Frauderegister: AVG en het bestrijden van (digitale) criminaliteit

Het plegen van fraude is van alle tijden. Door de toenemende digitalisering verplaatst fraude zich naar het digitale domein. Dit is een ontwikkeling die door de gevolgen van COVID-19 lijkt te zijn versterkt en versneld en het probleem speelt breed. Niet alleen in Nederland maar ook mondiaal is een sterk stijgende trend waar te nemen. De lockdowns als gevolg van de Corona-pandemie hebben niet alleen voor een toename van online aankopen gezorgd, maar heeft er ook voor gezorgd dat fraudeurs nieuwe wegen zijn gaan bewandelen om aan inkomen te komen.
Fraude is ook specifieker en professioneler geworden. Uit onderzoek blijkt dat 40% van de fraude professioneel georganiseerde fraude is. Het is gepersonaliseerd, afgestemd op de locatie (het land) en gericht op bepaalde doelgroepen. Voorbeeld: We zien een verschuiving van waar men voorheen een phising mail stuurde in slecht Nederlands met dubieuze afzender en slechte opmaak naar voorbeelden van social enginering over langere periode (bijv 2 maanden) waar men een individu langzaam bewerkt om tot actie over te gaan. De doelgroep is hier regelmatig “ouderen”.

Er zijn vele vormen van fraude met hun eigen varianten. Criminelen misbruiken onder andere buitgemaakte digitale identiteiten (account takeovers) voor eigen gewin ten koste van ondernemingen als webwinkels, banken en telecomaanbieders. Verder zien we veel vormen van “Afleverfraude” waarbij bijvoorbeeld een pakketje op een bepaalde manier wordt bezorgd of afgehaald, zonder dat ervoor is betaald. Achteraf betalen – een wettelijke verplichting in Nederland - is hierbij de meest voorkomende betaalmethode. Ook het zogenaamd niet bezorgde pakketje -dat wettelijk gezien door de retailer opnieuw moet worden verstuurd-, is een voorbeeld van afleverfraude. Een variant hierop is dat van een order van 5 artikelen er zogenaamd 2 ontbreken, en deze door de webwinkel opnieuw moet worden gestuurd.

Maatregelen

Als aanpak laat het uitwisselen van informatie over fraude-incidenten binnen specifieke branches een bewezen preventieve werking zien. Deze uitwisseling kan plaatsvinden via een frauderegister. Het uitwisselen van informatie ‘op maat’ tussen bedrijven onderling en met de overheid om fraude en het faciliteren van ondermijning tegen te houden, komt in Nederland echter niet goed van de grond. Dit terwijl we in andere (voormalige) Europese landen zoals Engeland en Ierland) hier wel, door autoriteiten goedgekeurde, toepassingen van zien.
In Nederland vormen de wet- en regelgeving rond het verwerken van strafbare gegevens en met name de uitleg van de privacywetgeving door de Autoriteit Persoonsgegevens (AP) vooralsnog de belemmering. Concreet: de AP geeft geen goedkeuring voor een frauderegister die over verschillende branches heengaat. Hierdoor is het in de ogen van bedrijven zo dat de bescherming van persoonsgegevens van criminelen belangrijker lijkt dan de aanpak van hun daden en hebben bedrijven het nakijken.

Om fraude te voorkomen en criminelen aan te pakken moet er daarom een manier komen om sectoroverschrijdende informatie-uitwisseling mogelijk te maken die én die past binnen de regels van de Europese AVG én die de privacy van (goedwillende) burgers beschermt. Gezien de urgentie van de aanpak van ondermijning en fraude vragen we de overheid om dit via wetgeving te regelen, zodat de AP niet langer een belemmering vormt en het voor aangewezen partijen mogelijk wordt hun verantwoordelijkheid te nemen. Als argument geeft de AP letterlijk het voorbeeld van de “lijsten” in de toeslagenaffaire. Het lijkt er op dat een verkeerd gebruikte methode zonder enige vorm van toezicht, het nu onmogelijk maakt om criminelen aan te pakken via een bewezen systeem. De AP kan daarbij prima haar taak als controleur vervullen.

Pak digitale criminaliteit aan door sectoroverschrijdende informatie-uitwisseling over criminelen wettelijk mogelijk te maken.