Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

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

Onze referentie
8120201

Datum 20 november 2026
Betreft Invoeringstoets doxing

Met deze brief informeer ik uw Kamer over de invoeringstoets naar aanleiding van de wet strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden (Stb. 2023, 274). Met de invoeringstoets zijn de werking van de wet in de praktijk en de gevolgen daarvan voor de bij de uitvoering betrokken organisaties in kaart gebracht. Doel hiervan was te bezien of bij de totstandkoming van het wetsvoorstel gehanteerde aannames over de uitvoerings- en financiële consequenties van de wet zich inderdaad hebben gemanifesteerd.[1]

De invoeringstoets is door mijn ministerie in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) verricht. Voor de invoeringstoets is gesproken met de organisaties die zijn betrokken bij de uitvoering van deze wet, waaronder de politie en het Openbaar Ministerie (OM). De eerste ervaringen van deze organisaties met deze wet zijn positief. De wet voorziet in een duidelijke behoefte voor de praktijk. Uit de invoeringstoets zijn daarnaast enkele aandachtspunten naar voren gekomen, die in deze brief nader worden toegelicht.

In het kader van deze invoeringstoets is ook gekeken naar enkele onderwerpen die in het kader van het wetgevingstraject aan de orde zijn gekomen, namelijk de gevolgen van deze wet voor journalisten,[2] het oogmerkvereiste[3] en de uitvoeringslasten voor de politie en het OM.[4] Daarnaast is de strafbaarstelling van doxing in relatie tot doxing van politieambtenaren onderzocht, zoals is toegezegd tijdens het mondelinge vragenuur op 18 juni 2024.[5] In het vervolg van deze brief wordt eerst een korte algemene toelichting op doxing en de invoeringstoets gegeven. Vervolgens worden de resultaten van de invoeringstoets besproken. Daarbij wordt achtereenvolgens ingegaan op het aangifte- en hulpproces, het bewijs, het verwijderen van persoonsgegevens buiten een strafrechtelijke context, de rol van de Autoriteit Persoonsgegevens (AP), doxing van politieambtenaren, aangifte van doxing tegen journalisten, en de uitvoeringslasten.

Doxing
Het gebruik van persoonsgegevens voor intimiderende doeleinden (hierna: doxing) is sinds 1 januari 2024 strafbaar op grond van artikel 285d van het Wetboek van Strafrecht (Sr). De strafbaarstelling betreft het zich verschaffen, verspreiden of anderszins ter

[1] Kamerstukken II 2021/22, 36171, nr. 3, p. 25.
[2] Kamerstukken II 2021/22, 36171, nr. 3, p. 22.
[3] Handelingen I 2022/23, nr. 42. Item 2.
[4] Eerste Kamer der Staten-Generaal, *Toezegging T03718: Toezegging informeren bij te hoge uitvoeringslasten*, Kamerstukdossier 36.171.
[5] Handelingen II 2023/24, nr. 85, item 2, 18 juni 2024 (toezegging aan het lid Mutluer inzake doxing).

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

Datum
20 november 2026

Onze referentie
8120201

beschikking stellen van persoonsgegevens van een ander of een derde met het oogmerk die ander vrees aan te (laten) jagen, ernstige overlast te (laten) bezorgen of te (laten) hinderen in de uitoefening van zijn ambt of beroep. Doxing kan ingrijpende en schadelijke gevolgen hebben voor het persoonlijke leven van slachtoffers. Met de strafbaarstelling is de duidelijke norm gesteld dat doxing onacceptabel is en is strafrechtelijk optreden hiertegen mogelijk gemaakt. Hiermee werd tegemoet gekomen aan een dringende oproep hiertoe vanuit de praktijk en de politiek.[6]

Invoeringstoets
De invoeringstoets heeft een looptijd gehad van twee jaar en bestond uit verschillende onderdelen: ten eerste zijn periodieke kwalitatieve en kwantitatieve uitvragen gedaan bij de betrokken organisaties (de politie, het OM, de Raad voor de Rechtspraak (hierna: de rechtspraak), Offlimits, Slachtofferhulp Nederland en de AP.[7] Dit deel van de invoeringstoets is door mijn departement uitgevoerd, samen met het CCV. Daarnaast zijn periodiek vragenlijsten gestuurd aan en gesprekken gevoerd met de politie en het OM om relevante inzichten op te halen. Een tweede onderdeel is de analyse die het CCV heeft uitgevoerd op de verzamelde data en de rapportage daarover.

Resultaten invoeringstoets
De reacties van de respondenten over de strafbaarstelling van doxing zijn overwegend positief. In de praktijk is gebleken dat artikel 285d Sr in een behoefte voorziet en goed aansluit bij actuele maatschappelijke ontwikkelingen, in het bijzonder de toename van online grensoverschrijdend gedrag. Door de strafbaarstelling van doxing kan strafrechtelijk worden opgetreden als er (nog) geen sprake is van andere strafbare gedragingen zoals bedreiging of stalking. Hierdoor kan verdere escalatie worden voorkomen. Daarnaast biedt de wet richting voor de uitvoeringspraktijk. Voor de politie is het makkelijker om bijvoorbeeld stopgesprekken te voeren, omdat de politie de verdachte erop kan wijzen dat doxing strafbaar is. Voor organisaties zoals Offlimits is het gemakkelijker om specifieke content te laten verwijderen, omdat platforms wettelijk verplicht zijn om strafbare content offline te halen. Ook is het enkel wijzen op de strafbaarheid van doxing – bijvoorbeeld wanneer een slachtoffer een verdachte aanspreekt op het strafbaar handelen – in sommige gevallen al voldoende gebleken om een einde aan de situatie te maken. Slachtoffers geven aan dat de strafbaarstelling een belangrijke erkenning is van hun slachtofferschap. Zij waarderen het dat er aandacht voor is doxing en dat er daadwerkelijk aangifte van doxing kan worden gedaan. In het kader van de invoeringstoets zijn ook enkele aandachtspunten naar voren gekomen die hierna worden toegelicht.

Aangifte- en hulpproces
Een belangrijk aandachtspunt betreft het aangifte- en hulpproces ten behoeve van slachtoffers. In het kader van de invoeringstoets is door de betrokken organisaties naar voren gebracht dat er behoefte is aan een gezamenlijk kader tussen de politie en de hulporganisaties over de gevallen waarin een slachtoffer naar een specifieke instantie moet worden verwezen. Dit moet voorkomen dat een slachtoffer telkens opnieuw naar een andere instantie wordt verwezen. Het is bijvoorbeeld niet altijd duidelijk in welke gevallen een slachtoffer naar Offlimits of naar Slachtofferhulp Nederland moet worden verwezen. Zo zijn er slachtoffers die een online bericht willen laten verwijderen door een platform. Zij zijn door de politie geadviseerd om een melding te maken in plaats van

[6] Kamerstukken II 2020/21, 35 564, nr. 13
[7] Met uitzondering van de laatste kwalitatieve uitvraag bij de Raad voor de Rechtspraak. Deze heeft in maart 2026 plaatsgevonden.

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

Datum
20 november 2026

Onze referentie
8120201

aangifte, of om helemaal geen aangifte of melding te doen. Dit terwijl enkele platforms op basis van eigen beleid om een bewijs van aangifte vragen voor het laten verwijderen van content. Naar aanleiding van deze signalen zal er vanuit het ministerie een gesprek met relevante partijen worden gefaciliteerd waarin eventuele verbeterpunten kunnen worden geïdentificeerd en bespreekbaar worden gemaakt.

Bewijs
Het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde is strafbaar als dit wordt gedaan met het oogmerk om die ander te (laten) intimideren, ernstige overlast te (laten) bezorgen of te (laten) hinderen in de uitoefening van zijn ambt of beroep. Bij de behandeling van het wetsvoorstel door de Tweede Kamer is toegezegd dat in het kader van de invoeringstoets ook naar dit oogmerkvereiste wordt gekeken.

In het kader van de invoeringstoets hebben opsporingsambtenaren aangegeven dat het op basis van de beschikbare informatie soms lastig te beoordelen is of sprake is van strafbare doxing. Daarbij wordt er onder meer op gewezen dat de intentie van degene die persoonsgegevens van een ander verspreidt niet altijd duidelijk is, waardoor naar de context waarbinnen dit is gebeurd moet worden gekeken. Opsporingsambtenaren geven ook aan dat voor hen soms onduidelijk is op welke wijze wordt beoordeeld of overlast *ernstig* is, in hoeverre daarbij van belang is dat het slachtoffer daadwerkelijk een zodanige overlast heeft ervaren.

In dit verband is relevant dat uit de invoeringstoets blijkt dat de bekendheid van de informatieproducten over doxing onder opsporingsambtenaren relatief laag is. Het versterken van de kennis over doxing kan eraan bijdragen dat zij strafbare doxing beter kunnen herkennen en slachtoffers beter kunnen helpen. Daarom zullen de informatieproducten binnen de opsporingsinstanties verder onder de aandacht worden gebracht.

Het overgrote deel van de officieren van justitie waarmee is gesproken heeft aangegeven dat het oogmerkvereiste niet als een drempel wordt ervaren om het feit ten laste te leggen of mee te wegen in een strafzaak. Uit de relatief beperkte jurisprudentie met betrekking tot artikel 285d Sr blijkt ook niet dat dit vereiste tot veel discussie leidt. Enkele officieren van justitie hebben aangegeven discussie te verwachten over de vraag of overlast als *ernstig* kan worden aangemerkt. Uit de invoeringstoets blijkt niet dat deze discussie zich in de rechtspraktijk al heeft voorgedaan.

Voor de bewijsvoering van doxing is doorgaans digitaal onderzoek vereist, zowel op socialmediaplatforms als op de telefoon van een verdachte. Digitaal onderzoek kent bemoeilijkende factoren, die hieronder worden toegelicht. Deze moeilijkheden spelen niet alleen bij onderzoeken naar doxing, maar worden ook ervaren bij digitaal onderzoek naar andere strafbare feiten.

De mate waarin bewijs kan worden verkregen is sterk afhankelijk van de omstandigheden van het geval. In sommige situaties kan de identiteit van een verdachte direct worden vastgesteld, bijvoorbeeld wanneer een verdachte persoonsgegevens onder eigen naam heeft verspreid, het gepleegde feit heeft bekend of reeds bekend is bij het slachtoffer. In andere gevallen is de dader niet altijd direct identificeerbaar en is nader onderzoek vereist. Het achterhalen van de identiteit van een verdachte kan complex zijn, met name op sociale media. Dit komt onder meer door het gebruik van

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

Datum
20 november 2026

Onze referentie
8120201

anonieme accounts en versleutelde internetverbindingen. Daarnaast vormt het tijdig vaststellen van bewijs een uitdaging, omdat berichten online snel en gemakkelijk, en in sommige gevallen automatisch, kunnen worden verwijderd. Wanneer niet al het relevante materiaal tijdig kan worden vastgelegd, kan dit leiden tot een onvolledig beeld van de feitelijke gebeurtenissen. Voorts kan de bewijsvergaring mede afhankelijk zijn van de bereidheid van een dienstaanbieder om mee te werken als gegevens over een verdachte worden gevorderd, zoals het gebruikte IP-adres. Met name dienstenaanbieders die in het buitenland zijn gevestigd of besloten kanalen aanbieden, verlenen niet altijd medewerking.

Digitale opsporingsonderzoeken zijn doorgaans tijdsintensief en vereisen in complexe zaken specialistische kennis. Gelet op de beperkte capaciteit en de intensiteit van het onderzoek, moet in veel gevallen een afweging worden gemaakt over de in te zetten opsporingsmiddelen. Bij de prioritering van zaken wordt vaak rekening gehouden met door slachtoffers ervaren gevolgen van doxing en met hun wensen ten aanzien de afdoening van de zaak. In voorkomende gevallen kan worden volstaan met het verwijderen van persoonsgegevens zodat deze niet langer voor anderen beschikbaar zijn.

Verwijderen van persoonsgegevens buiten een strafrechtelijke context
Slachtoffers van doxing kunnen bij Offlimits terecht voor hulp bij het (laten) verwijderen van onrechtmatige content. In specifieke gevallen kan de organisatie namens het slachtoffer rechtstreeks een verwijderverzoek bij een platform indienen. Voor organisaties zoals Offlimits is het in gevallen waarin niet evident is dat sprake is van strafbare doxing lastig om te bepalen of er namens het slachtoffer een verwijderverzoek bij een platform kan worden ingediend.

Offlimits heeft als trusted flagger onder de Digitaledienstenverordening (DSA) een bijzondere positie, waardoor een platform een melding van Offlimits met voorrang en binnen afzienbare tijd moet behandelen. In sommige gevallen kan de verwijdering binnen enkele minuten al plaatsvinden. Echter, doordat platforms eigen richtlijnen en gebruikersvoorwaarden hanteren en een melding van doxing niet in alle gevallen als zodanig herkennen, komt het voor dat een melding van onrechtmatige content niet of niet onverwijld wordt opgevolgd. Wanneer een platform een melding van doxing anders beoordeelt, kan dit ten nadele gaan van het vertrouwen in de meldingen van een trusted flagger. Dit heeft tot gevolg dat door Offlimits alleen meldingen worden gemaakt van evidente gevallen, om de betrouwbare status bij een platform te behouden.

Autoriteit Persoonsgegevens (AP)
In veel gevallen van doxing is ook sprake van een verwerking van persoonsgegevens in strijd met de AVG. De AP houdt toezicht op de naleving van de AVG. Als mensen slachtoffer worden van doxing, kunnen zij naast het maken van een melding bij de politie, een klacht indienen bij de AP. Tot op heden gaan de meldingen van doxing bij de AP over een individu, vaak met onvoldoende bewijs of aanknopingspunten om tot een vaststelling van een overtreding van de AVG te kunnen komen. De AP houdt risicogestuurd toezicht. Dat betekent dat zij klachten oppakt op basis van de ernst en impact die de verwerking heeft op mensen en de maatschappij. Een melding die meerdere mensen treft zal daardoor eerder worden opgepakt dan een melding die om een enkel persoon gaat. Naast het indienen van een klacht bij de AP, kunnen mensen bij

de AP terecht voor bemiddeling bij klachten.[8] Zo kan de AP slachtoffers helpen bij het laten verwijderen van gegevens bij zoekresultaten in zoekmachines.

Doxing politieambtenaren
Politieambtenaren worden vanwege de functie die zij vervullen geregeld slachtoffer van doxing. Via sociale media circuleren bijvoorbeeld video's van politieambtenaren die handhavend optreden of in undercover dienstvoertuigen rondrijden waarbij de kentekens van die voertuigen worden gedeeld. Ook zijn er gevallen waarin andere persoonsgegevens van politieambtenaren worden gedeeld, zoals hun privéadres, of waarin een oproep wordt gedaan om deze te delen. Het slachtoffer wordt hierdoor niet alleen gehinderd in de uitoefening van zijn of haar politiewerk, maar het heeft vaak ook gevolgen voor de familie- en vriendenkring. In 2025 zijn er 27 doxingzaken geregistreerd waarbij politiemedewerkers als slachtoffer betrokken waren.[9] Een aantal van de politieambtenaren die informatie hebben verstrekt voor de invoeringstoets zijn zelf slachtoffer geweest van doxing. Uit de verstrekte informatie blijkt dat de afhandeling van de zaak afhankelijk is van de casus. In enkele gevallen was het niet duidelijk voor de politieambtenaar of leidinggevende welke maatregelen moesten worden genomen of was de politieambtenaar teleurgesteld over de afhandeling van de zaak. De politie ondersteunt als werkgever haar medewerkers op verschillende manieren bij doxing. De werkgever biedt een gedoxte politiemedewerker sociale, emotionele of juridische hulp. Hiervoor is een handelingskader voor teamchefs opgesteld. Dit handelingskader is gericht op maatregelen die de politie neemt als politiemedewerkers online worden geïntimideerd of waarvan privégegevens worden gepubliceerd, zoals de begeleiding bij het aangifteproces. Ook hebben politiemedewerkers zelf een verantwoordelijkheid om het risico op doxing te minimaliseren, bijvoorbeeld door gebruik te maken van afgeschermde sociale media-accounts. De politie blijft zich inzetten om het bewustzijn van politiemedewerkers op het gebied van digitale veiligheid te versterken.

Journalisten
Bij de totstandkoming van de wet werd gevreesd dat de strafbaarstelling een risico zou vormen voor de vrijheid van meningsuiting en nieuwsgaring van journalisten. Om er zeker van te zijn dat de strafbaarstelling geen nadelige gevolgen voor de positie van journalisten heeft, bijvoorbeeld doordat zij worden geconfronteerd met onterechte aangiftes, is bij de invoeringstoets gekeken naar het aantal aangiftes van doxing door journalisten. Voor zover kon worden vastgesteld is er sinds de inwerkingtreding geen aangifte van doxing tegen een journalist gedaan.

Uitvoeringslasten
Bij het wetsvoorstel is een inschatting gemaakt van de te verwachten kosten voor de strafrechtketen als gevolg van de strafbaarstelling. Deze verwachtingen zijn uitgewerkt in drie scenario's:
- *scenario 1 lichte toename;*
- *scenario 2 substantiële toename; en*
- *scenario 3 sterke toename.*

Anders dan de inschatting van de politie, *een scenario 1 lichte toename*, meende het OM dat het aantal zaken aanzienlijk hoger zou kunnen uitkomen, namelijk *scenario 3 sterke toename*. De zorg daarbij was dat het aantal zaken de beschikbare capaciteit bij het OM en de politie zou overstijgen indien scenario 3, een sterke toename, werkelijkheid zou worden. Dit is niet gebeurd. Het aantal aangiften van doxing zit tussen scenario 1 en 2.

[8] Zie ook de website van de AP voor een privacyverhaal over bemiddeling door de AP bij klachten.
[9] Meer agressie en geweld tegen politie | politie.nl

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

Datum
20 november 2026

Onze referentie
8120201

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

Datum
20 november 2026

Onze referentie
8120201

Alhoewel de strafbaarstelling van doxing bij de politie en het OM tot extra werkzaamheden heeft geleid, is er geen extra capaciteit bijgekomen of vrijgemaakt voor doxing-zaken. In 2024 zijn er 295 misdrijven ter kennis gekomen van de politie en zijn er 261 aangiften gedaan. In 2025 zijn 406 misdrijven ter kennis gekomen van de politie en zijn er 330 aangiften gedaan.

In de eerste ruim anderhalf jaar tijd na de strafbaarstelling van doxing zijn er 140 strafzaken ingezonden naar het OM. Er kunnen omstandigheden zijn waarbij er naast doxing ook sprake is van andere (overlappende) strafbare gedragingen. Het is dan aan de officier van justitie om een besluit te nemen over de strafbare gedragingen waarvoor een verdachte wordt vervolgd. In de meeste strafzaken waarin doxing aan de orde is, wordt primair een ander feit ten laste gelegd. Uit cijfers van het OM blijkt dat doxing in bijna driekwart van de gevallen in combinatie met andere strafbare feiten wordt vervolgd; veelal belediging, smaad, bedreiging of belaging. Het OM constateert dat het aantal bedreigingszaken in diezelfde periode nagenoeg stabiel is gebleven, ruim 10.000 zaken op jaarbasis, en het aantal belagingszaken licht is toegenomen, ruim 1150 tot 1200 zaken. Uit de cijfers blijkt dus geen vervangingseffect van de delicten bedreiging en belaging door doxing.

In de memorie van toelichting is reeds rekening gehouden met de schaarste aan middelen en capaciteit, waardoor de organisaties binnen de strafrechtketen in bepaalde gevallen genoodzaakt zijn om een keuze te maken in de prioritering van opsporingszaken.[10] Ook is aangegeven dat naar aanleiding van de motie-Hermans middelen zijn vrijgemaakt voor de algehele versterking van de (digitale) capaciteit bij politie en OM. Bovendien wordt in het geval van doxing niet alleen het strafrecht ingezet om de strafbare gedraging tegen te gaan. Er zijn de afgelopen jaren geen specifieke middelen of capaciteit toegekend voor de aanpak van doxing. Wel zijn middelen vrijgemaakt die in brede zin van belang zijn voor de aanpak van online criminaliteit. Het gaat daarbij om de investeringen vanuit het kabinet-Schoof in de aanpak van gedigitaliseerde criminaliteit.[11] Ik heb in mijn beleidsbrief aangegeven dat het kabinet graag wil investeren in politiemedewerkers die gespecialiseerd zijn in het bestrijden van online criminaliteit.[12] Oplopend naar 2030 wordt structureel 44,5 miljoen euro beschikbaar gesteld voor de aanpak van online criminaliteit.[13] Dit betekent voor een groot deel uitbreiding van de formatie in de opsporing.

Conclusie
De invoeringstoets laat zien dat de strafbaarstelling van doxing in de praktijk voorziet in een duidelijke behoefte en in grote lijnen werkt zoals beoogd. Zowel uitvoeringsorganisaties als slachtoffers ervaren de strafbaarstelling als waardevol onder meer omdat eerder strafrechtelijk kan worden opgetreden in situaties waarin dat noodzakelijk is om doxing te beëindigen. Er zijn geen problemen ten aanzien van de strafbaarstelling naar voren gekomen in de invoeringstoets. Wel zijn er zoals in deze

[10] Kamerstukken II 2021/22, 36 171, nr. 3 (MvT).
[11] Brief TK Investeringen in de politie en (strafrecht)ketenpartners en juridische borging van de neutrale uitstraling van boa's, d.d. 14 november 2024, kamerstukken II, 2024/25, 36600-VI, nr. 32.
[12] Beleidsbrief ministerie van Justitie en Veiligheid, d.d. 24 april 2026, https://open.overheid.nl/documenten/db588de0-2e7a-4e78-9617-ca57cd2a6008/.
[13] Kamerbrief ten behoeve van wetgevingsoverleg Artikel 31 Politie, d.d. 28 oktober 2026, Kamerstukken II 2026/27, 2026D53911.

brief is beschreven enkele aandachtspunten voor de praktijk waarmee ik de komende tijd aan de slag ga. Door het verstrekken van de informatie in deze brief, beschouw ik de genoemde toezeggingen als afgedaan.

De Minister van Justitie en Veiligheid,

D.M. van Weel

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

Datum
20 november 2026

Onze referentie
8120201