

Vergaderjaar 2022–2023

**36 171**

## **Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafrecht BES, het Wetboek van Strafvordering en het Wetboek van Strafvordering BES in verband met de strafbaarstelling van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden (strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden)**

**Nr. 6**

### **NOTA NAAR AANLEIDING VAN HET VERSLAG**

Ontvangen 9 november 2022

#### **1. Inleiding**

Met veel belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Justitie en Veiligheid over dit wetsvoorstel. Ik dank de leden van de fracties van VVD, D66, PvdA, SP, ChristenUnie en SGP voor de door hen geleverde inbreng. Leden van deze fracties hebben de motie Michon-Derkzen c.s. (Kamerstukken II 2020/21, 35 564 nr. 13) waaraan dit wetsvoorstel uitvoering geeft (mede)ingediend en ik constateer met genoegen dat deze leden blijf geven van een positieve grondhouding ten aanzien van het wetsvoorstel. Graag ben ik bereid om de vragen te beantwoorden die zij hierover hebben gesteld. Bij de beantwoording van de gestelde vragen is de indeling van het verslag zoveel mogelijk gevolgd. Waar dit de duidelijkheid ten goede komt, is een aantal vragen samen beantwoord.

#### **2. Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden**

De leden van de SP-fractie vragen hoe de regering bedrijven, overheidsinstaties en burgers ervan gaat doordringen dat dataminimalisatie het uitgangspunt is bij de verwerking van gegevens en hoe ervoor wordt gezorgd dat persoonsgegevens minder makkelijk raadpleegbaar worden door derden.

Met de leden van de SP-fractie is de regering van mening dat, nu het door technologische ontwikkelingen steeds gemakkelijker wordt om gegevens te vinden over personen, het van groot belang is dat beperkingen worden betracht in hetgeen over anderen wordt verzameld en raadpleegbaar is. Dataminimalisatie is niet voor niets een van de basisbeginselen die bij de verwerking van persoonsgegevens in acht moeten worden genomen. Voorafgaand aan de verwerking moeten maatregelen worden genomen

om te voorkomen dat niet meer persoonsgegevens worden gebruikt dan nodig om het doel waarvoor deze zullen worden gebruikt te bereiken. Daarnaast moeten persoonsgegevens goed zijn beveiligd en moeten er passende technische en organisatorische maatregelen worden genomen, zodat persoonsgegevens niet raadpleegbaar zijn voor personen die daartoe niet zijn gerechtigd. Deze eisen vloeien rechtstreeks voort uit de Algemene Verordening Gegevensbescherming (AVG). De voorlichtende rol van de overheid met betrekking tot de AVG ligt primair bij de Autoriteit persoonsgegevens (AP), die daar onder meer met een website invulling aan geeft. Ook houdt de AP toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens, waaronder het vereiste dat de verwerking van persoonsgegevens goed moet zijn beveiligd. Daarnaast moet de overheid het goede voorbeeld geven als het gaat om de naleving van de AVG. Dat is op dit moment nog niet altijd het geval en dat heeft al langer de aandacht. Graag wijs ik in dit verband op de brief van 29 april jl. aan uw Kamer (Kamerstukken II 2021/22, 32 761, nr. 224) waarin het belang wordt onderstreept dat juist overheden de AVG naleven. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) doet op dit moment onderzoek naar de oorzaken van de steken die overheidsorganisaties op dit punt laten vallen. De resultaten worden eind dit jaar verwacht en zullen dan aan uw Kamer worden aangeboden.

De leden van de SGP-fractie vragen waarom het «zich verschaffen» van persoonsgegevens voor intimiderende doeleinden onder de reikwijdte van de voorgestelde strafbaarstelling valt. Deze leden wijzen erop dat het oogmerk van de betrokkene zich pas openbaart na het verspreiden of anderszins ter beschikking stellen van persoonsgegevens. Zij vragen hoe op het «zich verschaffen» van persoonsgegevens voor intimiderende doeleinden zal worden gehandhaafd.

Terecht merken de leden van de SGP-fractie op dat het niet altijd duidelijk zal zijn met welk oogmerk iemand zich gegevens verschaft. Dat neemt echter niet weg dat de verdachte al met dat oogmerk persoonsgegevens aan het verzamelen kan zijn. Dit kan blijken als daarvoor tijdens het verzamelen of nadien bij het aantreffen van de gegevens aanknopingspunten kunnen worden gevonden. Zo is voorstelbaar dat bij een doorzoeking een lijst van adressen wordt aangetroffen en de verdachte of een getuige verklaart dat deze persoonsgegevens zijn verzameld om de betrokkenen thuis te kunnen bedreigen. Daarbij hoeft de verdachte die persoonsgegevens nog niet verder te hebben verspreid. Een dergelijke situatie doet zich bijvoorbeeld voor als de verdachte via social media heeft gevraagd om persoonsgegevens van een groep beroeps- of ambtgenoten omdat hij vindt dat juist deze groep een lesje moet worden geleerd. Dat het oogmerk bij het «zich verschaffen» niet gemakkelijk vast te stellen zal zijn, doet naar mijn mening geen afbreuk aan de strafwaardigheid van de gedraging. Reeds het enkele feit dat persoonsgegevens met een vreesaanjagende of krenkende bedoeling worden verzameld, is zeer kwalijk. De handeling kan op zichzelf – zodra het slachtoffer hiermee bekend wordt – ook een zeer beangstigend effect hebben en onveiligheidsgevoelens teweegbrengen.

### *2.1 De verhouding tot bestaande strafbaarstellingen*

De leden van de SP-fractie vragen wat de voorgestelde strafbaarstelling toevoegt aan het arsenaal van het openbaar ministerie om ongewenst (online) gedrag te bestraffen. Zij vragen welk gat hiermee precies wordt gevuld en in welke gevallen het openbaar ministerie niet met de huidige strafbaarstellingen tot een vervolging zou kunnen komen, maar wel op grond van de voorgestelde strafbaarstelling.

Strafbaarstelling van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens met het doel een ander te intimideren (hierna ook: strafbare doxing) is noodzakelijk om in gevallen van intimidatie die binnen onze samenleving als dreigend en onacceptabel worden ervaren maar op dit moment nog niet strafbaar zijn, toch strafrechtelijk op te kunnen treden. Het kan, zoals de leden van de SP-fractie ook opmerken, daarbij gaan om situaties die dicht tegen reeds bestaande strafbare feiten aanliggen, zoals belaging en bedreiging. Dat maakt juist dat het onverteerbaar is dat deze gedragingen, die door slachtoffers in vergelijkbare mate als angstaanjagend of ernstig overlast- of hindergevend worden ervaren, nog niet strafbaar zijn. Er is bij strafbare doxing bijvoorbeeld geen sprake van strafbare bedreiging (artikel 285 Sr; artikel 298 Sr BES) omdat niet is bedreigd met bepaalde ernstige misdrijven. Vervolgung wegens belaging (artikel 285b Sr; artikel 313a Sr BES) is ook niet mogelijk omdat niet *stelselmatig* inbreuk is gemaakt op de persoonlijke levenssfeer van een ander. En de gedraging valt ook niet onder het misdrijf opruiing (artikel 131 Sr; artikel 137 Sr BES) omdat niet *in het openbaar* wordt opgeroepen tot het plegen van een strafbaar feit. Een voorbeeld van een situatie waarin de voorgestelde strafbepaling in een leemte voorziet, betreft het delen van adressen van bepaalde beroepsbeoefenaren in een appgroep met leden met een sterk sentiment tegen die beroepsgroep, waardoor iedereen weet waar zij wonen en een huisbezoek kan volgen. Hetzelfde geldt voor het vragen van adresgegevens van bepaalde personen zodat diegenen thuis kunnen worden lastiggevallen.

De leden van de PvdA-fractie vragen of de voorgestelde strafbaarstelling ook toegepast kan gaan worden ter voorkoming van online seksuele intimidatie, zoals dat in het wetsvoorstel seksuele misdrijven strafbaar wordt gesteld, en vragen hoe deze voorstellen zich tot elkaar verhouden.

De voorgestelde strafbaarstelling (artikel 285d) heeft betrekking op het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde om die ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of hem in de uitoefening van zijn ambt of beroep ernstig te (laten) hinderen. De in het wetsvoorstel seksuele misdrijven (Kamerstukken II 2022/23, 36 222, nr. 2) voorgestelde strafbaarstelling van seksuele intimidatie (artikel 429ter) waar de leden van de PvdA-fractie naar vragen, ziet op het in het openbaar een ander indringend seksueel benaderen door opmerkingen, gebaren, geluiden of aanrakingen op een wijze die vreesaanjagend, vernederend, kwetsend of ontterend is te achten. Deze bepalingen verschillen op een aantal onderdelen van elkaar. Zo staat bij de strafbaarstelling van doxing het vreesaanjagende of ernstig overlast- of hindergevende oogmerk tijdens het vergaren en verspreiden van andermans persoonsgegevens centraal, terwijl de essentie bij seksuele intimidatie is gelegen in het indringende karakter van het seksueel benaderen van iemand in het openbaar. Anders dan bij strafbare doxing vormen daarbij persoonsgegevens geen kernbestanddeel van de strafbare gedraging. De feitelijke, fysieke of online benadering – door opmerkingen, gebaren, geluiden of aanrakingen – die indringend seksueel van aard is, bepaalt de strafbaarheid van het gedrag. In de online context zal dat meestal met opmerkingen zijn – waarvan een intimiderend seksueel effect uitgaat. Het is denkbaar dat iemand zich persoonsgegevens verschafft of die persoonsgegevens verspreidt om die ander door middel van seksuele intimidatie vrees aan te (laten) jagen. In dat geval gaat het strafbare gebruik van persoonsgegevens voor intimiderende doeleinden vooraf aan seksuele intimidatie. De strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden kan daarmee bijdragen aan het

voorkomen van seksuele intimidatie doordat in een vroeg stadium de strafbare content offline kan worden gehaald.

De leden van de ChristenUnie-fractie vragen of de regering een strafverzwarringsgrond heeft overwogen voor de gevallen waarin iemand vanwege zijn ambt of beroep slachtoffer wordt van doxing omdat de impact dan verder kan reiken dan het slachtoffer en diens directe omgeving, dit de democratische rechtsstaat kan ondermijnen en anderen kan hinderen in het uitoefenen van hun beroep of ambt.

Evenals de leden van de fractie van de ChristenUnie hecht ik eraan dat in de door die leden genoemde gevallen van strafbare doxing om de door die leden genoemde redenen een passende, relatief hoge, straf kan worden geëist en opgelegd. Het feit dat persoonsgegevens worden verspreid om personen die een bepaald ambt of beroep vervullen te intimideren, kan bijvoorbeeld ertoe leiden dat mensen bepaalde functies niet meer durven te vervullen. Tegelijkertijd kan iedereen slachtoffer worden van doxing en hoeft het effect op slachtoffers en de samenleving niet noodzakelijkerwijs samen te hangen met de functie die slachtoffers vervullen. In gevallen van agressie en geweld tegen werknemers met een publieke taak en andere functionarissen werkzaam in het publieke domein geldt dat het openbaar ministerie de strafeis aanzienlijk naar boven bijstelt (zie paragraaf 6 van de Aanwijzing kader voor strafvordering meerderjarigen (2019A003)). Dat zal ook gebeuren in geval van strafbare doxing gepleegd in of door omstandigheden die verband houden met de uitvoering van de publieke taak. De strafeis, die per zaak op grond van een nog door het openbaar ministerie op te stellen strafvorderingsrichtlijn wordt bepaald, zal in die gevallen met 200% worden verhoogd. Binnen de bandbreedte die door het voorgestelde strafmaximum wordt geboden, is er voorts voldoende ruimte voor de strafrechter om de meest ernstige gevallen van strafbare doxing proportioneel te kunnen bestraffen. Daartoe behoren ook de door deze leden bedoelde gevallen met een effect dat verder reikt dan het slachtoffer en diens directe omgeving. Een afzonderlijke wettelijke strafverzwarringsgrond is daarom niet nodig.

## *2.2 De noodzaak van strafbaarstelling*

De leden van de VVD-fractie vragen de regering met voorbeelden nader toe te lichten onder welke omstandigheden sprake kan zijn van strafbare doxing, maar dit niet ernstig genoeg is voor het instellen van vervolging en bijvoorbeeld een niet-strafrechtelijke procedure aangewezen kan zijn om de dreiging weg te nemen en de dader aan te spreken op zijn gedrag.

De beslissing of strafvervolging wordt ingesteld wegens strafbare doxing, is aan het openbaar ministerie. Bij de beslissing om strafvervolging in te stellen, zijn onder andere de maatschappelijke impact van de gebeurtenis en de gevolgen voor het slachtoffer van belang. Een eventuele aangifte van een slachtoffer kan een indicatie geven van de gevolgen van de strafbare gedraging voor het slachtoffer. Als slachtoffers de situatie daarvoor zelf niet voldoende ernstig vinden, kunnen zij bijvoorbeeld overwegen geen aangifte te doen van strafbare doxing. Bij veel gevallen van strafbare doxing zal de ervaren dreiging een rol spelen bij deze beslissing: het idee dat anderen over persoonlijke gegevens van het slachtoffer beschikken en die gegevens zouden kunnen gebruiken om het slachtoffer te intimideren, kan een reden zijn om aangifte te doen zodat de dreigende situatie kan worden beëindigd en de daders zo nodig kunnen worden vervolgd. In sommige gevallen zal verwijdering van die gegevens van het internet voldoende kunnen zijn om die dreiging weg te nemen, ook zonder een strafrechtelijke interventie van politie en openbaar ministerie. Als bijvoorbeeld iemand op de voetbalclub wordt gepest en in

dat kader de adresgegevens van de gepeste persoon worden gedeeld met de oproep om diegene thuis op te wachten, kan in sommige gevallen het (doen) verwijderen van dat online bericht, in combinatie met een stevig gesprek van het bestuur van de voetbalclub met de leden die zich schuldig maken aan pesterijen, wellicht passender zijn en voldoende om de intimidatie te beëindigen en de acute dreiging weg te nemen. Indien de gegevens op een website zijn geplaatst of via een online platform zijn gedeeld, kan het slachtoffer een verwijderverzoek indienen bij het desbetreffende platform of de desbetreffende website en daarbij overwegen dat het doen van aangifte bij de politie verder geen toegevoegde waarde heeft. Dit alles betreft een inschatting; de praktijk zal moeten uitwijzen of het inderdaad zo is dat slachtoffers het in sommige gevallen niet nodig vinden om aangifte te doen als de desbetreffende gegevens op een andere manier kunnen worden verwijderd. Overigens kan het in bepaalde gevallen ook nadat aangifte is gedaan een effectievere interventie zijn om in plaats van een opsporingsonderzoek te starten een bemiddelings- of stopgesprek te laten voeren door de politie of derden, bijvoorbeeld wanneer sprake is van minderjarige verdachten.

De leden van de VVD-fractie vrezen dat de toevoeging van de kwalificatie «ernstig» voor overlast en hinder in de uitoefening van ambt of beroep ertoe zal leiden dat er slachtoffers van doxing zullen zijn die overlast ervaren of hinder in de uitoefening van hun ambt of beroep ondervinden, zonder dat er sprake is van strafbare doxing in de zin van het voorgestelde artikel 285d. Zij vragen waarom daarvoor is gekozen. Deze leden vragen ook in welke situaties de rechter zou kunnen vaststellen dat de overlast of hinder niet ernstig genoeg was. Zij vragen of de regering het met deze leden eens is dat de omvang van de ondervonden hinder of overlast niet relevant zouden moeten zijn voor de strafbaarheid van de gedraging, maar dat dit wel een rol zou kunnen en moeten spelen bij het bepalen van de strafmaat.

Voor strafbaarheid op grond van de voorgestelde strafbaarstelling is niet vereist dat daadwerkelijk sprake is geweest van ernstige overlast of hinder in de uitoefening van ambt of beroep. Het gaat erom dat het oogmerk van de dader daarop moet zijn gericht. Dit oogmerk betreft een belangrijk onderdeel van deze strafbaarstelling, omdat de gedragingen waar het om gaat – het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens – zonder dat oogmerk in de regel niet strafbaar zijn. Voor het onderscheid tussen wel en niet strafwaardig handelen is de intentie van degene die zich persoonsgegevens verschafft, deze verspreidt of anderszins ter beschikking stelt aldus leidend: het bepaalt in belangrijke mate de ernst en afkeurenswaardigheid van het delict. Wat de verdachte met zijn handelen beoogt moet van zodanige aard zijn – en een bepaalde mate van intensiteit hebben – dat dit door het slachtoffer als intimiderend kan worden ervaren. Daarvan is sprake bij «vrees aanjagen», maar ook bij het veroorzaken van «ernstige overlast» of «ernstige hinder in de uitoefening van ambt of beroep». Dat het handelen van de verdachte door het slachtoffer ook als zodanig is ervaren, en bijvoorbeeld aanleiding is geweest om aangifte te doen, is voor strafbaarheid niet vereist. In de omschrijving van het oogmerk is een grens getrokken tussen gedragingen die naar de maatstaven van fatsoen als onbehoorlijk moeten worden beschouwd en gedragingen die vallen onder de voorgestelde strafbaarstelling. Die grens wordt overschreden als uit het oogmerk blijkt van een gerichte wil om anderen te beschadigen in hun persoonlijk leven. Daarvan hoeft nog geen sprake te zijn in gevallen van «gewone» hinder en overlast, reden waarom voor een dergelijke ruime formulering mede uit een oogpunt van duidelijkheid en voorzienbaarheid niet is gekozen. Overigens merk ik nog op dat het feit dat een bepaalde

gedraging niet strafrechtelijk verboden is – zoals bij hinder en overlast – geenszins betekent dat zij maatschappelijk geoorloofd is. De leden van de VVD-fractie vragen om een nadere toelichting op de samenhang tussen het voorgestelde artikel 285d en het huidige artikel 285 Sr waarin bedreiging strafbaar is gesteld, in het bijzonder of het klopt dat strafbare doxing met name kan zien op de gevallen waarin een concrete bedreiging in de zin van artikel 285 Sr nog niet kan worden bewezen.

Voor strafbare bedreiging (artikel 285 Sr) is vereist dat iemand wordt bedreigd met bepaalde ernstige misdrijven. Voor strafbare doxing (voorgestelde artikel 285d) is vereist dat iemand persoonsgegevens verzamelt of verspreidt met het oogmerk van intimidatie: vrees (laten) aanjagen, ernstige overlast (laten) aandoen of ernstig (laten) hinderen in de uitoefening van ambt of beroep. Dit kan bijvoorbeeld het geval zijn als iemand gegevens opvraagt van een ander zodat hij die ander kan bedreigen, of als hij voor dat doel aan iemand anders gegevens verstrekt. Op dat moment is (nog) geen sprake van bedreiging met een ernstig misdrijf. Ook is het mogelijk dat de persoonsgegevens wel zijn gebruikt om bijvoorbeeld iemand een bezoek te brengen maar dat diegene niet met een ernstig misdrijf is bedreigd, terwijl het bezoek door het slachtoffer wel als angstaanjagend is ervaren. Het gelijktijdig of opeenvolgend plegen van beide misdrijven is eveneens mogelijk: de verspreiding van persoonsgegevens gaat bijvoorbeeld gepaard met ernstige bedreigingen of de bedreiging volgt ter plaatse nadat persoonsgegevens over iemands huisadres zijn verspreid.

Vervolgens vragen de leden van de VVD-fractie of de regering heeft overwogen om extra maatregelen te treffen tegen degenen die persoonsgegevens van slachtoffers van doxing gebruiken voor het plegen van bedreigingen en andere misdrijven. Zij vragen of bijvoorbeeld is overwogen een strafverzwarringsgrond toe te voegen aan artikel 285 Sr voor de bedreigingen ten aanzien van personen van wie de persoonsgegevens als gevolg van doxing in de openbaarheid zijn gekomen.

Indien gegevens die zijn verspreid met het oogmerk van intimidatie worden gebruikt voor het plegen van gedragingen die reeds strafbaar zijn, is het aan de officier van justitie te beslissen voor welk feit of welke feiten de verdachte wordt vervolgd. Een strafverzwarringsgrond bij artikel 285 Sr voor de situatie waarvoor de leden van de VVD-fractie aandacht vragen, is niet overwogen. Indien na het plegen van strafbare doxing nog andere strafbare feiten worden begaan, ligt het immers in de rede dat de verdachte behalve voor die strafbare feiten ook afzonderlijk voor strafbare doxing zal worden vervolgd.

De leden van de PvdA-fractie vragen of wordt afgewacht of IT-bedrijven op grond van zelfregulering online geplaatste persoonsgegevens verwijderen voordat de officier van justitie, na daartoe door de rechter-commissaris gemachtigd te zijn, het bevel geeft om die gegevens ontoegankelijk te maken en hoe ervoor kan worden gezorgd dat de snelheid die nodig is om die gegevens te verwijderen gewaarborgd wordt. Deze leden vragen daarnaast hoe de infrastructuur voor het melden en ontoegankelijk maken van illegale content zich gaat verhouden tot de zelfregulering van IT-bedrijven en de bevoegdheid van de officier van justitie om ontoegankelijkmaking te bevelen.

Teneinde de gewraakte content verwijderd te krijgen kan een slachtoffer kiezen tussen: het melden van deze content bij de internettussenpersoon, zoals een platform; het doen van aangifte vanwege strafbare doxing waarna een strafrechtelijk traject kan volgen in het kader waarvan de officier van justitie in bepaalde gevallen, nadat de rechter-commissaris

daartoe een machtiging heeft verleend, een bevel kan geven strafbare content ontoegankelijk te maken; of een civielrechtelijk traject, waarbij via de civiele rechter een verwijderbevel wordt verzocht voor content die als onrechtmatig kan worden aangemerkt. Het voornemen bestaat daarnaast een laagdrempelige voorziening in het leven te roepen waarbij evident onrechtmatige content gemeld kan worden. Hiermee wordt tegemoetgekomen aan de door de Tweede Kamer aangenomen motie Van Nispen (Kamerstuk 34 602, nr. 3) die oproept tot het oprichten van een laagdrempelige voorziening om (o.a. verschillende vormen van) internetpesten tegen te gaan. Om een dergelijke voorziening effectief te kunnen laten opereren, zijn goede afspraken met de internetsector van belang, zodat – net zoals dat reeds het geval is bij meldingen bij het meldpunt kinderporno van het EOKM en het meldpunt internet discriminatie (MiND) – meldingen snel en effectief worden opgepakt en verwerkt. Door het faciliteren van een laagdrempelige meldvoorziening wordt de toegankelijkheid van de internetsector voor burgers bevorderd. Mocht een internet tussenpersoon van mening zijn dat het verwijderen (of beter: het ontoegankelijk maken) van de gewraakte content niet aan de orde is, dan kan het slachtoffer er alsnog voor kiezen de zaak voor te leggen aan een civiele rechter (eventueel via een kortgedingprocedure) of om aangifte te doen bij de politie. Zo ontstaat een evenwichtige infrastructuur waarbinnen slachtoffers eenvoudig melding kunnen maken van illegale content, en de overheid invulling kan geven aan haar verantwoordelijkheid met betrekking tot het optreden tegen strafbare content op het internet.

De leden van de ChristenUnie-fractie merken op dat het vaak niet duidelijk zal zijn wat de doelen zijn van iemand om zich gegevens te verschaffen en vragen zich af wat de precieze reikwijdte van het «zich verschaffen» is. Daarbij vragen zij wat de mogelijkheden zijn voor het openbaar ministerie om te kunnen bewijzen dat sprake was van het «zich verschaffen» van persoonsgegevens voor intimiderende doeleinden.

Bij het «zich verschaffen» van persoonsgegevens van een ander gaat het om het verzamelen en het verkrijgen van deze gegevens. Op grond van de voorgestelde bepaling is dit strafbaar indien dit gebeurt voor intimiderende doeleinden. Dat de bedoeling van een persoon bij het verzamelen van gegevens vaak niet duidelijk zal zijn, is een gegeven. In de gevallen waarin dit oogmerk niet kan worden afgeleid uit uiterlijkheden of verklaringen, zal het openbaar ministerie het oogmerk van de verdachte bij het «zich verschaffen» van persoonsgegevens van een ander en daarmee dit delict dan ook niet kunnen bewijzen. Dit doet, zoals ik ook heb aangegeven in mijn antwoord op een soortgelijke vraag van de leden van de SGP-fractie waarnaar ik hier graag verwijs, echter niet af aan de strafwaardigheid van dit gedrag. Daarnaast zullen zich ook situaties kunnen voordoen waarin het voor strafbaarheid vereiste oogmerk wel bewezen kan worden. Als bijvoorbeeld bij een doorzoeking grote hoeveelheden persoonsgegevens worden aangetroffen waarvan uit een aantekeningenboekje blijkt met welke kwaadaardige bedoeling deze gegevens door de verdachte zijn verzameld, zal strafrechtelijk optreden wel degelijk mogelijk zijn. In zo'n geval kan namelijk het bewijs van het strafbare oogmerk via het aantekeningenboekje worden geleverd.

De leden van de ChristenUnie-fractie vragen naar de gevolgen die de strafbaarstelling van het «zich verschaffen» van persoonsgegevens voor intimiderende doeleinden kan hebben voor onderzoeksjournalisten. Ook wijzen zij erop dat het werk van journalisten als beperkend kan worden ervaren door mensen waarover wordt gepubliceerd en dat kritische publicaties van journalisten kunnen leiden tot het hinderen van de uitoefening van een ambt of beroep. Deze leden vragen naar het effect

van voorliggend wetsvoorstel op journalisten en vragen nader aan te geven hoe deze groep is beschermd binnen voorliggend wetsvoorstel.

Graag verduidelijk ik de aan het woord zijnde leden dat de voorgestelde strafbaarstelling uitsluitend betrekking heeft op personen die persoonsgegevens verzamelen en verspreiden met *kwaadaardige* bedoelingen. Als er geen sprake is van het voor strafbaarheid bepalende oogmerk van intimidatie maar de intentie van de betrokkene is gericht op nieuwsgaring, zoals bij journalisten, is de voorgestelde bepaling niet van toepassing. Ik hecht er dan ook aan te benadrukken dat deze strafbaarstelling geen gevolgen heeft voor onderzoeksjournalisten en anderen die niet het oogmerk hebben een ander te intimideren. Zij kunnen onderzoek doen en hun bevindingen publiceren en hebben daarbij niet te vrezen voor strafvervolging omdat het voor strafbaarheid vereiste oogmerk in hun geval ontbreekt.

De leden van de SGP-fractie vragen de regering waarom niet bij strafbaarstellingen is aangesloten die enkel gezagsdragers en personen met een publieke functie of uit hoofde van hun beroep beschermen. Deze leden vragen daarnaast of een strafverzwarringsgrond ingeval van doxing ten aanzien van personen met een publieke taak wordt overwogen.

De voorgestelde strafbaarstelling betreft strafbaar handelen waarvan iedereen het slachtoffer kan worden: het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens treft niet alleen gezagsdragers en personen met een publieke functie. Er kunnen allerlei redenen zijn waarom iemand een ander wil intimideren. Naast het vervullen van een bepaalde functie kan dit bijvoorbeeld ook zijn vanwege het hebben van bepaalde overtuigingen of eigenschappen of vanwege een persoonlijke relatie tussen het slachtoffer en de dader. In alle gevallen wordt door het strafbare gedrag een inbreuk gemaakt op fundamentele rechten van het slachtoffer. Het effect op het persoonlijk leven van het slachtoffer kan dan ook in alle gevallen groot zijn. Daarom is het van belang dat eenieder hiertegen wordt beschermd. Uiteraard zal – zoals eerder is aangegeven – een hogere straf eis aangewezen kunnen zijn als het slachtoffer vanwege het vervullen van een (publieke) functie met strafbare doxing wordt geconfronteerd. Ten aanzien van een eventuele strafverzwarringsgrond in geval van strafbare doxing bij personen met een publieke taak verwijs ik de leden van de SGP-fractie graag naar mijn antwoord op een gelijklopende vraag van de leden van de ChristenUnie-fractie.

De leden van de SGP-fractie vragen tevens naar de uitvoeringslast wanneer eenieder aangifte kan doen van het gebruik van persoonsgegevens voor intimiderende doeleinden. Zij vragen of de politie voldoende capaciteit heeft om achter iedere melding of aangifte aan te gaan.

De politiecapaciteit is nooit onuitputtelijk. Dit betekent dat de politie niet na elke aangifte of melding van een strafbaar feit een opsporingsonderzoek zal kunnen starten. Het is aan het openbaar ministerie om te prioriteren. Belangrijke factoren daarbij zijn opsporingskans, bewijsbaarheid en ernst van de zaak. Jaarlijks wordt uw Kamer via de strafrechtenmonitor geïnformeerd over het aantal ter kennis van de politie gekomen misdrijven die om verschillende redenen, waaronder gebrek aan capaciteit, niet worden opgevolgd. Een en ander staat evenwel los van de noodzaak om bij de maatschappelijke ongewenstheid van bepaald afkeurenswaardig gedrag te voorzien in een daarop toegesneden strafbaarstelling als daartegen, zoals bij doxing het geval, met de bestaande strafwetgeving onvoldoende kan worden opgetreden.

### *2.3 Het belang van preventieve en niet-strafrechtelijke maatregelen*

De leden van de D66-fractie vragen toe te lichten welke mogelijkheden de regering ziet om bewustwording omtrent schadelijk en immoreel onlinegedrag te vergroten en op welke wijze de preventieve maatregelen zullen worden getroffen met betrekking tot online gedrag en normstellingen. Vervolgens vragen de leden van de D66-fractie of de regering rekening heeft gehouden met de duur van een civiele procedure gericht op het afdwingen van verwijdering van berichten in het geval dat providers of platformen niet meewerken en met andere obstakels die aan een prompte en een toegankelijke oplossing voor het wegnemen van dreiging in de weg staan. Zij vragen of de regering bereid is in gesprek te gaan met de grote providers en platformen die in Nederland actief zijn over doxing en het verlenen van medewerking aan verwijdering van strafbare berichten en welke aanvullende mogelijkheden de regering ziet tot het inrichten van laagdrempelige procedures die snelle verwijdering van strafbare berichten mogelijk maken. Over het verwijderen van persoonsgegevens vragen ook de leden van de PvdA-fractie of bij onwillige tussenpersonen die gegevens niet verwijderen, de gang naar de civiele rechter niet te veel tijd vergt. Daarbij vragen zij of het bevel van de officier van justitie het geëigende instrument blijft als snelheid gewenst is. Deze leden vragen de regering nader in te gaan op de voornemens voor laagdrempelige mogelijkheden om actie te ondernemen tegen illegale content. De leden van de ChristenUnie-fractie vragen de regering over te gaan tot preventieve en niet-strafrechtelijke maatregelen tegen doxing, zoals bewustwordings- en voorlichtingscampagnes.

Geïnvesteed wordt in een duidelijke en begrijpelijke infrastructuur voor het kunnen melden en verwijderen van illegale – dat wil zeggen strafbare en anderszins onrechtmatige – online content. Onderdeel daarvan is een laagdrempelige meldvoorziening, die content kan classificeren en illegale content met een verwijderverzoek kan doorgeleiden naar internet tussenpersonen. Dat is een maatregel die de druk op de strafrechtketen en op de civiele rechter moet verminderen. Een publiekscampagne, waarbij tevens aandacht is voor online gedrag, kan sluitstuk zijn van het opzetten van een dergelijke structuur. Daarbij is van belang dat de structuur wordt gedragen door alle betrokken partijen en er duidelijkheid en overeenstemming bestaat over elkaars rol. Het is daarom nog te vroeg om nu reeds in te zetten op een brede campagne, maar zal zeker worden gezien welke vorm van publiekscommunicatie passend is op het moment dat de meldvoorziening is gerealiseerd.

### *2.4 Gebruik van persoonsgegevens in het algemeen belang*

De leden van de VVD-fractie vragen welke handvatten de rechter heeft om in het geval een verdachte van het plegen van doxing zich beroept op het «aan de kaak willen stellen van misstanden» te beoordelen of er sprake is van een «misstand» die op geen andere manier aan de kaak kon worden gesteld dan via doxing.

Het aan de kaak willen stellen van misstanden biedt geen rechtvaardiging voor het met kwaadaardige bedoelingen verspreiden van persoonsgegevens. Met een voorbeeld kan dit wellicht inzichtelijk worden gemaakt. In het geval dat iemand op de hoogte is geraakt van een misstand en het idee heeft dat dit naar buiten moet worden gebracht, ligt het in de rede dat dit wordt gemeld bij de – afhankelijk van de situatie – aangewezen instantie of dat hier publiekelijk aandacht voor wordt gevraagd. In dit soort situaties mag duidelijk zijn dat de betrokkene probeert een misstand aan de orde te stellen. Dit is anders als de betrokkene, in een appgroep of op een online platform met personen die een sterke afkeer tegen een

bepaald persoon hebben, telefoonnummers of andere hem betreffende persoonlijke gegevens verspreidt met directieven om deze persoon een toontje lager te laten zingen. Dan houdt het verweer dat een misstand aan de kaak werd gesteld geen stand. De betrokkene had immers het oogmerk de ander te (laten) intimideren. Of sprake is van strafbare doxing zal de rechter aan de hand van de concrete feiten en omstandigheden van het geval moeten beoordelen. Daarbij kan betekenis toekomen aan de gedragingen en uitlatingen van de verdachte bij het verzamelen en verspreiden van persoonsgegevens en aan de context waarbinnen dit gebeurt.

De leden van de SP-fractie vragen naar de verhouding tussen dit wetsvoorstel en de AVG, in het bijzonder vragen zij te verduidelijken in welke gevallen het openbaar ministerie moet optreden en wanneer de AP als sprake is van strafbare doxing en overtreding van de AVG. Zij vragen of de AP automatisch wordt ingelicht wanneer het openbaar ministerie een zaak begint wegens strafbare doxing, zodat ook onderzoek kan worden gedaan naar overtreding van de AVG. Als dat het geval is, vragen deze leden of de AP daar ook extra capaciteit voor krijgt. De leden van de SP-fractie vragen ook naar de omgekeerde situatie: of de AP in alle gevallen het OM moet inlichten bij het tegenkomen van een onrechtmatige verwerking van persoonsgegevens waarbij het erop lijkt dat die verwerking tot doel heeft iemand te intimideren.

Het voorgestelde artikel 285d heeft betrekking op het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens met het doel een ander te intimideren. De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2, eerste lid, AVG). Er zijn situaties waarin zowel sprake kan zijn van strafbare doxing als van handelen in strijd met de AVG, bijvoorbeeld als door een organisatie een bestand zou worden aangelegd van gegevens van personen die aan een bepaald kenmerk voldoen zodat leden van die organisatie diegenen kunnen intimideren. Conform artikel 5:44 van de Algemene wet bestuursrecht zal de AP een gedraging waarvoor een bestuurlijke boete kan worden opgelegd en die ook een strafbaar feit is, aan de officier van justitie moeten voorleggen zodat de officier van justitie kan beoordelen of er strafrechtelijke vervolging moet worden ingesteld. Als daartoe niet wordt overgegaan, kan de AP bepalen of een bestuurlijke boete moet worden opgelegd. Daarnaast kan een ieder aangifte doen van een strafbaar feit waarvan diegene kennis draagt. De beoordeling of in een zaak strafvervolging wordt ingesteld is aan het openbaar ministerie. Voor het openbaar ministerie is er geen verplichting om de AP te informeren bij signalen van een onrechtmatige verwerking van persoonsgegevens. Wel kan het openbaar ministerie, net als ieder ander, een melding doen bij de AP in geval van een vermoeden dat een organisatie persoonsgegevens verwerkt op een manier die in strijd is met de AVG. In het wetsvoorstel is niet voorzien in extra capaciteit voor de AP. Daarvoor bestaat ook geen aanleiding. De gevallen waarin de AP handhavend kan optreden veranderen met dit wetsvoorstel niet.

De leden van de SGP-fractie vragen of de strafbaarstelling ziet op het delen van persoonsgegevens met een ander die daarom vraagt, terwijl de verstrekker geen weet heeft van de intimiderende doeleinden van de ontvanger. Zij vragen aan te geven of opzet vereist is om tot een bewezen feit te komen.

Voor strafbaarheid is vereist dat degene die zich persoonsgegevens van een ander verschafft, deze verspreidt of anderszins ter beschikking stelt daarbij het oogmerk heeft om die ander vrees aan te jagen dan wel aan te laten jagen, ernstige overlast aan te doen dan wel aan te laten doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel ernstig te laten hinderen. De betrokkene moet dus zelf het oogmerk van intimidatie hebben. In het door de leden van de SGP-fractie genoemde voorbeeld, waarbij de verstrekker van persoonsgegevens niet het oogmerk heeft van intimidatie en ook geen weet heeft van het oogmerk van de ontvanger, is de verstrekker niet strafbaar. Van hem mag overigens wel de nodige zorgvuldigheid worden verwacht; bij het verstrekken van andermans persoonsgegevens ligt het om redenen van fatsoen voor de hand dat men vooraf nagaat waarom deze gegevens worden gevraagd.

### **3. Adviezen**

De leden van de VVD-fractie vragen of doxing jegens politieambtenaren of andere personen met een publieke taak onder de werking van het taakstrafverbod kan worden gebracht.

Deze leden vragen daarnaast of in geval van doxing jegens een persoon met een publieke taak altijd de strafvorderingsrichtlijn van het openbaar Ministerie van toepassing is op grond waarvan de strafeis met 200% wordt verhoogd bij incidenten van agressie en geweld tegen personen met een publieke taak en of het openbaar ministerie hiervoor de strafvorderingsrichtlijn zal aanpassen.

Voor de toepasselijkheid van het bestaande taakstrafverbod is in hoge mate bepalend of sprake is van een misdrijf dat «een ernstige inbreuk op de lichamelijke integriteit van het slachtoffer ten gevolge heeft gehad». Omdat dit bij strafbare doxing niet het geval zal zijn, zou het onderbrengen van dit misdrijf onder het taakstrafverbod de bestaande systematiek doorbreken hetgeen onwenselijk voorkomt. Dit betekent uiteraard niet dat gevallen van doxing jegens politieambtenaren of andere personen met een publieke taak geen verhoogde aandacht behoeven. Agressie en geweld tegen medewerkers met een publieke taak wordt niet getolereerd. Medewerkers met een publieke taak dienen hun werk onbelemmerd te kunnen uitoefenen. Ten behoeve van de opsporing en vervolging van geweldszaken tegen werknemers met een publieke taak zijn Eenduidige Landelijke Afspraken gemaakt. Onder agressie en geweld wordt verstaan: lichamelijke en verbale geweldplegingen, belaging, intimidatie en bedreiging gepleegd in of door omstandigheden die verband houden met de uitvoering van de publieke taak (al dan niet door middel van, of gepaard gaand met beschadiging van goederen). Strafbare doxing valt onder deze definitie. Het openbaar ministerie zal een strafvorderingsrichtlijn opstellen voor strafbare doxing op grond waarvan per zaak de strafeis kan worden bepaald. In lijn met de Aanwijzing kader voor strafvordering meerderjarigen (2019A003) zal ook bij strafbare doxing gepleegd in of door omstandigheden die verband houden met de uitvoering van de publieke taak de strafeis met 200% worden verhoogd. Aanpassing van deze aanwijzing is hiervoor niet nodig. Conform de aanwijzing hanteert het openbaar ministerie dezelfde strafverhoging bij agressie of geweld tegen journalisten. Ook journalisten behoren vrijelijk en ongestoord hun belangrijke maatschappelijke rol in de samenleving te kunnen vervullen.

De leden van de VVD-fractie vragen of Slachtofferhulp Nederland is geconsulteerd over dit wetsvoorstel.

Slachtofferhulp Nederland is niet afzonderlijk geconsulteerd, maar is tijdens de consultatiefase via [www.internetconsultatie.nl](http://www.internetconsultatie.nl) de gelegenheid gesteld om op dit wetsvoorstel te reageren. Van die gelegenheid heeft Slachtofferhulp Nederland geen gebruik gemaakt.

De leden van de VVD-fractie vragen of de officier van justitie na inwerking-treding van het wetsvoorstel providers en eigenaren van platformen kan bevelen berichten met privéinformatie direct offline te halen.

In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv kan de officier van justitie met een machtiging van de rechter-commissaris aan een aanbieder van een communicatiedienst bevelen om gegevens ontoegankelijk te maken als dit noodzakelijk is ter beëindiging van een strafbaar feit. Dit is geregeld in artikel 125p Sv. Onderdeel van onderhavig wetsvoorstel is een wijziging van artikel 67, eerste lid, Sv waardoor het voorgestelde artikel 285d Sr daarin wordt opgenomen. Dit betekent dat in die gevallen waarin dit noodzakelijk is ter beëindiging van de strafbare doxing de officier van justitie na inwerking-treding van dit wetsvoorstel inderdaad aanbieders van communicatie-diensten kan bevelen persoonsgegevens ontoegankelijk te maken.

De leden van de VVD-fractie vragen of er, gelet op de verantwoordelijkheid van social media-platformen om persoonsgegevens die worden gebruikt voor strafbare doxing zo snel mogelijk van hun platformen te verwijderen, in het kader van onderhavig wetsvoorstel contact is geweest met socialemediaplatformen over het tegengaan van doxing op hun platformen. Deze leden vragen daarnaast welke maatregelen de regering treft om uitingen van strafbare doxing zo snel mogelijk offline te laten halen en om de NTD-procedures sneller en effectiever te maken.

Het onderwerp doxing is zijdelings ter sprake gekomen in gesprekken met de internetsector in het kader van andere beleidsdossiers, zoals online seksueel kindermisbruik. Enkele platformen, waaronder Facebook en Google, hebben aangegeven dat zij naar aanleiding van de wens van de Tweede Kamer om doxing strafbaar te stellen, hun moderatiebeleid met betrekking tot doxing reeds hebben aangepast. Een adequate toepassing van de Notice-and-Takedown (NTD) gedragscode volstaat om gewraakte content snel offline te halen. Daarbij helpt het als de melding afkomstig is van een zogenaamde «trusted flagger». Het voornemen bestaat om de inrichting van de eerdergenoemde laagdrempelige meldvoorziening zorgvuldig met de sector af te stemmen, zodat het meldpunt een dergelijke status kan verkrijgen. De Digital Services Act bevat aanvullende verantwoordelijkheden en verplichtingen voor zowel de overheid als de internetsector met betrekking tot illegale content. Het ligt daarom voor de hand om binnen afzienbare tijd de bestaande NTD-afspraken tegen het licht te houden en aan te passen op grond van de nieuwe wetgeving.

Ook de leden van de SP-fractie vragen aan te geven hoe ervoor wordt gezorgd dat het delen van persoonsgegevens met een intimiderend karakter zo snel als mogelijk tot een halt wordt toegeroepen door deze gegevens offline te halen. Zij vragen of slachtoffers van doxing snel genoeg worden geholpen door providers en online platformen en wat de regering zo nodig gaat doen om dit te verbeteren. In dat licht vragen zij ook hoe het staat met de uitvoering van de aangenomen motie Van Nispen c.s. (Kamerstuk 34 602, nr. 3) over het in het leven roepen van een loket waar slachtoffers zich kunnen melden en of slachtoffers van doxing zich straks ook bij dit loket kunnen melden zodat hun gegevens zo snel als mogelijk offline worden gehaald.

Met het wetsvoorstel wordt een duidelijke norm gesteld dat het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden niet is toegestaan. De internetsector heeft eigen afspraken over het uitvoering geven aan verwijderverzoeken. Graag verwijs ik naar het antwoord op de vragen van de leden van de PvdA-fractie over het zo snel mogelijk verwijderen van persoonsgegevens die online zijn geplaatst waarin is ingegaan op de inrichting van een laagdrempelige meldvoorziening. De inzet is erop gericht het slachtoffers zo makkelijk mogelijk te maken om gevallen van doxing te melden.

De leden van de PvdA-fractie vragen waarom niet toch een explicietere strafuitsluitingsgrond voor journalisten in het wetsvoorstel wordt opgenomen.

De Raad van State heeft opgemerkt dat er geen noodzaak is om een strafuitsluitingsgrond op te nemen voor degenen die te goeder trouw in het algemeen belang persoonsgegevens verzamelen en verspreiden, zoals journalisten, omdat zij op grond van de voorgestelde strafbaarstelling niet strafbaar zijn vanwege het ontbreken van het daarvoor vereiste oogmerk. Daarbij heeft de Raad van State terecht erop gewezen dat door het opnemen van een strafuitsluitingsgrond in de strafbaarstelling ook de indruk kan ontstaan dat er situaties zijn waarin het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens met het doel een ander te intimideren gerechtvaardigd is omdat het algemeen belang hiermee zou zijn gediend. Dat is nadrukkelijk niet de bedoeling. Personen met niet-kwaadaardige bedoelingen die persoonsgegevens verzamelen of verspreiden, zoals journalisten, maken zich niet schuldig aan strafbare doxing. Personen die daarentegen wel kwaadaardige bedoelingen hebben, maken zich wel schuldig aan strafbare doxing en kunnen zich niet op een hoger doel beroepen. Het opnemen van een strafuitsluitingsgrond in het wetsvoorstel zou dit wel mogelijk maken.

De leden van de ChristenUnie-fractie roepen de regering op bij wetgeving uit te gaan van werking in Caribisch Nederland, en hiervan enkel beargumenteerd af te zien.

Aan de oproep van de leden van de ChristenUnie-fractie voldoe ik graag. De burgers in Caribisch Nederland moet hetzelfde niveau van strafrechtelijke bescherming worden geboden als de burgers in het Europese deel van Nederland, dat is het kabinetsbeleid. Daarom is in dit wetsvoorstel een wijziging van het Wetboek van Strafrecht BES en het Wetboek van Strafvordering BES opgenomen.

#### **4. Uitvoerings- en financiële consequenties**

De leden van de VVD-fractie vragen hoe het «barrièremodel» dat inzichtelijk maakt op welke momenten de strafrechtketen kan worden ontlast door het inzetten van andere niet-strafrechtelijke afdoeningsmodaliteiten werkt. Deze leden vragen of dit model enkel betrekking heeft op dit wetsvoorstel of dat dit ook voor andere delicten inzichtelijk wordt gemaakt.

Het barrièremodel met betrekking tot het melden en doen verwijderen van strafbare, onrechtmatige en ongewenste online content zal worden uitgewerkt door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Reeds bestaande barrièremodellen zijn te raadplegen op de website [www.barrieremodellen.nl](http://www.barrieremodellen.nl). Een barrièremodel kan vanuit verschillende perspectieven worden ontwikkeld, namelijk vanuit crimineel

oogpunt of juist vanuit het slachtofferperspectief. Het gehele proces dat een crimineel of slachtoffer doormaakt wordt in opeenvolgende stappen in kaart gebracht. Experts vanuit verschillende overheidsinstanties, bedrijfsleven en wetenschappers, bepalen aan het begin van ieder traject vanuit welk perspectief het barrièremodel wordt gemaakt. Het initiatief voor het maken van een barrièremodel ontstaat vaak als een organisatie, zoals bijvoorbeeld de politie of het openbaar ministerie, doorkrijgt dat een delict samen met andere partners moet worden aangepakt, omdat bijvoorbeeld opsporing niet voldoende is of niet de juiste manier is om het probleem te voorkomen, te stoppen of rechterlijk af te doen. Een barrièremodel is een goed beleidsinstrument dat in- en overzicht biedt voor professionals om te bepalen welke organisatie op welk moment wat kan betekenen om criminelen te stoppen of juist om slachtoffers te helpen in de fase waarin een slachtoffer of crimineel zich in het geschetste proces van het barrièremodel bevindt.

De leden van de VVD-fractie vragen welk bestuursrechtelijk instrumentarium er bestaat voor gemeenten die willen optreden tegen doxing en of overleg is gevoerd met de Vereniging van Nederlandse Gemeenten (VNG) over het bestuursrechtelijk optreden. Deze leden vragen of ook wordt gedoeld op het in kaart brengen van de wenselijkheid van een digitaal contactverbod.

Gemeenten hebben een aantal bestuurlijke instrumenten en handelingsmogelijkheden tot hun beschikking om op te treden bij online aangejaagde openbare ordeproblematiek waaronder online intimidatie. De bestuurlijke instrumenten zijn het aanwijzen van een veiligheidsrisicogebied, een licht bevel, een noodbevel, een noodverordening en een last onder dwangsom. De last onder dwangsom is in een enkel geval toegepast in het digitale domein onder de noemer «digitaal gebiedsverbod». De handelingsmogelijkheden zijn: als gemeente zichtbaar zijn op social media en de-escaleren door een videoboodschap van bijvoorbeeld de burgemeester, het gesprek aangaan met mensen die ongewenst gedrag op internet vertonen en hen vragen onrechtmatige content te verwijderen en het door socialemediaplatformen laten verwijderen van onrechtmatige content door middel van een NTD-procedure.

De leden van de D66-fractie vragen of de regering voldoende rekening houdt met de uitvoerbaarheid van het wetsvoorstel nu politie, het openbaar ministerie en de rechterlijke macht aangeven extra capaciteit nodig te hebben om het wetsvoorstel te kunnen uitvoeren en daarvoor geen investeringen worden gedaan. Een vergelijkbare vraag wordt gesteld door de leden van de SP-fractie. Zij vragen of de regering bereid is te investeren, bovenop de gelden uit het coalitieakkoord en de motie-Hermans (Kamerstuk 35 925, nr.13) in politie en OM, om de verwachte werkdrukverhoging ten gevolge van dit wetsvoorstel op te vangen. Ook de leden van de ChristenUnie-fractie vragen naar de uitvoeringskosten. Zij vragen naar de impact van voorliggend voorstel op de capaciteit op het OM.

Het strafbaar stellen van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens met het doel een ander te intimideren komt voort uit de maatschappelijke en politieke wens om vanuit de overheid een antwoord te formuleren op het fenomeen van online normvervaging en de consequenties daarvan in de fysieke wereld.

Voor dat doel zijn bij het coalitieakkoord en als gevolg van de motie Hermans (Kamerstuk 35 925, nr.13) extra financiële middelen vrijgemaakt om politie en openbaar ministerie te versterken met betrekking tot opsporing en vervolging in het digitale domein. De uitgangspunten die

door politie, openbaar ministerie en de rechtspraak zijn gehanteerd bij het berekenen van de benodigde extra capaciteit voor de uitvoering van het wetsvoorstel lopen erg uiteen. De verwachting is dat aangiftes van strafbare doxing in de praktijk gepaard zullen gaan met aangifte van andere strafbare feiten, zoals bedreiging of opruiing. Dit is ook uiteengezet in de memorie van toelichting bij dit wetsvoorstel. Ook nu vinden veel mensen reeds de weg naar de politie om aangifte te doen van delicten die samenhangen met online intimidatie. Met dit wetsvoorstel wordt de drempel voor politie en openbaar ministerie om actief op te kunnen treden verlaagd, omdat reeds het gebruik van persoonsgegevens voor intimiderende doeleinden strafbaar wordt gesteld. Bovendien wordt actief ingezet op het inrichten van een infrastructuur om illegale online content laagdrempelig te kunnen melden en te doen verwijderen zonder tussenkomst van politie en openbaar ministerie. De nieuwe strafbaarstelling zal daarbij extra houvast bieden omdat hiermee tot uitdrukking wordt gebracht dat het gebruik van persoonsgegevens voor intimiderende doeleinden de grens van het toelaatbare overschrijdt. Dat alles neemt echter niet weg dat aanvullende strafbaarstellingen nopen om keuzes te maken, al is het maar vanwege de te verwachten keteneffecten. Het voorgaande in overweging nemende, bestaat er geen noodzaak om op voorhand extra middelen vrij te maken voor het kunnen uitvoeren van dit wetsvoorstel. Mocht gaandeweg, bijvoorbeeld bij de invoeringstoets, blijken dat politie en openbaar ministerie onvoldoende geëquipeerd zijn om gevallen van strafbare doxing die leiden tot een aangifte bij de politie strafrechtelijk af te doen, dan zal die constatering worden meegenomen in de algemene afweging van het beschikbaar stellen van middelen voor de inzet van politie en openbaar ministerie met betrekking tot criminaliteitsbestrijding en rechtshandhaving in relatie tot andere maatschappelijke vraagstukken.

De leden van de SP-fractie vragen aan te geven met welke prioriteit politie en openbaar ministerie doxing-zaken oppakken en welke zaken minder prioriteit moeten krijgen als doxing-zaken een hoge prioriteit moeten krijgen.

Het is aan het openbaar ministerie om te bepalen of, hoe en met welke prioriteit zaken worden opgepakt. De middelen die het openbaar ministerie en de politie daartoe ter beschikking worden gesteld zijn gebaseerd op democratische besluitvorming met betrekking tot de verdeling van schaarse middelen. Vooral na de extra investeringen die voortvloeien uit het coalitieakkoord en de motie-Hermans, en de niet-strafrechtelijke maatregelen die in de memorie van toelichting van dit wetsvoorstel nader worden toegelicht moeten, zoals hiervoor reeds in antwoord op vragen van de leden van de D66-fractie is aangegeven, de mogelijkheden voor het openbaar ministerie om effectief te vervolgen en te handhaven op grond van dit nieuwe wetsartikel vooralsnog toereikend worden geacht.

## **II. ARTIKELSGEWIJZE TOELICHTING**

### Artikel I (Wijziging Wetboek van Strafrecht)

De leden van de VVD-fractie vragen onder verwijzing naar de vergelijking met artikel 133 Sr in de toelichting op het voorgestelde strafmaximum naar het aantal mensen dat de afgelopen vijf jaren is veroordeeld wegens het plegen van het misdrijf dat in dat artikel strafbaar is gesteld.

In de periode 2017 tot en met augustus 2022 is er in totaal in minder dan 10 zaken iemand veroordeeld wegens het plegen van het misdrijf strafbaar gesteld in artikel 133 Sr.

De leden van de VVD-fractie stellen dat de gevolgen van doxing ingrijpender kunnen zijn voor slachtoffers dan het openbaar aanbieden van inlichtingen om enig strafbaar feit te plegen (artikel 133 Sr). Zij vragen het gekozen strafmaximum nader te motiveren. Daarbij geven zij in overweging de maximumstraf te verhogen naar maximaal twee jaar gevangenisstraf of geldboete van de vierde categorie en zij vragen in te gaan op de mogelijkheden die rechter heeft om een passende straf op te leggen en op de afschrikwekkende werking die hiervan uitgaat.

Het voorgestelde strafmaximum van een jaar gevangenisstraf of geldboete van de derde categorie wordt passend geacht voor het nieuwe misdrijf gebruik van persoonsgegevens voor intimiderende doeleinden. Dat strafmaximum is tweemaal zo hoog als het strafmaximum van artikel 133 Sr. Het geeft daarmee in de onderlinge afstemming tot dat delict uitdrukking aan de opvatting van de wetgever dat het gebruik van persoonsgegevens voor intimiderende doeleinden als een ernstiger strafbaar feit moet worden beschouwd. Ten opzichte van de wettelijke strafmaxima van andere misdrijven, in het bijzonder de misdrijven die daadwerkelijk strafbare bedreiging opleveren (artikel 285 Sr; strafmaximum van drie jaar) dan wel leiden tot een daadwerkelijke aantasting van de fysieke integriteit van het slachtoffer (artikel 300 Sr; strafmaximum van drie jaar) moet de voorgestelde strafpositie zich eveneens verhouden. En ook in die verhouding is bij de voorgestelde maximale strafhoogte sprake van evenredigheid. Het strafmaximum biedt daarmee de rechter voldoende ruimte een straf te bepalen die recht doet aan de specifieke feiten en omstandigheden van het geval en is naar verwachting hoog genoeg om potentiële daders af te kunnen schrikken.

De leden van de VVD-fractie vragen of voorwaardelijk opzet – bewust aanvaarden van de aanmerkelijke kans dat een gedraging tot gevolg heeft dat het slachtoffer vrees wordt aangejaagd overlast ondervond of werd gehinderd in zijn beroepsuitoefening – voldoende is om te voldoen aan de oogmerken uit het voorgestelde artikel 285d Sr.

Voorwaardelijk opzet is niet voldoende om te voldoen aan het in artikel 285d opgenomen opzetvereiste. Vereist is dat de verdachte het gevolg van zijn gedraging heeft beseft en (mede) heeft beoogd, niet dat hij daarmee eventueel rekening heeft gehouden en dat op de koop heeft toegenomen. Ten tijde van de gedraging heeft de verdachte de bedoeling – het oogmerk – het slachtoffer vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in zijn beroepsuitoefening. Aan dit oogmerkvereiste kan ook worden voldaan in geval van noodzakelijkheidsbewustzijn. Daarvan is sprake als het niet anders kan dan dat de verdachte heeft beseft dat het noodzakelijke gevolg van zijn handelen is dat het slachtoffer vrees zal worden aangejaagd, ernstige overlast zal worden aangedaan of in de uitoefening van zijn ambt of beroep ernstig zal worden gehinderd. Niet vereist is dat het slachtoffer daadwerkelijk is beangstigd, gehinderd of overlast heeft ervaren. Het gaat aldus om het beoogde effect, of dit op het slachtoffer ook die uitwerking heeft of zou hebben gehad is voor strafbaarheid niet relevant. Uiteraard kan dit wel meewegen bij de vervolgingsbeslissing, de strafeis en de op te leggen straf.

De Minister van Justitie en Veiligheid,  
D. Yesilgöz-Zegerius