Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
24 april 2026

Onze referentie
7478923

nota

Beslisnota Beleidsreactie evaluatie wet CCIII

1. Aanleiding

Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) heeft eind 2025 zijn rapport over de evaluatie van de Wet Computercriminaliteit III (Wet CCIII) opgeleverd. Dit rapport is door uw voorganger op 13 januari jl. aan de Kamer aangeboden. Daarbij is aangegeven dat het rapport omvangrijk is en dat het opstellen en afstemmen van de beleidsreactie tijd vergt. De beleidsreactie zou zo spoedig mogelijk aangeboden worden. Deze beleidsreactie ligt nu voor.

2. Geadviseerd besluit

Instemmen met de bijgevoegde beleidsreactie en verzending daarvan aan de Tweede Kamer.

3. Kernpunten

Opzet evaluatie

- Het WODC onderzocht in hoeverre de doelstellingen van de Wet CCIII in de praktijk zijn gerealiseerd. De directe aanleiding van het onderzoek was een wettelijke verplichting om deze wet vijf jaar na inwerkingtreding te evalueren.
- Met de Wet CCIII is het juridisch instrumentarium ten aanzien van de bestrijding van criminaliteit in het digitale domein versterkt. Er zijn vijf nieuwe of aangepaste strafbaarstellingen in het Wetboek van Strafrecht en twee nieuwe bevoegdheden in het Wetboek van Strafvordering opgenomen.
- Bij de strafbaarstellingen ging het om het stelen van gegevens (art. 138c Sr), het helen van gegevens (art. 139g Sr), online handelsfraude (art. 326e Sr), verleiding van een minderjarige (art. 248a Sr) en grooming (art. 248e Sr). De twee nieuwe bevoegdheden zien op de ontoegankelijkmaking van gegevens (art. 125p Sv) en het op afstand binnendringen in een geautomatiseerd werk (de “hackbevoegdheid” (art. 126nba, 126uba en 126zpa Sv)).
- De hackbevoegdheid is al eerder geëvalueerd. Uw ambtsvoorganger heeft op 7 december 2023 haar beleidsreactie daarop gegeven. Dit nieuwe WODC-rapport ziet niet alleen op de hackbevoegdheid, maar op de gehele wet en hoe deze uitpakt in de praktijk.

Evaluatie algemeen

In zijn algemeenheid hebben de geëvalueerde bepalingen en bevoegdheden hun waarde in de praktijk bewezen. Van belang is dat de nieuwe artikelen intussen onderwerp zijn geweest van rechterlijke toetsing, waardoor de reikwijdte en toepassing in de praktijk nader zijn verduidelijkt. In de evaluatie zijn vier aspecten naar voren gekomen die meerdere wettelijke bepalingen uit de Wet CCIII raken:

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Datum
24 april 2026

Onze referentie
7478923

1. Nieuwe ontwikkelingen. Bijvoorbeeld de gevolgen van een toename van de illegale handel in (persoons-)gegevens en het aantal slachtoffers daarvan. Het kabinet zal hiervoor aandacht houden en dit ook meenemen bij de uitwerking van de verhoging van de strafmaxima voor ernstige cyberdelicten zoals aangekondigd in het coalitieakkoord.
2. Beschikbare capaciteit. Capaciteitsoverwegingen spelen mee bij de inzet van bevoegdheden. Oplossingen hiervoor zijn niet eenvoudig, er zullen binnen opsporingsonderzoeken altijd keuzes gemaakt moeten worden welke (combinatie van) inzet van bevoegdheden passend is.
3. Zaken met een internationale component. Daarbij zijn vaak tijdrovende rechtshulpverzoeken nodig. Het kabinet zet actief in op verbeterde samenwerking met en binnen Europol. Daarnaast kan de implementatie van de Europese E-evidence verordening de grensoverschrijdende samenwerking versnellen.
4. (Rechtsstatelijke) Waarborgen bij de inzet van bijzondere opsporingsbevoegdheden. Het WODC beschrijft dat er spanning bestaat tussen de inzet van bijzondere opsporingsbevoegdheden en grondrechten. Om die reden zijn de bevoegdheden met meerdere rechtsstatelijke waarborgen omkleed. Uit de evaluatie blijkt dat deze waarborgen soms het opsporingsbelang (onnodig) in de weg kunnen zitten.

Kernpunten evaluatie per onderwerp

- Het stelen en helen van gegevens is in de beleidsreactie samengenomen. Deze bepalingen hebben hun waarde in de praktijk bewezen. Er konden verdachten worden vervolgd in zaken waar dat voorheen minder goed mogelijk was. Ook zijn er andere voordelen behaald, zoals de mogelijkheid voor slachtoffers om zich te voegen in het strafgeding. Het kabinet onderschrijft de conclusie in het rapport dat de huidige strafmaxima voor deze delicten niet in verhouding staan tot de ernst, schaal en maatschappelijke impact. In het coalitieakkoord is aangekondigd dat de strafmaxima voor zware cyberdelicten zullen worden verhoogd. Bij de nadere beleidsuitwerking hiervan zal ook aandacht worden besteed aan recente incidenten zoals hacks bij Odido en Clinical Diagnostics. Ook de richtlijn strafvordering voor cybercrime en gedigitaliseerde criminaliteit van het OM wordt herzien.
- Online handelsfraude: het rapport concludeert dat de nieuwe strafbaarstelling vervolging en bewijsvoering eenvoudiger heeft gemaakt. Er worden twee aandachtspunten genoemd die al bij de algemene punten zijn toegelicht: capaciteit en zaken met een internationale component. Dit laatste is een belangrijk punt voor het kabinet. In Europees verband wordt per medio 2029 geregeld dat identificerende gegevens van bankrekeninghouders door bevoegde autoriteiten grensoverschrijdend kunnen worden opgevraagd via het koppelingssysteem voor registers van bankrekeningen (bank account registers interconnection system — BARIS). Specifiek voor online handelsfraude wordt nog geconstateerd dat in de praktijk vaak geen grootschaligheid (een dader met veel slachtoffers) is vastgesteld. De redenen hiervoor zijn onduidelijk gebleven. Het kabinet is van oordeel dat deze grootschaligheid om uiteenlopende redenen buiten beeld blijft. Binnen de integrale aanpak online fraude dragen publieke en private partners bij aan de samenwerking met webshops en platforms om online aan- en verkoopfraude op een effectieve en efficiënte manier te bestrijden.
- Ook de punten ten aanzien van verleiding van een minderjarige en grooming zijn samengenomen. Het betreft de inzet van de “lokpuber”. De evaluatie bevestigt dat de inzet van de lokpuber een effectief middel kan zijn in de bestrijding van

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Datum
24 april 2026

Onze referentie
7478923

seksueel kindermisbruik. Er zijn verschillende voorbeelden van zaken waarin een lokpuber is ingezet en het tot een veroordeling is gekomen. Lokmiddelen zijn echter wel zware opsporingsmiddelen. Vanuit proportionaliteit en subsidiariteit zet de politie ze terughoudend in. Het evaluatierapport concludeert dat de bevoegdheid in de praktijk beperkt ingezet wordt. Genoemde oorzaken zijn de capaciteit, het aantal "brengzaken" (waar bij de aangifte al bewijs wordt aangeleverd) waardoor de inzet van een lokpuber niet meer noodzakelijk is, en de grens met uitlokking. Op dit laatste punt zal nadere jurisprudentie nodig zijn.

- Ten aanzien van het ontoegankelijk maken van gegevens wordt geconstateerd dat de bevoegdheid slechts beperkt wordt ingezet. Het artikel voldoet niet altijd voor de opsporingspraktijk; het proces van afgifte van een machtiging van de rechter-commissaris en het horen van de aanbieder vooraf nemen veel tijd in beslag. Het kabinet zal bezien of het mogelijk en wenselijk is om toepassing van deze bevoegdheid te vereenvoudigen zonder afbreuk te doen aan de rechtsstatelijke waarborgen. Het zoeken naar de juiste balans is noodzakelijk.
- Tot slot de hackbevoegdheid. De evaluatie laat zien dat de hackbevoegdheid een waardevolle bevoegdheid is voor de politie.[1] In 60% van de gevallen wordt sturingsinformatie of bewijs verkregen. Een aandachtspunt is de arbeidsintensiviteit van de procedures die gelden voor de inzet van deze bevoegdheid. Deze procedures zijn van belang vanwege de ingrijpendheid van de bevoegdheid. Verder vraagt het WODC aandacht voor de toetsing van de ingezette technische hulpmiddelen door de zittingsrechter, de keuring daarvan, en de betekenis hiervan voor het bewijs. Het WODC vraagt zich af of die toetsing in de praktijk wel plaatsvindt, bij gebrek aan weergave daarvan in vonnissen. De inzet van een technisch hulpmiddel staat altijd in het proces-verbaal. De rechter kan op basis daarvan, of na bespreking ter zitting, een oordeel vellen. Het niet weergeven daarvan in het vonnis betekent niet dat er geen aandacht aan is geschonken door de rechter.

4. Toelichting

4.1. Politieke context

Bij de individuele punten zijn de meest opvallende (politieke) punten al benoemd. Dit betreft met name:

- Strafmaximum voor stelen en hele van gegevens. In het coalitieakkoord is aangekondigd dat de strafmaxima bij zware cyberdelicten zullen worden verhoogd. Bij de beleidsuitwerking zal aandacht worden besteed aan incidenten als de hacks bij Odido en Clinical Diagnostics.
- Schaarse opsporingscapaciteit die aanleiding kan zijn om strafbaarstellingen en opsporingsbevoegdheden slechts beperkt te benutten. In de opsporing moeten altijd keuzes worden gemaakt. Daarbij spelen onder meer alternatieven een rol, die ertoe kunnen leiden dat andere strafbaarstellingen of bevoegdheden worden ingezet.
- Het zoeken naar de juiste balans tussen het opsporingsbelang en de rechtsstatelijke waarborgen. Het kabinet gaat bezien of het mogelijk en wenselijk is om het proces rond ontoegankelijkmaking van gegevens te vereenvoudigen zonder afbreuk te doen aan de waarborgen.

5. Informatie die niet openbaar gemaakt kan worden

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.

[1] En in voorkomende gevallen voor andere opsporingsdiensten zoals KMar, FIOD en BOD'en.