



Meer mogelijkheden voor opsporing en vervolging computercriminaliteit Wet computercriminaliteit III kent echter ook aantal aandachtspunten

In maart 2019 is de **Wet computercriminaliteit III** (CCIII) in werking getreden. Het doel van deze wet is om de politie en het Openbaar Ministerie meer mogelijkheden te bieden om computercriminaliteit en andere vormen van ernstige criminaliteit op te sporen en te vervolgen. De nieuwe strafbaarstellingen en de nieuwe bijzondere opsporingsbevoegdheden zijn vastgelegd in **nieuwe of aangepaste wettelijke bepalingen** in het Wetboek van Strafrecht en in het Wetboek van Strafvordering.

Om te kijken hoe de wet in haar eerste vijf jaar benut wordt in de opsporingspraktijk heeft het ministerie van Justitie en Veiligheid het WODC gevraagd de Wet CCIII te evalueren. De resultaten van deze evaluatie zijn hieronder weergegeven.

Van het stelen van digitale gegevens tot aan de hackbevoegdheid De nieuwe strafbaarstellingen en bijzondere opsporingsbevoegdheden op een rijtje

Voor invoering CCIII	Na invoering CCIII	Bijzonderheden
Verdachten van het stelen en helen van gegevens konden niet goed worden vervolgd.	Het stelen en helen van digitale gegevens —zoals persoonsgegevens, foto's en afbeeldingen—is strafbaar (artikel 138c en 139g Sr).	
Online handelsfraude werd onder andere wetsartikelen vervolgd, zoals oplichting (artikel 326 Sr).	Het plegen van online handelsfraude —zoals via marktplaats.nl goederen verkopen of diensten aanbieden, maar niet leveren na betaling—is strafbaar (artikel 326e Sr).	
Vervolging van verleiding van een minderjarige en grooming kon alleen plaatsvinden als een 'echte' puber daarvan slachtoffer werd.	Het inzetten van een lokpuber —een politieagent die zich online voordoeft als minderjarige— is toegestaan bij de opsporing van verleiding van een minderjarige en grooming (artikelen 248a/e Sr). Sinds juli 2024 is de inzet van lokpuber opgenomen in de Wet seksuele misdrijven.	
Digitale gegevens met strafbare inhoud konden niet altijd ontoegankelijk gemaakt worden.	Aanbieders van strafbare digitale gegevens —zoals kinderpornografie of illegale verkoopsites—kunnen met een bevel van de officier van justitie gedwongen worden deze te verwijderen (artikel 125p Sv).	
De politie mocht geen apparaten van verdachten hacken.	De politie mag onder voorwaarden apparaten van verdachten hacken —zoals telefoons en servers (artikel 126nba, 126uba en 126zpa Sv).	

Nieuwe ontwikkelingen vragen om actie

Beperktere inzet door beschikbare capaciteit opsporingsinstanties

Internationale component bemoeilijkt uitvoering

Spanning tussen uitvoering en (rechtsstatelijke) waarborgen

Nieuwe mogelijkheden Wet CCIII worden echt ingezet in opsporingspraktijk Wel aandacht nodig voor rechtsstatelijke waarborgen bij inzet bijzondere opsporingsbevoegdheden

Wat de wetgever met de Wet CCIII beoogde is **gelukt**: het pakket aan mogelijkheden om computercriminaliteit en andere vormen van ernstige criminaliteit op te sporen en te vervolgen is versterkt. Denk bijvoorbeeld aan het helen van digitale gegevens en online handelsfraude.

Toch zijn er **aandachtspunten** rondom de toepassing van de wet in de praktijk. De nieuwe opsporingsbevoegdheden zijn bijvoorbeeld **ingrijpende** bevoegdheden. Daarom is het van belang dat **stevige toetsingsvoorwaarden** blijven bestaan. Wel zou voor de ontoegankelijkmaking van digitale gegevens gekeken kunnen worden of er meer variatie kan komen wat betreft toetsing door de rechter-commissaris. Voor de hackbevoegdheid worden sommige voorwaarden al anders ingericht. Een aandachtspunt daarbij is dat een zittingsrechter lang niet altijd het verzamelde bewijs met de hackbevoegdheid toetst. Daardoor wordt niet altijd recht gedaan aan een **rechtsstatelijke waarborg** die verondersteld wordt aanwezig te zijn.

Bron. Evaluatie Wet computercriminaliteit III — Een empirisch onderzoek naar de toepassing in de praktijk (Van Uden, Nijhuis & Van der Meer, 2025). WODC, Cahier 2025-10.