AUTORITEIT
PERSOONSGEGEVENS

AP - Gespreksnotitie Rondetafelgesprek Fraudepreventie (CIFAS) – 13 januari 2022 – vaste commissie voor Justitie en Veiligheid

In een vrije, democratische samenleving moeten mensen erop kunnen vertrouwen dat organisaties en bedrijven zorgvuldig omgaan met hun gegevens. Bedrijven, centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over steeds meer – vaak gevoelige en bijzondere – persoonsgegevens. Deze data worden ingezet om maatschappelijke en economische kansen te creëren, maar kunnen ook worden gebruikt om fraude tegen te gaan. In de basis zijn fraudepreventie- en bestrijding nobele doelstellingen. Het is immers belangrijk dat burgers en bedrijven niet het slachtoffer worden van fraudeurs. En het is ook belangrijk dat burgers en bedrijven zich tegen fraude kunnen verweren.

Het verwerken en koppelen van bestanden om fraude te voorkomen, kan echter ook averechts werken en zelfs kwalijke gevolgen hebben: burgers kunnen erdoor in grote problemen komen. Mensen die (onterecht) op een fraudeurslijst staan, krijgen mogelijk te maken met stigmatisering. Ook is het mogelijk dat mensen per ongeluk op 'het verkeerde lijstje' terechtkomen. De kans is dan groot dat je nergens meer een telefoonabonnement kunt afsluiten of in Nederland niets meer via internet kunt bestellen. Dan kun je dus in feite niet meer normaal leven. De Toeslagenaffaire heeft aangetoond hoe fout het kan gaan als bestanden ten onrechte en foutief gekoppeld worden. Het is dus belangrijk dat we zeer zorgvuldig omgaan met het fundamentele recht van gegevensbescherming, en daarmee onze rechtsstaat. De Autoriteit Persoonsgegevens (AP) maakt zich hier sterk voor.

Samenvatting:

- **Het recht op gegevensbescherming is een fundamenteel recht van burgers en essentieel voor onze rechtstaat en samenleving.**
- **Bedrijven en organisaties beschikken over steeds meer gevoelige en bijzondere persoonsgegevens. Deze kunnen worden ingezet voor fraudebestrijding.**
- **Het is belangrijk dat burgers en bedrijven zich verweren tegen fraude.**
- **Private partijen kunnen strafrechtelijke persoonsgegevens ten behoeve van derden verwerken, als de AP hier een vergunning voor heeft afgegeven.**
- **In het bijzonder voor cross-sectorale deling van strafrechtelijke gegevens geldt een strenge toets. Private organisaties mogen dus niet zomaar een 'fraudeursdatabase' beheren en delen.**
- **Het overhevelen van overheidstaken met betrekking tot fraudeopsporing –en bestrijding naar een private partij is een hele grote en principiële stap. De AP is hier zeer kritisch over.**

Nadere toelichting AP

- Fraudeopsporing- en bestrijding zijn primair een taak van de overheid en voornamelijk belegd bij de politie. De politie moet zorgen voor de handhaving van de rechtsorde en hulp geven aan mensen die dit nodig hebben. Het strafrechtdomein bevat daarom ook een hoop wetten, regels en waarborgen om betrokkenen te beschermen. Dit houdt bijvoorbeeld in dat een verdachte onschuldig is, tenzij het

tegendeel wordt bewezen. Deze 'onschuldpresumptie' is een groot goed in de democratische rechtsstaat.

- Fraudeopsporing- en bestrijding mogen niet zomaar door iedereen worden uitgevoerd. Bij fraudeopsporing- en bestrijding is het belangrijk dat de vereiste waarborgen voor gegevensverwerking en gegevensdeling worden nageleefd. Zo moet de verwerkingsverantwoordelijke controleren of de gegevens kloppen en moet de proportionaliteit en subsidiariteit van de verwerking worden afgewogen.

- Belangrijk om te benadrukken, is dat burgers en bedrijven zichzelf natuurlijk mogen verweren en beschermen tegen fraudeurs omdat dat immers een gerechtvaardigd belang betreft en zolang zij dit zorgvuldig doen. Hierbij mogen zij ook persoonsgegevens verwerken als dat noodzakelijk is, tenzij de belangen van de betrokkenen zwaarder dienen te wegen. Bedrijven die te maken hebben met fraude kunnen bijvoorbeeld aangifte doen bij de politie of advies vragen bij een organisatie zoals de Fraudehelpdesk. Ook is voorlichting aan burgers van groot belang. Iedereen kent de nare voorbeelden van illegale websitelinks waar je per ongeluk op klikt en plots je geld of gegevens kwijt bent, of malafide clubs die valselijk vragen om een kopie van je bankpas of identiteitsbewijs. Het is belangrijk dat burgers daar bewust van zijn.

- Maar het is een grote en principiële stap om politietaken – zoals fraudeopsporing- en bestrijding - over te hevelen naar een private stichting of organisatie. Daar is nu ook geen wettelijke grondslag voor. Als de wetgever in Nederland hier toch een grondslag voor wilt creëren, moet zij hier heel terughoudend mee omgaan. Als de politie te weinig capaciteit heeft om fraudezaken te behandelen, is dit een serieus probleem. De oplossing voor dat probleem zou echter niet moeten zijn dat politietaken worden overgeheveld naar private organisaties.

- Private partijen - bijvoorbeeld verenigingen of stichtingen - die een bijdrage willen leveren aan fraudepreventie- en bestrijding moeten zich houden aan de voor hen geldende wettelijke kaders. Zo moeten zij zich houden aan de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Voor hen geldt immers niet een specifiek wettelijk kader zoals dat geldt voor politie en justitie.

- De AVG stelt dat elke verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen alleen onder toezicht van de overheid plaatsvindt of indien het Unierechtelijk of lidstatelijk recht de verwerking toestaat.[1]

- In de UAVG staat onder meer dat strafrechtelijke gegevens ten behoeve van derden alleen mogen worden verwerkt wanneer de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden.[2]

- Een vergunning voor het verwerken van strafrechtelijke persoonsgegevens ten behoeve van derden[3] (bijvoorbeeld fraudeslachtoffers) wordt door de AP niet zomaar afgegeven. Zeker als het gaat om het cross-sectoraal delen van strafrechtelijke persoonsgegevens van (mogelijke) fraudeurs moet een zeer

[1] Artikel 10 AVG
[2] Artikel 1, 32 en 33 UAVG
[3] Zoals bedoeld in artikel 33, vierde lid, onder c, UAVG jo. artikel 33, vijfde lid, UAVG

strenge toets worden doorstaan. Het gaat hier immers om het delen van mogelijk gevoelige gegevens van burgers tussen verschillende sectoren. Om dit proces te verduidelijken heeft de AP de Handreiking cross-sectorale gegevensdeling tussen private partijen opgesteld.

- Deze wetgeving is in het leven geroepen om burgers te beschermen tegen oneigenlijke gegevensverwerkingen. Als het gaat om verwerkingen van strafrechtelijke persoonsgegevens is dit recht zeer belangrijk, omdat burgers echt in de knel kunnen komen. Zo kan een burger op een zwarte lijst komen te staan of in een database worden opgeslagen als 'fraudeur', zonder dat deze 'fraudelijst' hiervoor een bevoegdheid heeft én zonder inachtneming van de benodigde waarborgen.

- Private partijen zoals Vereniging VODIOM en de Fraudehelpdesk zetten zich in voor burgers en bedrijven die slachtoffer zijn van fraude en om anderen te behoeden voor fraude. Voor het uitvoeren van de werkzaamheden willen zij persoonsgegevens van strafrechtelijke aard verwerken ten behoeve van derden. Zij hebben hiervoor een vergunning aangevraagd bij de AP. De AP heeft deze vergunningsaanvragen afgewezen; de risico's voor betrokkenen zijn te groot. Voor verdere toelichting zie: hier voor Vereniging VODIOM en zie hier voor de Fraudehelpdesk.

- De AP heeft eerder wel vergunningen afgegeven voor het verwerken van strafrechtelijke persoonsgegevens, de zogenaamde 'zwarte lijsten'. Het gaat hierbij om vergunningen die slechts sectoraal of in een klein geografisch gebied gelden, zoals Pifi of het Collectief winkelverbod Wageningen-Binnenstad.

- In het Verenigd Koninkrijk (VK) wordt gebruik gemaakt van Cifas. Dit is een non-profit organisatie die haar leden helpt om fraude zoveel mogelijk te voorkomen. Cifas deelt met behulp van haar database informatie met haar leden met betrekking tot fraude. Het gaat hierbij om het grootschalig, landelijk en cross-sectoraal delen van persoonsgegevens van strafrechtelijke aard. Dit betekent dat de inbreuk op het recht van gegevensbescherming van de betrokkenen enorm is.

- Waarom kan er in Nederland geen gebruik gemaakt worden van een systeem zoals Cifas? De AVG laat ruimte aan lidstaten om op bepaalde vlakken zelf invulling te geven aan de AVG, en dus eigen wetten en regels op te stellen. In het VK is er voor de activiteiten van Cifas een wettelijke basis, oftewel een grondslag, waarop de verwerking gebaseerd is en waardoor de verwerking is toegestaan. In Nederland is er tot nog toe niet voor gekozen om een dergelijke wettelijke basis te creëren voor dit soort verwerkingen door private partijen.

- Als de wetgever er toch voor kiest om de verwerking van strafrechtelijke gegevens ten behoeve van derden naar de private sfeer te halen, dan moeten er voldoende waarborgen zijn. Vergelijkbaar met de waarborgen die een verdachte heeft in de strafrechtketen. Dit kan bijvoorbeeld worden vastgelegd in een wet; zo wordt de democratische legitimiteit gewaarborgd. Daarnaast kan worden gedacht aan waarborgen die bestaan voor particuliere recherchebureaus. Zij werken volgens een strikte gedragscode, hebben een vergunningplicht en staan onder toezicht van de overheid. De AP kijkt in het geval van een wetsvoorstel voor een wettelijke basis zeer kritisch mee. Voor ons staat voorop dat burgers en onze rechtsstaat beschermd worden.