

Vergaderjaar 2000–2001

27 834

Criminaliteitsbeheersing

Nr. 3

BRIEF VAN DE MINISTER VAN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 augustus 2001

Tijdens het Algemeen Overleg op 30 augustus 2000 (26 800 VI, nr. 87) en het twee minuten debat op 12 september 2000 over het kabinetsstandpunt Handhaven op niveau (Kamerstukken II, 1999–2000, 26 800-VI, nr. 67) heeft de heer Van der Staaij aandacht gevraagd voor **de handhaving in de elektronische omgeving**. De heer Van der Staaij heeft mij bij die gelegenheid gevraagd te bevestigen dat er wordt gewerkt aan plannen om de handhavingstekorten in dit opzicht weg te nemen. Ik heb daarop toegezegd medio dit jaar met een brief te komen over de handhaving in de elektronische omgeving. Met deze brief kom ik aan die toezegging tegemoet.

Zoals u heeft kunnen zien, heeft het onderwerp cybercrime nadrukkelijk een plaats gekregen in de nota Criminaliteitsbeheersing (Kamerstukken II 2000–2001, 27 834, nrs. 1–2) die u onlangs is aangeboden. In de nota wordt geconcludeerd dat de kwaliteit van de opsporing krachtig versterking behoeft in het licht van de ontwikkelingen op het gebied van de Informatie- en communicatietechniek. De nota Criminaliteitsbeheersing bouwt voort op de uitgangspunten van het Nationaal actieprogramma digitaal rechercheren van de Raad van Hoofdcommissarissen van januari 1998 (u toegezonden als bijlage bij de antwoorden op vragen over de nota Wetgeving voor de elektronische snelweg, Kamerstukken II, 1998–1999, 25 880, nr. 3). Als uitgangspunt voor de handhaving in de elektronische omgeving geldt dat de rechtbescherming van de burger in een «on line» situatie gelijkwaardig dient te zijn aan de «off line» situatie (zie ook notitie Internationalisering en rechtsmacht, Kamerstukken II, 1999–2000, 25 880, nr. 10).

Criminaliteitsbeheersing begint bij preventie, zo stelt de nota Criminaliteitsbeheersing. Preventie poogt aan te grijpen bij de oorzaken van criminaliteit. Als we kijken naar criminaliteit gerelateerd aan de elektronische omgeving dan kunnen twee belangrijke oorzaken worden onderscheiden voor het ontstaan van die criminaliteit.

In de eerste plaats biedt de elektronische omgeving gelegenheidsstructuren om criminaliteit te plegen. Denk bijvoorbeeld aan de onveiligheid van bepaalde betaalmiddelen (credit cards) in een elektronische omgeving of het constant online zijn van computers (internetten via de kabel). In de nota Criminaliteitsbeheersing worden diverse voorbeelden gegeven hoe de gelegenheid tot criminaliteit in een elektronische omgeving kan worden beperkt.

In de tweede plaats heeft de gebruiker onvoldoende kennis over de veiligheidsrisico's die in de elektronische omgeving spelen en over de maatregelen die genomen kunnen worden om die risico's te beheersen. De positie van de eindgebruiker dient derhalve versterkt te worden («empowerment»). In de nota Criminaliteitsbeheersing worden in dit verband voorbeelden gegeven van voorlichting en het streven om met de private sector een kader te scheppen voor alternatieve geschillenbeslechting (zie notitie Internationalisering en rechtsmacht, Kamerstukken II, 1999–2000, 25 880, nr. 10). Gewezen kan ook worden op de beleidsnota Kwetsbaarheid op Internet van de ministeries van Verkeer en Waterstaat en Economische Zaken. Hierin worden naast voorlichting ook de ontwikkeling van informatiebeveiligingsmethoden hulpmiddelen en de inrichting van een Trusted Third Party structuur genoemd als initiatieven die eraan bijdragen dat de positie van de eindgebruiker wordt versterkt.

Als sluitstuk van de preventie van criminaliteit dient er in de elektronische omgeving een geloofwaardige strafrechtelijke handhaving te zijn. De nota Criminaliteitsbeheersing signaleert dat politie en justitie een inhaalslag moeten maken, willen ze de aansluiting met de ontwikkelingen op het gebied van de informatie- en communicatietechniek niet missen. De actiepunten die in de nota Criminaliteitsbeheersing worden genoemd zijn: het vergroten van de kennis van digitaal opsporen, het ontwikkelen van digitale opsporingsmiddelen, indien nodig het uitbreiden van opsporingsbevoegdheden, aanzienlijke uitbreiding van de capaciteit bij de bureaus digitale expertise en aanpassingen in het personeelsbeleid gezien de concurrentie op de personeelsmarkt voor gekwalificeerd IT-personeel.

Per 1 juli jongstleden is onder verantwoordelijkheid van de Raad van Hoofdcommissarissen gestart met de uitvoering van het Nationaal actieprogramma digitaal rechercheren. De ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Justitie hebben hiervoor een startsubsidie beschikbaar gesteld van in totaal 2 miljoen gulden voor de periode 1 juli 2001 tot 1 juli 2002. De regiokorpsen hebben daar een bedrag van 900 000 gulden aan toegevoegd, zodat in totaal bijna 3 miljoen gulden beschikbaar is voor het eerste jaar. Daarmee kunnen in eerste instantie de grootste knelpunten op het terrein van opleiding en de ontwikkeling en aanschaf van opsporingsmiddelen worden aangepakt. Om het totale pakket aan actiepunten uit het Nationaal actieprogramma te kunnen realiseren wordt in de nota Criminaliteitsbeheersing een bedrag van ongeveer 65 miljoen gulden gevraagd. Naast opleidingen en de ontwikkeling en aanschaf van opsporingsmiddelen gaat het dan om activiteiten in het kader van implementatie van het kennislagen model (inclusief uitbreiding capaciteit van de Bureau's Digitale Expertise), wet- en regelgeving, bescherming kritieke infrastructuren en (inter)nationale samenwerking.

In het kader van de handhaving van de ordeningswetgeving is de aandacht voor de pro-actieve surveillance op het Internet in het Nationaal actieprogramma digitaal rechercheren van belang. In het kader van een dergelijke surveillance wordt gericht gezocht naar strafbare handelingen op het Internet. Geconstateerde strafbare feiten moeten vervolgens uitmonden in concrete opsporingsonderzoeken. Op dit moment is de capaciteit voor een dergelijke surveillance beperkt. Het verspreiden van

kinderpornografie via het Internet is een vast aandachtspunt voor de pro-actieve surveillance. Daarnaast is er ruimte voor nog één aandachtsgebied. In het verleden is onder andere aandacht geweest voor het organiseren van rellen rond voetbalwedstrijden (met name in het kader van Euro 2000). Thans wordt een aanpak ontwikkeld waarbij wordt gekeken naar het gebruik van Internet voor de affichering van drugs. Met de uitbreiding van de capaciteit voor digitaal rechercheren is het de bedoeling dat in het kader van de pro-actieve Internet surveillance 4 tot 5 onderwerpen tegelijkertijd opgepakt kunnen worden. Denk daarbij bijvoorbeeld aan onderzoek naar credit card fraude, het aanbieden van valse (identiteits)documenten, illegaal gokken en het te koop aanbieden van medicijnen.

Terug naar de vraag die is gesteld: er wordt momenteel door alle partijen hard gewerkt om het handhavingstekort in de elektronische omgeving weg te nemen. De komende drie tot vier jaar zullen in het teken staan van de noodzakelijk te maken inhaalslag met als doel het bevorderen van een meer veilige digitale informatiemaatschappij en het verminderen van ICT gerelateerde criminaliteit.

De Minister van Justitie,
A. H. Korthals