Innovatie in de opsporing

Maatschappelijke en technologische ontwikkelingen stellen politie en OM continue voor nieuwe uitdagingen. Om toekomstbestendig te worden en te blijven is het aan de organisaties om samen deze uitdagingen aan te gaan en hierop zowel een visie als concrete acties te organiseren. Een integrale aanpak is cruciaal, maar kent ook uitdagingen. Deze notitie gaat nader in op de innovatie van de opsporing en gaat in op de bestrijding van cybercrime.

Politie en OM zijn gezamenlijk het programma Toekomstbestendig Opsporen en Vervolgen (TOV) gestart vanuit het gedeelde besef dat een aantal maatschappelijke- en technologische ontwikkelingen grote invloed heeft op de vakinhoudelijke- en organisatievraagstukken van de politie en OM. Vanuit het TOV geven politie en OM richting aan deze transitie van de opsporing en vervolging.

Een van de belangrijke thema´s binnen het programma om mee te experimenteren en richting aan te geven is publiek private samenwerking (PPS). Bedrijven onderzoeken steeds vaker zelf, parallel, voorafgaand of opvolgend op opsporing en vervolging door politie en OM. Echter blijft de gegevensuitwisseling een uitdaging met private partijen. Hierover is het wetsvoorstel gegevensverwerking samenwerkingsverbanden (Wgs) dat nu ter behandeling bij de Tweede Kamer ligt. Duidelijkheid hierover is in het belang van de opsporing en vervolging.

Een daaraan gelieerd thema binnen het TOV is burgeropsporing. Geïnteresseerde en betrokken burgers onderzoeken steeds vaker zelf strafbare feiten waar zij slachtoffer van zijn of die in de media worden gemeld. Dat kan parallel, voorafgaand of opvolgend op opsporing door de politie gebeuren. De bijdrage van burgers kan een waardevolle aanvulling zijn op het onderzoek van de politie, maar kan dat onderzoek ook onbedoeld negatief beïnvloeden. Politie en OM stellen zich met het experimenteren met burgeropsporing open voor nieuwe modaliteiten en sturing om het maatschappelijk effect van hun handelen te vergroten. Dat is een ontdekkingstocht, die juridisch-ethische vragen oproept, waarover het debat in een brede context worden gevoerd. Bijvoorbeeld over de afbakening van het handelingsperspectief van private partijen bij het aanpakken van maatschappelijke veiligheidsproblemen. Onderzoek door burgers is immers niet door dezelfde wettelijke en beleidskaders afgebakend als het optreden van politie en OM. Er moet dan ook goed voor gewaakt worden dat de legitimiteit van handelen is geborgd en het geweldsmonopolie van de Staat gewaarborgd blijft.

Cybercrime is een actueel voorbeeld van een concrete criminaliteitsvorm onderhevig aan maatschappelijke en technologische ontwikkelingen. De computer en het internet zijn niet meer weg te denken uit onze samenleving. Technologie ontwikkelt zich in sneltreinvaart en heeft een steeds grotere impact op ons leven. Nieuwe technologie is echter niet altijd veilig. Dezelfde technologie die ons leven verrijkt, wordt ook door criminelen gebruikt en zal bovendien altijd kwetsbaarheden bevatten waar criminelen misbruik van kunnen maken. Daardoor ontstaan nieuwe delicten en nieuwe modi operandi, waarbij computers zowel middel als doelwit kunnen zijn en landsgrenzen vervagen. In de afgelopen jaren is sprake van een explosieve toename van cybercrime en gedigitaliseerde criminaliteit. Deze toename heeft niet alleen een toenemende impact op het leven van slachtoffers, maar

zorgt ook voor steeds hogere financiële en maatschappelijke kosten. De ramingen lopen uiteen, maar de schade bedraagt jaarlijks tenminste vele miljarden euro's. Om deze trend te keren, staan politie, OM en hun samenwerkingspartners voor de kritieke opgave om te komen tot een toekomstbestendige integrale en innovatieve aanpak. In die aanpak staat het effect van het optreden altijd centraal en wordt de klassieke strafrechtelijk aanpak verrijkt met de publiek-private bestrijding van cybercrime. De capaciteit van het OM blijft echter achter bij de politie.[1]

Met de bestrijding van cybercrime wordt de digitale veiligheid vergroot, worden criminele activiteiten en netwerken verstoord en de gevolgen ervan aangepakt, wordt strafbaar gedrag voorkomen, worden criminele winsten afgepakt en wordt opgetreden tegen oorzaken en ondersteuners van strafbaar gedrag. Door samen te werken in een netwerk van publieke en private stakeholders kan het maatschappelijk effect worden gemaximaliseerd, waarbij politie en OM handelen met een neus voor kansen en een oog op rechten en belangen.

Conform de afspraken in de Veiligheidsagenda is naast de reguliere opsporingsonderzoeken in 2019 door de politie en het OM gestart met de aanpak van eenheidsoverstijgende (vaak internationale) fenomenen, zoals ransomware, tech support scams en business email compromise. Het zijn deze fenomenen die de bulk uitmaken van de cybercriminele activiteiten in Nederland. De modus operandi erachter kenmerkt zich door een gecoördineerde samenwerking tussen verschillende criminele partijen en bewuste en onbewuste ondersteuning door legale en illegale dienstverleners. Kennis van de businessmodellen achter criminele fenomenen is de eerste stap in de bestrijding ervan. Vanuit die kennis kunnen barrièremodellen worden ontwikkeld, waarin samenwerkende publieke en private partners elk een rol hebben bij het verstoren van het criminele businessmodel.

Rondom de meest voorkomende fenomenen wordt een aanpak ontwikkeld, waarbij publiek-private samenwerking en innovatie een belangrijke rol spelen. Iedere regio(nale eenheid) heeft een geprioriteerd fenomeen geadopteerd en ontwikkeld daarvoor een integrale, multidisciplinaire aanpak. De opgedane kennis en inzichten worden neergelegd in een zogenaamd book of crime. Een book of crime is niet een echt boek, maar een proces. Het is een methode om samen met onze partners het criminele proces achter veel voorkomende fenomenen inzichtelijk te maken en effectieve interventies op te werpen om dit proces te verstoren. De opgedane kennis wordt vastgelegd in kennisproducten, die worden verspreid binnen politie en OM, en worden gedeeld met onze partners. Een book of crime is in principe nooit af, maar is een cyclisch proces. Waar criminele businessmodellen zich over tijd ontwikkelen, zal de book of crime methode moeten meebewegen.

Om in de integrale samenwerking als betrouwbare, slagvaardige en standvastige overheid nu en in de toekomst te kunnen blijven opereren, is het essentieel dat de kennis en capaciteit binnen de héle strafrechtsketen wordt versterkt. De specialistische kennis- en vaardigheden op het gebied van cybercrime en gedigitaliseerde criminaliteit van nu vormen de basiskennis van morgen. Om de maatschappelijke en technologische ontwikkelingen het hoofd te bieden is het noodzakelijk dat de basiskennis van politie en OM wordt verstevigt, de kennis van professionals wordt doorontwikkeld en beide organisaties worden versterkt met professionals van buiten het opsporing- en vervolgingsdomein.

---

[1] **Kamerbrief** over voortgang integrale aanpak van cybercrime, 29 juni 2020