## Rechtmatigheid van de gegevensverwerking

In Nederland bestaat er geen wettelijke basis voor de verwerking van strafrechtelijke gegevens door private partijen ten behoeve van cross-sectorale gegevensverwerking, omdat er geen uitzondering is op het verwerkingsverbod van strafrechtelijke gegevens. De enige route die openstond voor VODIOM was het doen van een vergunningsaanvraag bij de Autoriteit Persoonsgegevens.

Door het afwijzen van de vergunningsaanvraag van VODIOM door de Autoriteit Persoonsgegevens bestaat er geen mogelijkheid meer om rechtmatig persoonsgegevens te verwerken in het kader van fraudebestrijding.

Dit is anders in het Verenigd Koninkrijk. CIFAS heeft daar een wettelijk verankerde status als ‘fraud prevention organisation’. Dit stelt hen in staat om met publieke en private instanties strafrechtelijke gegevens te delen.[[1]](#footnote-2)

Om meer mogelijkheden te creëren voor het delen van strafrechtelijke gegevens is dus een specifieke wettelijke basis nodig.

## Naar een wettelijke basis voor cross-sectorale gegevensdeling in Nederland?

Bij de vraag of er een wettelijke basis voor cross-sectorale gegevensdeling moet komen in Nederland moeten grofweg twee belangen worden gewogen: dat van het beschermen van consumenten en bedrijven tegen fraude en dat van de bescherming van de rechten en vrijheden van de geregistreerden. In het bijzonder moet daarbij rekening worden gehouden met personen die mogelijk onterecht in het systeem komen.

*Zwaarwegend maatschappelijk belang*

Hoewel het aantal geregistreerde misdrijven al jarenlang daalt, nemen de bedrog- en valsheidsmisdrijven elk jaar toe.[[2]](#footnote-3) Omdat de politie niet de hoogste prioriteit toekent aan de opsporing en vervolging van fraude, ligt de verantwoordelijkheid grotendeels bij het bedrijfsleven zelf. Deze verantwoordelijkheid kunnen zij maar beperkt nemen omdat zij geen gegevens mogen delen die de vroegtijdige signalering van potentiële fraudeurs tussen sectoren mogelijk maakt. Uit onderzoek van CIFAS blijkt dat jaarlijks meer dan een miljard euro aan schade wordt voorkomen omdat frauders in een vroegtijdig stadium worden gesignaleerd.[[3]](#footnote-4)

Tenslotte moet nog gewezen worden op een bijkomend positief effect van CIFAS: de ‘preventieve registratie’. Deze registratie zorgt ervoor dat mensen die het slachtoffer zijn van identiteitsfraude niet ten onrechte worden geweigerd door banken of andere instellingen. Hiermee draagt Cifas dus bij aan de bescherming van de rechten en vrijheden van betrokkenen.

*Risico’s voor de betrokkenen*

Daar tegenover staan de risico’s voor de betrokkenen. Zoals de Autoriteit Persoonsgegevens terecht aangeeft is het risico van een cross-sectoraal systeem voor gegevensuitwisseling groot. Met name (sociale) uitsluiting is een risico van het inrichten van een dergelijk systeem. Daarnaast valt te denken aan reputatieschade voor de betrokkenen.

Bij mijn weten is er geen (wetenschappelijk) onderzoek gedaan naar de omvang en de impact van registraties in het CIFAS systeem op de betrokkene. Wel is er anekdotisch bewijs dat er sprake is van vals-positieven, met een negatief effect op betrokkenen. Met name de aantasting van de credit score van betrokkenen kan een negatief effect hebben op de betrokkene.

## Waarborgen

Mocht de wetgever besluiten om cross-sectorale gegevensdeling mogelijk te maken, dan is het van groot belang dat de volgende waarborgen wettelijk verankerd worden:

* Er moeten duidelijke grenzen worden gesteld aan het gebruik van het fraudepreventiesysteem.
* De registratie moet beperkt worden tot duidelijke afgebakende categorieën misbruik.
* De criteria voor registratie en de bijbehorende bewijslast moeten zeer stevig zijn, zodat vals-positieven worden voorkomen.
* De betrokkene moet duidelijk geïnformeerd worden bij opname.
* Er moeten toegankelijke bezwaar- en beroepsmogelijkheden zijn.
* De registratie moet betrekking hebben op substantiële fraude en het gebruik van de data moeten in relatie staan tot die fraude.
* De registratie moet beperkt zijn in de tijd (beperkte bewaartermijnen).
* Een registratie moet aanleiding zijn voor aanvullende toetsing of risico-beperking aan de kant van de ondernemer, niet uitsluiting.

Voorts is intern en extern toezicht van groot belang. Naast het toezicht van de Autoriteit Persoonsgegevens kan daarbij bijvoorbeeld gedacht worden aan een verplichte ombudspersoon.

## Ten slotte: brede aanpak fraudebestrijding

Mocht een cross-sectoraal systeem van gegevensuitwisseling worden ingericht en succesvol zijn, dan valt het te verwachten dat criminelen zich zullen richten op andere vormen van fraude met een lagere pakkans en een hogere succesgraad. Om te voorkomen dat andere vormen van fraude populairder worden, is het verstandig in wet- en regelgeving te anticiperen op dit mogelijke ‘waterbed effect’.

1. Schermer, B. W., Schop, T. (2019), *Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding*, Considerati, p. 32 [↑](#footnote-ref-2)
2. <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1638179804094>. Zie ook: Jaarverantwoording Politie 2020 [↑](#footnote-ref-3)
3. https://www.cifas.org.uk/newsroom/highest-numbers-2019 [↑](#footnote-ref-4)