Eén front tegen criminaliteit

Visie op criminaliteit

Inhoudsopgave

Vooraf

Hoe snijden we criminelen preventief de pas af? Voorkomen is altijd beter dan genezen. Het helpt daarbij als het bedrijfsleven **één front tegen criminaliteit** vormt. En daarbij optimaal samenwerkt met de overheid om criminaliteit te bestrijden; ieder vanuit zijn eigen rol en verantwoordelijkheid. Door de krachten te bundelen, ontstaat meer slagkracht.

In deze notitie beschrijven VNO-NCW en MKB-Nederland de ontwikkelingen en problemen op het gebied van criminaliteit en welke stappen gezet kunnen worden om deze problemen aan te pakken. Dat betreft zowel stappen van het bedrijfsleven zelf als stappen die wij verlangen van de overheid.

Samenvatting

Wat gaat het bedrijfsleven zelf doen?

- Het brede bedrijfsleven staat op tegen criminaliteit. In woord en gedrag zal aangegeven worden dat er werk wordt gemaakt van het buiten de deur houden van criminelen. De "Eén front" missie tegen criminaliteit zal projectmatig vanuit VNO-NCW en MKB-Nederland worden ondersteund.
- Iedere branche en iedere ondernemer moet aandacht hebben voor digitale weerbaarheid en cyberveiligheid. Dat vraagt investeringen, trainingen en aandacht.

Wat gaat het bedrijfsleven doen in samenwerking met de overheid?

- Versterk de publiek-private samenwerking. Criminaliteitsbestrijding kan alleen door samenwerking tussen het bedrijfsleven en de overheid. Dat moet op landelijk niveau met ministeries en branches maar ook op regionaal niveau via de Platforms Veilig Ondernemen. Versterking kan gerealiseerd worden door o.a. gebruik te maken van de innovatieve kracht van het bedrijfsleven maar ook door goede onderlinge afspraken, waardoor preventie loont.
- Het delen van kennis over trends, ontwikkelingen en modus operandi tussen de overheid en het bedrijfsleven moet standaard werkwijze worden.
- In de witwasaanpak dient risico-gebaseerd gewerkt te worden. Poortwachters hoeven zo niet meer alles uit te vragen en te melden, maar kunnen hun inzet concentreren op de door de overheid vastgestelde hoog-risico gevallen.

Wat verlangt het bedrijfsleven van de overheid?

- Creëer een wet waarin de mogelijkheden tot gegevensdeling worden uitgebreid zodat het bedrijfsleven weet met wie het zaken doet en preventief kan acteren.
- Centrale regie op witwasaanpak, waardoor deze effectiever, efficiënter en veiliger wordt. Daarbij hoort ook synergie in acties tussen de verschillende toezichthouders.
- Geen verschuiving van verantwoordelijkheden. Het geweldsmonopolie blijft voorbehouden aan de overheid evenals repressieve taken.
- Voorkom versnippering van initiatieven. De overheid maakt veel geld vrij voor de aanpak van ondermijning, maar er is geen regie noch overzicht. Verschillende overheidsinstanties vragen hierdoor het bedrijfsleven acties te ondernemen zonder van elkaar te weten dat er al eerdere initiatieven lopen, convenanten zijn afgesloten, afspraken gemaakt, enz. Er wordt veel in pilots gewerkt zonder ervan te leren en tot voortzetting of uitbreiding van goede initiatieven te komen.
- Investeer in de aanpak van nieuwe vormen van criminaliteit. Digitale criminaliteit en cybercrime zullen toenemen. Zorg dat politie, OM, rechtbanken, toezichthouders en andere overheidspartijen op deze ontwikkeling zijn voorbereid. Dat geldt voor opleidingen, mankracht maar ook voor toereikende wetgeving om dit soort criminaliteit aan te pakken.

Inleiding

Nederland heeft een goed investerings- en vestigingsklimaat waardoor het hier goed ondernemen is. De goede infrastructuur, een open economie, uitstekende logistieke knooppunten en een gunstige ligging naar het Europese achterland zijn elementen die daarbij een rol spelen. Ook criminelen gedijen bij deze omstandigheden. Ook voor hen is het hier goed ondernemen. Daar komt nog bij dat door de grote tekorten bij de opsporing en vervolging de pakkans laag is. Een criminele win-winsituatie.

Nederland vervult mede door deze factoren een belangrijke rol in de internationale drugshandel[5], met alle negatieve gevolgen van dien: brute liquidaties, vermenging van boven- en onderwereld, witwassen van grote sommen (contant) geld, bedreiging van ondernemers en hun personeel, afpersing en omkoping. Naast het algemeen maatschappelijk ontwrichtende effect op de samenleving tast het ontstane beeld van Nederland als *narcostaat* ook het vestigings- en investeringsklimaat aan. Veiligheid is namelijk een basisvoorwaarde voor een goed functionerende samenleving en economie.

Enkele cijfers over criminaliteit in Nederland op een rij[6][7:89]:

- de hoeveelheid cocaïne die de Douane jaarlijks in Nederland in beslag neemt, is toegenomen van ongeveer 10.000 kilo in 2017 naar bijna 50.000 kilo in 2020. En in 2021 is alleen al in Rotterdam 72.808 kilo cocaïne in beslaggenomen, een stijging van 74 procent vergeleken met een jaar eerder.
- Tussen 2012 en 2021 is het aantal mensen van 15 jaar of ouder dat naar eigen zeggen slachtoffer werd van traditionele criminaliteit met 43 procent gedaald. Het totaal aantal door de politie geregistreerde misdrijven daalde met 52 procent. Het aantal slachtoffers van online fraude steeg daarentegen. 1 op de 6 Nederlanders werd slachtoffer van fraude. Totale schade was 2,75 miljard.
- 1 op de 5 mkb-bedrijven maakt een cyberincident mee met financiële schade.
- In Nederland wordt naar schatting 16 miljard euro per jaar witgewassen, al valt dit per definitie moeilijk vast te stellen.

5 ao-dlio--2-22---de-narcostand-van-nederland-fenomeenbeeld-drugs-2021.pdf (politie.nl)
6 HARC-team onderschept 72.808 kilo cocaïne in 2021 | Nieuwsbericht | Openbaar Ministerie (om.nl)
7 |, Fraudevictimisatie in Nederland | Fraudevictimisatie in Nederland (utwente.nl),
8 lectoraat-cybercrime-cybersecurity-de-geleerde-lessen-van-4-jaar-onderzoek-naar-cybersecurity (dehaagsehogeschool.nl)
9 DNB Van herstel naar balans

1. Informatie- en gegevensuitwisseling

- Het moet wettelijke mogelijk worden om gegevens onderling te delen.
- Het delen van kennis over trends, ontwikkelingen en modus operandi tussen de overheid en het bedrijfsleven moet standaard werkwijze worden.

1.1 Informatie delen

Criminelen zijn innovatief, opereren heimelijk en zullen er alles aan doen om onder de radar te blijven. Om hen te bestrijden moeten we beschikbare informatie ontsluiten. Juist daar zit een belangrijke bottleneck. In Nederland zijn de mogelijkheden tot nu toe beperkt en blijven kansen onbenut. Dit is onnodig. Bij de verschillende actoren - denk aan de Belastingdienst, de politie, de gemeente, een transporteur, een bank, een webwinkel, een telecomprovider of een verhuurder - is veel informatie voorhanden. Zoals een aangifte met een verklaring van het slachtoffer, een valse factuur met bijbehorend rekeningnummer van een crimineel of diens handlanger, camerabeelden waaruit een signalement van de dader te zien is, enz.

In de strijd tegen criminaliteit is het essentieel dat de verschillende (publieke en private) spelers de puzzelstukjes bij elkaar leggen om zo zicht te krijgen op de criminelen en ze te kunnen weren.

1.2 Wettelijke basis voor delen persoonsgegevens

In plaats van het voorkomen van criminaliteit kiezen we voor bescherming van de privacy, ook die van criminelen. Informatiedeling is vaak niet mogelijk. Maar in sommige gevallen zijn er uitzonderingen mogelijk: op basis van een (wetenschappelijke) pilot, een convenant of een vergunning. Hierdoor is een lappendeken ontstaan waardoor voor menigeen onduidelijk is wat wel of niet kan of mag. Dit alles leidt ertoe dat iedereen in een kramp schiet en er weinig tot niets gebeurt.
Gegevensdeling, dus namen en andere persoonsgegevens delen, levert maatschappelijke discussie op. Privacy is een groot goed maar de criminaliteit en het handhavingstekort nemen dusdanige vormen aan dat het niet mogen delen van informatie over daders ter discussie dient te worden gesteld. Voor zover deze discussie momenteel wordt gevoerd, prevaleert nog altijd het privacybelang. Om criminaliteit goed te kunnen bestrijden, ook preventief, zou het maatschappelijk belang om criminaliteit te voorkomen door de politiek zwaarder gewogen moeten worden.

In Nederland kan de Autoriteit Persoonsgegevens (AP) onder strenge voorwaarden een vergunning verlenen voor het delen van strafrechtelijke persoonsgegevens ten behoeve van derden. Er moet een zwaarwegend belang zijn en bij de uitvoering moeten voldoende waarborgen zijn ingebouwd om de persoonlijke levenssfeer van de betrokkene niet onevenredig te schaden. De AP acht onvoldoende aannemelijk dat een dergelijke gegevensverwerking ook noodzakelijk is voor andere (private) partijen. Fraudebestrijding is, aldus de AP, een overheidstaak. Ondernemers mogen elkaar hier onderling daarom niet waarschuwen.

Fraudepreventie is echter óók een taak van het bedrijfsleven, vinden VNO-NCW en MKB-Nederland. En dient een maatschappelijk belang. Een klant verlangt namelijk dat geen misbruik wordt gemaakt van zijn gegevens en een ondernemer wil kunnen checken met wie hij zaken doet. Een crimineel kan nu steeds weer toeslaan zonder al teveel hindernissen. Dat betekent steeds weer een slachtoffer, schade, een aangifte en belasting van het justitiële apparaat. Dit terwijl dit alles ook voorkomen had kunnen worden.

Het Verenigd Koninkrijk kent wél een - succesvol - systeem van onderlinge gegevensdeling. Op verzoek van de politie nemen ondernemers gegevens van frauderende klanten met onderliggend bewijs op in een centraal register. Hierdoor kan een ondernemer voordat hij of zij een overeenkomst

sluit met een nieuwe klant, eerst checken of deze klant bekend staat als fraudeur. Dit gaat via een hit/no hit systeem. Het systeem is met allerlei waarborgen omkleed, werkt al decennia en voorkomt voor miljoenen euro's aan fraude bij de aangesloten bedrijven. Ook de politie in het VK maakt gebruik van het systeem en heeft daardoor een betere informatiepositie. Eén front dus tegen fraudeurs, waarbij de overheid minimaal wordt belast en veel nieuwe fraudegevallen worden voorkomen. Een poging van MKB-Nederland om een vergelijkbaar systeem ook in Nederland in te voeren, is gestrand bij de privacy-autoriteit[10]. Er was voor de vergunningaanvraag een separate vereniging opgericht genaamd VODIOM[11].

Een stevige wettelijke basis zou zelfs tot meer privacybescherming kunnen leiden omdat de spelregels wettelijk zijn verankerd.

Het bedrijfsleven roept de politiek maar ook andere actoren op om een wettelijke basis te creëren om (strafrechtelijke) persoonsgegevens te kunnen delen tussen overheidsdiensten onderling, tussen overheid en bedrijfsleven, maar ook tussen bedrijven uit diverse sectoren. Een wettelijke basis maakt dan een einde aan de ontstane lappendeken en de overbelasting van de AP met vele vergunningsaanvragen.

1.3 Nieuwe inzichten door delen van kennis

De overheid en het bedrijfsleven zouden veel meer moeten kunnen bouwen op een solide publiek-private samenwerking, waarbij op een structurele, niet vrijblijvende wijze, over en weer kennis wordt uitgewisseld. De verkramping in onze samenleving ten aanzien van informatiedeling leidt er toe dat de mogelijkheden die er nu al zijn onvoldoende worden benut.

De overheid weet veel over criminaliteitsvormen en de modus operandi van criminelen. Het bedrijfsleven op haar beurt heeft veel kennis over de eigen bedrijfsprocessen, bijvoorbeeld over hoe een lading bananen vanuit Zuid-Amerika bij de supermarkt in de schappen komt. Deze beide werelden hebben ieder een schat aan informatie maar vinden elkaar nog veel te weinig. Door dit soort informatie bij elkaar te brengen ontstaan nieuwe inzichten en kennis. Het gaat daarbij uitdrukkelijk niet om persoonsgegevens maar om algemene informatie en kennis zoals trends, ontwikkelingen en criminele handelswijzen (modus operandi).

Door deze werelden bij elkaar te brengen krijgen bedrijven informatie over hun kwetsbaarheden en worden zij in staat gesteld om barrières op te werpen tegen criminelen die misbruik maken van het bonafide bedrijfsleven zoals de transport- en vastgoedsector en de financiële instellingen. De overheid is op haar beurt beter in staat zicht te krijgen op criminelen. Hierdoor gaat de pakkans omhoog. Overheid en bedrijfsleven vormen op deze manier één front tegen de criminaliteit.
In de haven van Rotterdam wordt deze methodiek succesvol toegepast[12]. Het kost tijd om elkaar te vinden en vertrouwen in elkaar te hebben maar deze vruchtbare samenwerking levert concrete resultaten op.

Overheid en bedrijfsleven hebben ieder een schat aan informatie, maar vinden elkaar nog veel te weinig. Door dit soort informatie bij elkaar te brengen ontstaan nieuwe inzichten en kennis.

[10] Op 8 oktober 2021 heeft de Autoriteit Persoonsgegevens de vergunningaanvraag om cross-sectoraal gegevens te mogen delen om fraude te voorkomen, afgewezen: https://www.autoriteitpersoonsgegevens.nl/documenten/besluit-afwijzen-vergunning-vodiom
[11] VODIOM: Veilig Ondernemen Door Informatiedeling Op Maat
[12] Deze samenwerking wordt voorgegeven in een Information Sharing Centre (ISC)

2 Publiek-private samenwerking

- Inzet op preventie wordt beloond doordat de politie die omstandigheid meeweegt bij de verdeling van de schaarse capaciteit.
- Zorg voor een veilig en eenvoudig aangifteproces.
- De witwasaanpak heeft regie en centrale sturing nodig waarbij risicogebaseerd gewerkt wordt en effectiviteit en efficiëntie vergroot wordt.
- Repressieve taken zijn en blijven voorbehouden aan de overheid.
- Innovatie in de publiek–private samenwerking is essentieel.

2.1 Aangifte doen

Ondernemers doen in lang niet alle gevallen aangifte. Hierdoor is de echte aard en omvang van criminaliteit niet goed in beeld te brengen.

Ondernemers voelen zich alleen staan. Aangifte doen kost veel tijd. Bovendien is er bij de handhaving geen prioriteit voor hun zaken. Politie, Openbaar Ministerie, rechterlijke macht en toezichthouders zijn structureel onder bemenst, met een groot handhavingstekort als gevolg[13]. Daders van zowel fysieke criminaliteit (bijvoorbeeld winkeldiefstal en witwassen) als van digitale criminaliteit (online fraude of cybercrime) blijven nu veelal ongemoeid. ‘Bloed & spoed’ krijgen (al jaren) voorrang op andere zaken[14]. Een winkeldiefstal of cyberaanval, die voor ondernemers veel impact heeft, valt echter zelden in die categorie. Het gevolg is een negatieve spiraal.

Om deze spiraal te doorbreken is het zinvol om preventie veel meer te belonen. Voorkomen van schade en slachtofferschap draagt tegelijkertijd bij aan het verminderen van de overbelasting van het systeem. Ondernemers die - ondanks dat ze alle mogelijke maatregelen hebben genomen in hun bedrijf om criminaliteit zoveel mogelijk buiten de deur te houden - toch getroffen worden, zouden voorrang moeten krijgen. Dat wil zeggen dat bij weging van het oppakken van een zaak de aangifte waarbij aantoonbaar eigen preventiemaatregelen zijn getroffen zou moeten prevaleren boven een slachtoffer die niet heeft geïnvesteerd in het nemen preventieve maatregelen.

Het mes snijdt daarbij aan twee kanten. Ondernemers worden aangespoord meer te investeren in preventie en vaker aangifte te doen. En dat zal een olievlekeffect hebben op andere ondernemers om zich ook beter te beveiligen. Als de buurman betere hekken plaatst, zal jij mee moeten om te voorkomen dat boeven bij jou komen. Die aangifte is echter óók interessant voor de politie. De crimineel die over de verhoogde dijk heeft weten te klimmen (en derhalve het ‘kruimeldiefniveau’ is ontstegen) komt zo beter in beeld.

Het aangifteproces kan ook een stuk eenvoudiger, door digitaal aangifte doen mogelijk te maken. Momenteel moeten ondernemers nog vaak fysiek naar een politiebureau, daarbij gehinderd omdat veel bureaus gesloten zijn waardoor ze verder moeten reizen en of beperkte openingstijden hebben. Digitaal aangifte doen is momenteel technisch niet mogelijk. Het wordt tijd dat de politiesystemen hier spoedig op aangepast worden. Dat scheelt veel kostbare tijd van ondernemers en levert de politie veel waardevolle informatie op. Belangrijk is dat, naast de standaard digitale aangifte, vertrouwelijk c.q. anoniem melden tot de mogelijkheden behoort. Veiligheid bij het melden van onraad, bijvoorbeeld door havenmedewerkers of poortwachters is essentieel. Zeker gezien de verharding van de ondermijnende criminaliteit.

[13] In 2022 bedraagt het tekort bij de politie veertienhonderd voltijdsbanen (www.politie.nl). De rechter ligt er wakker van: het lukt niet meer om op tijd én goed te vonnissen - NRC, 8 januari 2023 en Kamerstuk 2022Z15184, Personeelstekort rechtbank noodzaakt tot sepot zaken (rechtspraak.nl)
[14] Met bloed & spoed wordt bedoeld een moordzaak, verkrachting e.d. of directe hulpverlening

De aangiftebereidheid van ondernemers zal omhoog gaan als aangifte doen voortaan ook digitaal kan en dus minder tijd kost. Ook belonen van het nemen van preventiemaatregelen helpt hierbij.

2.2 Witwassen

Het doorbreken van het criminele verdienmodel en het tegenhouden van criminele geldstromen vormt een speerpunt van de overheid. Ondernemers hebben vanuit de Wet voorkoming Witwassen en het Financieren van Terrorisme (WWFT) verplichtingen zoals het checken van (nieuwe) klanten ('ken je klant') en het controleren van (bank-)transacties zoals een meldplicht bij ongebruikelijke overboekingen. De belangrijkste spelers die deze taken moeten uitvoeren zijn de zogenoemde poortwachters: makelaars, banken, advocaten, trustkantoren, notarissen, accountants en levensverzekeraars. Zij moeten voorkomen dat criminelen misbruik maken van het betalingsverkeer of van andere financiële transacties.

Maar waar ligt de scheidslijn tussen publieke en private taken? Ondernemers in de financiële sector worden disproportioneel vaak ingezet voor publieke taken. Eén vijfde van het bankpersoneel is verplicht bezig met het afvinken van compliance regels en het doen van meldingen, die vervolgens nauwelijks worden opgepakt door de overheid. De bestrijding van financiële criminaliteit is veel effectiever als deze mensen anders worden ingezet. Door de grote inzet op witwassen kunnen financiële dienstverleners minder financiële diensten leveren terwijl dit toch hun *core business* zou moeten zijn. Veel veelal kleinere ondernemers krijgen hierdoor geen financiering meer en zoeken noodgedwongen hun heil elders. Zij zijn hierdoor vatbaar voor criminelen die de 'helpende hand' willen bieden. Deze financiële steun wordt duur betaald. Ondernemers hebben echter onvoldoende ruimte om het goede te doen.

Leiden alle inspanningen ook daadwerkelijk tot het tegengaan criminele geldstromen en witwassen? Het ontbreekt aan een afdoende functionerend meetinstrumentarium om dit goed te onderzoeken. Ook is er te weinig regie op de nationale witwasaanpak waardoor er een versnipperde aanpak is en onvoldoende zicht op het brede plaatje. Het witwassen van echt grote drugswinsten verloopt niet via reguliere financiële instellingen, maar via een wereldwijd netwerk van ondergronds bankieren. Onderschepte communicatie tussen drugscriminelen heeft dit bewezen. Dit ontslaat poortwachters uiteraard niet van hun wettelijke verplichtingen. Middelgrote en kleinere criminelen trachten nog altijd hun geld via bonafide ondernemers wit te wassen. Maar het zou wel moeten leiden tot een goede discussie over de proportionaliteit van de huidige verplichtingen en de gevolgen daarvan voor Nederlandse ondernemers.

Het bredere plaatje moet ook Europees worden bezien. Is er een level playing field of worden Nederlandse ondernemers aan strengere regels onderworpen dan bijvoorbeeld Duitse ondernemers? Ook onze exportpositie is hierbij van belang. Er vindt veel internationale handel plaats vanuit Nederland met derde landen, waarbij in sommige van die landen witwascontroles lastig uit te voeren zijn en de internationale handel van Nederlandse ondernemers wordt geschaad. Witwassen is een internationaal probleem en kan dus niet alleen nationaal worden bekeken en beheerst.

De politiek heeft poortwachters tegen wil en dank een belangrijke rol gegeven. Maar verzuimt deze groep hiertoe te equiperen: er zijn te weinig wettelijke instrumenten en er is te weinig overheidssteun om 'de poort te wachten' en dus hun wettelijke taak goed uit te oefenen.
Financiële instellingen vragen momenteel bij alle transacties en klanten om de kans op witwassen volledig uit te sluiten. Dit heeft tot gevolg dat er onnodig vaak nee wordt verkocht en er onnodig veel meldingen worden gedaan bij de FIU[15]. Als poortwachters meer risico-gebaseerd kunnen werken en alleen informatie verstrekken over transacties die daadwerkelijk interessant zijn in het kader van het tegengaan van witwassen, komt er meer balans in. Betere informatiedeling onderling en samenwerking met de verschillende toezichthouder(s) en de overheid is hiervoor essentieel. Het voorkomt shopgedrag van criminelen. Na het doen van een melding, zou een terugkoppeling van de overheid aan de meldende instantie moeten zorgen voor versterking van de aanpak. Deze feedbackloop ontbreekt nu.

[15] De Financial Intelligence Unit - Nederland, de overheidsinstantie waaraan alle meldingsplichtigen ongebruikelijke transacties of zaken waarvan zij vermoeden dat ze te maken hebben met witwassen van geld of financiering van terrorisme, moeten melden

Verbetering moet er ook komen in het meldproces zelf. De overheid legt de poortwachters een wettelijke taak op maar verzuimt de hierbij horende randvoorwaarden te leveren en het proces dusdanig in te richten dat dit veilig gebeurt. Melden is een tijdrovende bezigheid en namen van meldende instanties worden niet afgeschermd met alle gevaren van dien.

De publiek-private samenwerking staat onder druk. Er is veel meer regie van de overheid nodig op het witwasdossier en meer balans in de keten. Poortwachters slaan de handen ineen om hun 'keten' effectiever en efficiënter te maken zodat bonafide klanten niet onnodig worden gecontroleerd. Hiertoe hebben ze de inzet en steun van de overheid nodig[16].

2.3 Preventie versus repressie

Repressie zonder preventie is dweilen met de kraan open, maar preventie zonder repressie een tandeloze tijger.

Voorkomen is beter dan genezen. Private partijen willen, kunnen en moeten criminaliteit zoveel mogelijk voorkomen. Investeren in preventie loont. Iedere euro die daarin wordt geïnvesteerd, verdient zich driedubbel terug. Het leidt tot minder schade bij bedrijven, minder kosten voor de burger en minder inzet van het overbelaste justitieel apparaat. Preventie en repressie moeten echter altijd hand in hand gaan.

Repressie is in principe het mandaat van publieke partijen zoals de politie die het geweldsmonopolie heeft en boetes kan opleggen. De inzet van bijvoorbeeld beveiligingsbedrijven is hieraan ondersteunend. Beveiligers hebben geen geweldsmiddelen. Maar door (personeels-)tekorten verschuift de overheid nu veel repressieve taken naar het bedrijfsleven, en worden regels voor ondernemers aangescherpt. Dat zie je bijvoorbeeld terug bij de invulling van de poortwachtersrol of winkeliers die zelfstandig boetes opleggen aan winkeldieven.

Verschuiving van rollen en verantwoordelijkheden is echter onwenselijk. Preventief handelen moet strikt gescheiden worden van repressieve taken, die aan overheid dienen te blijven voorbehouden. Waar gaten dreigen te vallen, kan publiek-private samenwerking een goede oplossing zijn, maar wel ieder vanuit (zijn) eigen rol en verantwoordelijkheid. Sommige taken, zoals het informeren van beveiligingsbedrijven over signalementen van gezochte personen of voertuigen, of het bewaken van een plaats delict, of het begeleidend van voertuigen voor een alcoholcontrole kan worden uitgevoerd door private beveiligers. Dit ontlast de politie. Maar zonder het specifieke politiewerk over te nemen. Het aanhouden van een verdachte of het afnemen van een blaastest bijvoorbeeld blijft een taak van de politie.

Preventie en repressie zijn gescheiden rollen. Private partijen kunnen sommige taken overnemen van de politie. Maar nooit verantwoordelijk worden voor het echte politiewerk.

2.4 Innovatie

Criminelen zijn innovatief, lenig en adaptief. Dat is het bedrijfsleven ook. Maatschappelijke en technologische ontwikkelingen gaan snel. Inzet op innovatie is daarom essentieel. Denk aan gebruik van techniek voor het monitoren van ongebruikelijke transacties, het gebruik van AI en het valideren van echtheid, gebruik van slimme containers in de havens of slimme camera's tegen winkelcriminaliteit.

De overheid is minder wendbaar maar kan wel een belangrijke rol spelen in het faciliteren en equiperen van het bedrijfsleven om criminaliteit tegen te gaan. Bijvoorbeeld met subsidies en wetten die innovatie mogelijk maken.

Innovatie kan ook plaatsvinden in de samenwerking tussen het bedrijfsleven en de overheid. Daar waar de politie geen tijd heeft om een eenvoudige winkeldiefstal af te doen, zou een BOA daar wellicht taken kunnen overnemen.

---

[16] Poortwachters willen regierol overheid in aanpak witwassen | VNO-NCW en rapport: 'Krachten gebundeld' van KPMG, augustus 2023

De overheid kan ondernemers steunen en stimuleren bij innovaties op het gebied van preventie. Daarbij dienen good practices uit het buitenland ook meenomen te worden.

3 Een front tegen criminaliteit

- Als bedrijfsleven een gezamenlijke vuist tegen criminaliteit.
- Aandacht voor trainingen, tegengaan van crimineel geld, weerbaarheid binnen bedrijfsleven.
- Voorkom versnippering van succesvolle acties en initiatieven. Regie en ondersteuning van de overheid is nodig.

3.1 De overheid moet regie nemen

De overheid is uiteraard een belangrijke speler als het gaat om het tegengaan van criminaliteit. Op de 'justitieketen' is in het verleden echter fors bezuinigd. De gevolgen daarvan zijn nog altijd voelbaar bij politie, Openbaar ministerie en bij rechtbanken.

De laatste jaren is het tij gekeerd.[17] Het kabinet Rutte IV heeft één miljard euro geïnvesteerd in het versterken van de keten[18], de aanpak van ondermijning en de inzet op preventie. Desondanks kampt de hele justitieketen nog altijd met grote tekorten. Veel aangiftes blijven onbeantwoord, veel vacatures blijven onvervuld, het OM heeft veel zaken die op de plank blijven liggen en rechtbanken kampen met grote achterstanden[19].

De vraag rijst daarnaast of alle overheidsinvesteringen voldoende (hebben) bijgedragen aan het tegengaan van criminaliteit.

Ook het bedrijfsleven investeert veel, met name in het tegengaan van criminaliteit. Exacte cijfers hierover ontbreken maar de voorbeelden zijn eindeloos: beveiligingspoortjes, alarmsystemen, hekken, trainingen, computernetwerkbeveiligingssystemen, beveiligers, speurhonden, data-analisten, noem maar op.

Via allerlei ministeries en potjes wordt geïnvesteerd in het tegengaan van criminaliteit, maar er is geen overkoepelende, alles overziende, stevige regisseur. Hierdoor wordt onvoldoende rendement gehaald uit gedane investeringen van zowel de overheid als het bedrijfsleven. Een overzicht van alle lopende pilots ontbreekt, net zoals van reeds beproefde pilots. Hierdoor wordt onvoldoende geleerd van eerdere trajecten[20]. Dagelijks bevragen verschillende overheidsorganisaties van alles aan ondernemers, zonder dat van elkaar te weten. Dit zorgt voor spanning in de publiek-private samenwerking. De overheid zou bedrijven ook meer kunnen ondersteunen. Zoals de al eerder genoemde behoefte aan meer wettelijke mogelijkheden om informatie te delen en te ontvangen, en de mogelijkheid om van alle strafbare feiten digitaal aangifte te doen dan wel melding te maken.

Als overheid en bedrijfsleven meer samen optrekken tegen criminelen en criminele activiteiten en meer in elkaars verlengde werken, kan vaak meer worden bereikt. Zo'n gezamenlijk publiek-privaat front vraagt om stevige regie vanuit de overheid.

[17] Bekostiging van politie, OM en rechtspraak onderzocht | Nieuwsbericht | WODC - Wetenschappelijk Onderzoek- en Documentatiecentrum
[18] Voor het versterken van de justitiële keten is door Rutte IV tot en met 2031 jaarlijks 200 miljoen euro beschikbaar gesteld, en structureel 150 miljoen euro. Dit komt bovenop de reguliere begroting
[19] blg-1099779.pdf (officielebekendmakingen.nl) Eindrapport parlementaire verkenningen: prestaties in de strafrechtketen
[20] Zie ook rapport "Koers bepalen; over de lessen van de versterking aanpak georganiseerde drugscriminaliteit"; nov 2022 Koers bepalen (wodc.nl)

3.2 Het bedrijfsleven

De overheid moet regie nemen en ondernemers ondersteunen. Maar het bedrijfsleven moet ook zelf aan de bak met een heldere boodschap en een gezamenlijke vuist. Dit is cruciaal om diefstal, criminele inmenging, agressie, (digitale) afpersing en witwassen tegen te gaan. Ondernemers laten zo zien dat ze hun verantwoordelijkheid nemen als het om preventie gaat, tonen zich saamhorig met de overheid in de strijd tegen criminaliteit, geven gehoor aan de oproep om op te staan tegen ondermijning[21]en laten criminelen zien dat ze zich gewapend hebben.

Een goed voorbeeld hiervan komt uit Italië, waar de inmenging en het geweld van de maffia dagelijkse praktijk is. Het bedrijfsleven heeft zich verenigd en als collectief hiertegen geageerd. Er is een anti-maffia dag, bedrijven tonen met stickers dat zij geen *pizzo* (beschermgeld) betalen en er zijn anti-maffiatrainingen. Publiekelijk de afkeer van criminaliteit tonen is zinvol en, zo leert de Italiaanse praktijk, effectief.

Er lijkt in Nederland soms nog schroom om extern te communiceren over het risico op criminaliteit in een sector en hoe hiermee om te gaan. Soms vanwege het imago bij potentiële sollicitanten of klanten. Vaak ook uit schaamte. Veel criminaliteit blijft onbesproken, onaangepakt en er wordt niet tegen geageerd. Dit terwijl het bedrijfsleven hier steeds meer last van heeft en veel schade door lijdt. Dat geldt voor het individuele bedrijf, maar ook voor de reputatie van (ondernemend) Nederland in zijn geheel. Die schroom zou afgeschud moeten worden. Ondermijning, een cyberaanval of digitale fraude kan iedereen overkomen. Andere ondernemers kunnen lering trekken uit de ervaringsverhalen. En de overheid is gebaat bij inzicht in aard en omvang.

Bedrijven moeten dus de vlucht naar voren nemen. Ze moeten laten zien dat zij als werkgever niet bang zijn en hun medewerkers hulpmiddelen geven om het werk veilig te kunnen doen. Zoals de weerbaarheidstrainingen die sommige brancheorganisaties organiseren voor het personeel van hun leden. Bijvoorbeeld door te communiceren dat crimineel geld niet welkom is.

Het bedrijfsleven moet zich gezamenlijk en openlijk uitspreken tegen criminaliteit. VNO-NCW en MKB-Nederland willen een project starten om ondernemers bewust te maken van de noodzaak hiervan. Onderdeel van het project is het ontwikkelen van communicatiemiddelen die ondernemers kunnen gebruiken. Branches kunnen, samen de Platforms Veilig Ondernemen, trainingen organiseren.

3.3 Het brede publiek

Tot slot is ook bij de burger meer waakzaamheid nodig. Het brede publiek kan bijdragen aan het vormen van één front tegen criminaliteit. Het vermoeden van strafbare feiten moet niet onbesproken blijven, agressie en geweld moeten niet gewoon worden. Let beter op bij het doen van een online transactie, ben je er meer van bewust dat je eigen handelen ook bij kan dragen aan de criminaliteit en onveiligheid in Nederland. Deze boodschappen zouden breed verspreid moeten worden. Uiteindelijk worden de kosten van winkelcriminaliteit, verzekeringsfraude en ladingdiefstal verrekend in de prijzen van goederen. Daar betalen we dus allemaal voor.

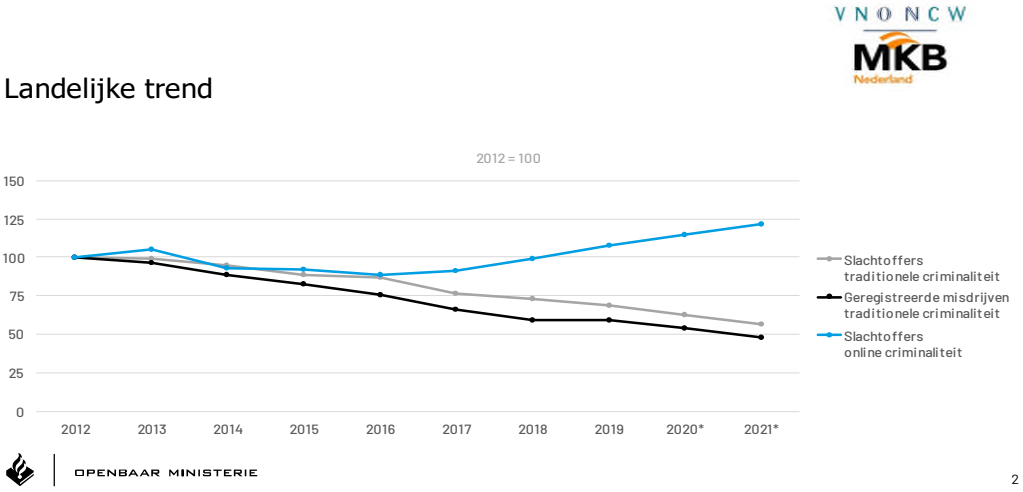
Het brede publiek moet zich bewuster worden van de risico's van criminaliteit en hoe hun eigen handelen hier invloed op heeft.

[21] OM-topman: 'Ik mis de verontwaardiging over criminaliteit die het bedrijfsleven ondermijnt' (fd.nl)

4 Inzet op digitale criminaliteit

- Investeer in digitale beveiliging.

Het aantal overvallen, straatroven en inbraken daalt al jaren. Dat is goed nieuws. Helaas komt er wel iets anders voor in de plaats. Het aantal online fraudes (factuurfraude, aan-en verkoopfraude, BEC fraude[22]) stijgt enorm. Ransomware (het 'gijzelen' van gegevens op computers) is inmiddels een ware plaag binnen het bedrijfsleven. De coronapandemie waarin veel mensen thuiswerkten, heeft deze ontwikkeling versneld. De verwachting is dat de trend zich de komende jaren verder zal doorzetten en steeds geraffineerder wordt.



Eén op de vijf mkb-ondernemers krijgt jaarlijks te maken met een cyberincident met de bijbehorende financiële schade. Het merendeel daarvan betreft ransomware. Het is daarom essentieel dat bedrijven én de overheid inspelen op deze ontwikkelingen en investeren in kennis, digitale beveiliging, awareness en mankracht om digitale- en cybercriminaliteit het hoofd te bieden.

Criminelen kunnen nu nog vrij eenvoudig zorgen voor een digitale hartstilstand (het hele bedrijf ligt plat) of gevoelige bedrijfsgegevens bemachtigen en vervolgens de ondernemer en of de klanten hiermee afpersen. Fysiek hang- en sluitwerk is voor iedereen de normaalste zaak van de wereld. Niemand zet zijn fiets weg zonder slot(en) of laat zijn voordeur open staan. Voor de digitale infrastructuur moet beveiliging (digitaal hang- en sluitwerk) net zo normaal zijn. Fraudepreventie en cyberweerbaarheid moet bij iedere ondernemer op de agenda en als kostenpost op de begroting staan.
Er zijn al de nodige initiatieven. Het Digital Trust Center (DTC23) ontwikkelt eenvoudige tools voor ondernemers. Bij VNO-NCW en MKB-Nederland aangesloten brancheorganisaties en hun leden kunnen kosteloos het cyberweerbaarheidsprogramma Samen Digitaal Veilig volgen24. De Platforms Veilig Ondernemen organiseren awareness-bijeenkomsten.

[22] Je halve omzet kwijt aan oplichters. Dit is BEC-fraude
[23] Digital Trust Center
[24] Samen Digitaal Veilig

Ook de overheid moet hierin een been bijtrekken. De informatieverstrekking aan bedrijven over dreiging(en) is nog niet goed en niet snel genoeg. De opsporing en de verdere justitieketen moeten ingericht worden op deze digitale ontwikkeling. Personeel moet opgeleid worden. De overheid kan ook meer doen om bedrijven en consumenten/burgers voor te lichten.

Digitale en cybercriminaliteit stijgt zorgwekkend. Ondernemers moeten meer doen aan fraudepreventie en weerbaarheid en investeren in digitale veiligheid. Ook de overheid is nog onvoldoende toegerust op deze ontwikkeling.

Colofon

Deze brochure is een uitgave van VNO-NCW en MKB-Nederland
November 2023

Voor meer informatie:
Karijn van Doorne, strategisch beleidsadviseur
doorne@vnoncw-mkb.nl.

Foto omslag:
Pixabay, joshgmit

Contact:
VNO-NCW en MKB-Nederland
Postbus 93002,
2509 AA Den Haag
070-3490909

VNO NCW

MKB Nederland