude.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk