



Advies Raad van State inzake 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)

Nader Rapport

5 juli 2022

Nr. 4081510

Directie Wetgeving en Juridische Zaken

Ministerie van Justitie en Veiligheid

Aan de Koning

Nader rapport inzake 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)

Blijkens de mededeling van de Directeur van Uw kabinet van 24 februari 2022, nr. 2022000452, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 4 mei 2022, nr. W16.22.0024/II, bied ik U hierbij aan.

Het voorstel heeft de Afdeling advisering van de Raad van State (hierna: de Afdeling of de Afdeling advisering) aanleiding gegeven tot het maken van opmerkingen ten aanzien van de reikwijdte van de strafbaarstelling, de strafuitsluitingsgrond, de verwachte uitvoeringslasten, de weergave van de internetconsultatiereacties in de memorie van toelichting en de strafbaarstelling van doxing in Caribisch Nederland. De Afdeling is van oordeel dat het voorstel aanpassing behoeft en dat de toelichting op bepaalde punten dient te worden aangevuld. Graag ga ik op deze opmerkingen in het navolgende in.

Het wetsvoorstel introduceert de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden. Deze gedragingen maken inbreuk op de persoonlijke levenssfeer van slachtoffers en kunnen schadelijk zijn voor de democratische rechtsstaat en de instituties die daarvan deel uitmaken.

De Afdeling advisering van de Raad van State onderschrijft de wens van de regering om het gebruik van persoonsgegevens voor intimiderende doeleinden strafbaar te stellen. Mede in het licht van de ruime reikwijdte van de beoogde strafbaarstelling moeten de uitvoeringslasten nader worden gemotiveerd. De Afdeling adviseert verder af te zien van het bestanddeel 'zich verschaffen' in de delictomschrijving, alsmede van een bijzondere strafuitsluitingsgrond. Verder maakt zij een opmerking over verwerking van de internetconsultatie en vraagt zij aandacht voor Caribisch Nederland. In verband met deze opmerkingen adviseert de Afdeling het wetsvoorstel en de toelichting aan te passen.

1. Achtergrond en inhoud van het voorstel

Het wetsvoorstel heeft betrekking op het onderwerp 'doxing'. Dit woord is afgeleid van het Engelse 'docs' en ziet op het openbaar maken van iemands privé-informatie.¹ In het rapport 'Online ontspoord' van het Rathenau Instituut wordt doxing omschreven als 'het openbaar maken van iemands persoon-

¹ De Van Dale geeft als omschrijving: mbt. een persoon op internet of de sociale media vertrouwelijke informatie verzamelen en publiceren over (...)

lijke, sensitieve en privé-informatie zoals adres, telefoonnummer, paspoort, werkgever, gegevens van familie en foto's van iemands kinderen'.² Rond het jaar 2000 wordt voor het eerst doxing signaleerd, maar sinds de coronapandemie heeft dit fenomeen een vlucht genomen. Over de precieze omvang van doxing is echter nog weinig bekend.³

De redenen van mensen om aan doxing te doen, zijn niet eenduidig. Waar sommigen hieruit enkel plezier willen halen, zetten anderen doxing in als middel om politieke of maatschappelijke doelen te bereiken. Het Rathenau Instituut kwalificeert doxing als een vorm van 'digitaal vigilantisme', waarbij de drijfveer morele afkeuring en eigenrichting is. Doxing wordt schadelijk geacht omdat privé-informatie van slachtoffers online gemakkelijk misbruikt kan worden, bijvoorbeeld om iemand te bedreigen of diens werkgever lastig te vallen. Het kan bovendien leiden tot (online) zelfcensuur omdat personen bang zijn zelf slachtoffer te worden van doxing.⁴

Het wetsvoorstel beperkt zich tot doxing voor intimiderende doeleinden. Met het voorstel wordt het strafbaar om persoonsgegevens van een ander of een derde te verschaffen, verspreiden of anderszins ter beschikking stellen met het oogmerk 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. Op het misdrijf wordt een gevangenisstraf van ten hoogste een jaar of een geldboete van de derde categorie gesteld.⁵

Dit wetsvoorstel geeft uitvoering aan de breed gesteunde motie Michon-Derkzen c.s.⁶ In de motie wordt overwogen dat doxing in toenemende mate voorkomt richting onder meer hulpverleners, journalisten, wetenschappers en politici, en grote gevolgen heeft voor de veiligheid van deze personen.

In de toelichting bij het wetsvoorstel wordt vermeld dat doxing met intimiderende doeleinden een grote impact kan hebben op de slachtoffers en hun naasten, de groep waartoe zij behoren of de organisatie waarvoor zij werkzaam zijn. Het verspreiden van bijvoorbeeld het woonadres of de naam van de school van hun kinderen maakt de drempel lager om de slachtoffers of hun naasten fysiek te confronteren. Dit leidt ertoe dat personen vrezen voor hun eigen veiligheid en die van hun naasten, omdat zij niet kunnen voorzien hoe voor hen onbekenden met deze informatie zullen omgaan in de fysieke wereld. Daarom passen zij hun gedrag aan en voelen zij zich minder vrij in hun doen en laten. In sommige gevallen leidt doxing daadwerkelijk tot anonieme, collectieve en gecoördineerde acties tegen het slachtoffer.⁷ Ook organisaties, en gedragszagers daarbinnen, kunnen zich door doxing gedwongen voelen om hun handelswijze aan te passen. Op die manier kan doxing met intimiderende doeleinden invloed uitoefenen op het functioneren van de democratische rechtsstaat en haar instituties.⁸

De Afdeling onderschrijft dat doxing met intimiderende doeleinden grote impact kan hebben op slachtoffers en hun naasten. Daarnaast kan doxing in bepaalde gevallen een potentiële bedreiging vormen voor het functioneren van de democratische rechtstaat. De Afdeling onderschrijft daarom de wens van de regering om te komen tot strafbaarstelling van het verspreiden of ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden. Niettemin heeft zij enkele opmerkingen over de voorgestelde strafbaarstelling.

2. Reikwijdte van de strafbaarstelling

Het wetsvoorstel heeft als doel doxing met intimiderende doeleinden strafbaar te stellen. De voorgestelde strafbaarstelling is ruim omschreven en omvat een gevarieerd palet aan situaties. In de toelichting worden voorbeelden aangehaald van politieagenten, journalisten, opiniemakers, wetenschappers, politici en bestuurders die vanwege hun werk of functie het slachtoffer van doxing worden.⁹ Deze voorbeelden zijn ook in lijn met de motie die de aanleiding vormt voor dit wetsvoorstel. In de toelichting wordt echter vermeld dat de strafbaarstelling, in tegenstelling tot in Frankrijk, niet is beperkt tot 'bepaalde beroepsgroepen of personen', omdat op voorhand niet goed is te bepalen welke

² Rathenau Instituut, *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland* (onderzoek in opdracht van het WODC), juli 2021, p. 15.

³ Rathenau Instituut, *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland* (onderzoek in opdracht van het WODC), juli 2021, p. 41.

⁴ Rathenau Instituut, *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland* (onderzoek in opdracht van het WODC), juli 2021, p. 40.

⁵ Voorgesteld artikel 285b Sr.

⁶ Kamerstukken II 2020/21, 35564, nr. 13.

⁷ Toelichting, paragraaf 4.

⁸ Toelichting, paragraaf 1.

⁹ Toelichting, paragraaf 1 en 4.

beroepsgroepen hiermee zullen worden geconfronteerd en omdat het effect op slachtoffers niet samenhangt met hun beroep.¹⁰

Binnen de ruime strafbaarstelling zoals voorgesteld vallen dus situaties waarin personen niet vanwege hun ambt, beroep of maatschappelijke functie met doxing worden geïntimideerd. In de toelichting worden hiervan echter geen voorbeelden genoemd. Om beter zicht te krijgen op de situaties waar het hier om gaat, acht de Afdeling dat wel gewenst. Zij denkt hierbij aan iemand die een foto en telefoonnummer van een ex-partner op een online forum zet, een buurtbewoner die het adres van een zedendelinquent in de buurtapp rondstuurt of een slachtoffer dat de volledige naam van een verdachte in een strafzaak via sociale media verspreidt.

Het is evident dat voornoemde situaties bedreigend kunnen zijn voor de betrokkenen. De Afdeling begrijpt in dat licht gezien de wens om doxing ook in dergelijke situaties strafbaar te stellen. Deze situaties kunnen echter onderscheiden worden van situaties waarin personen geïntimideerd worden wegens hun ambt, beroep of maatschappelijke functie en die kunnen doorwerken in het functioneren van de democratische rechtsstaat en haar instituties. De strafbaarstelling van doxing in andere situaties behoeft daarom in de motivering zelfstandig aandacht. De Afdeling acht de toelichting op dit punt nog niet toereikend.

De ruime reikwijdte van de strafbepaling in het voorstel lijkt met name te zijn ingegeven doordat het moeilijk is tot afbakening te komen van beroepsgroepen die met doxing worden geconfronteerd. De Afdeling constateert dat het Wetboek van Strafrecht meer bepalingen bevat die specifiek gericht zijn op personen met een bepaald ambt, beroep of maatschappelijke functie.¹¹ Dit argument acht de Afdeling daarom niet overtuigend. Zij begrijpt het wetsvoorstel zo dat omdat doxing (ook) een bedreiging kan zijn voor personen die niet tot de in de toelichting genoemde beroepsgroepen behoren, gekozen is voor een ruime strafbaarstelling.

De Afdeling adviseert in de toelichting nader in te gaan op de strafbaarstelling van doxing in gevallen waarin dit geen verband houdt met het ambt, beroep of de maatschappelijke functie van slachtoffer en hiervan voorbeelden te noemen in de toelichting.

2. Reikwijdte van de strafbaarstelling

Een ieder kan slachtoffer worden van doxing. Dat kan zijn vanwege een functie of vanwege bepaalde overtuigingen, als het slachtoffer bijvoorbeeld volksvertegenwoordiger of wetenschapper is, maar ook om meer persoonlijke redenen, als de dader bijvoorbeeld een rancuneuze ex-partner is. De impact die doxing op het slachtoffer kan hebben, hoeft niet samen te hangen met diens beroep of functie, de aard van de gegevens die worden verspreid en de kring waarbinnen dit gebeurt zal hiervoor in sommige gevallen meer bepalend zijn. Daarom wordt een strafbaarstelling met een ruime reikwijdte voorgesteld.

Naar aanleiding van het advies van de Afdeling over de reikwijdte van de strafbepaling is de memorie van toelichting aangevuld. De aangedragen voorbeelden zijn aan de toelichting toegevoegd en in verschillende passages is gewezen op de impact die doxing kan hebben op slachtoffers die niet tot bepaalde beroepsgroepen behoren. De door de Afdeling aangehaalde passage over de keuze om de strafbaarstelling niet tot bepaalde beroepen te beperken is aangepast om te verduidelijken dat iedereen mogelijk slachtoffer kan worden van doxing en daartegen moet worden beschermd. In de gevallen waarin iemand vanwege zijn ambt of beroep slachtoffer wordt van doxing kan de impact verder reiken dan het slachtoffer en diens directe omgeving. Het kan er bijvoorbeeld toe leiden dat mensen bepaalde functies niet meer durven te vervullen. Ook kan het functioneren van de democratische rechtsstaat gevaar lopen omdat belangrijke functionarissen en organisaties hun taken niet meer ongehinderd kunnen uitvoeren. In die gevallen zal een hogere strafeis aangewezen kunnen zijn. Het voorgestelde strafmaximum biedt daartoe voldoende ruimte.

3. Verwachte uitvoeringslasten

Gegeven de ruime strafbaarstelling zoals onder punt 2 is beschreven, is te meer van belang dat de gevolgen daarvan voor de uitvoering zorgvuldig worden bezien. De Afdeling vindt de toelichting in dat opzicht niet toereikend.

In de toelichting wordt aangegeven dat er weinig informatie is over de omvang van het fenomeen doxing in Nederland, maar dat er een toename van het gebruik van sociale media voor 'ontoelaatbare

¹⁰ Toelichting, paragraaf 3.

¹¹ Toelichting, paragraaf 2.1 (De verhouding tot bestaande strafbaarstellingen).

uitingen' is te zien.¹² In de uitvoeringsparagraaf wordt geconcludeerd dat de structurele gevolgen voor de uitvoering, en als gevolg daarvan de financiële consequenties, van het wetsvoorstel beperkt zullen zijn en kunnen worden opgevangen binnen de begrotingen van politie, openbaar ministerie en de rechtspraak. Dit wordt onder meer gebaseerd op de overweging dat een deel van de slachtoffers ook thans naar de politie stapt, waarbij ook nu een afweging van de strafwaardigheid moet worden gemaakt.

Verder is aangegeven dat slachtoffers ook via internettussenpersonen de gewraakte content ontoegankelijk kunnen maken. Daarnaast wordt opgemerkt dat uiterlijk twee jaar na de inwerkingtreding van de wet een invoeringstoets wordt uitgevoerd om te bezien of deze aanname van beperkte uitvoerings- en financiële gevolgen klopt.

De Afdeling acht deze toelichting onvoldoende. In algemene zin kan worden gesteld dat online criminaliteit toeneemt en complexer wordt, terwijl de digitale (opsporings)capaciteit bij politie en het OM beperkt is en onder druk staat.¹³ Dit noopt ertoe dat bij nieuwe strafbaarstellingen van (mede) in het digitaal domein gepleegde gedragingen in het bijzonder aandacht wordt besteed aan de uitvoerings- en handhavingcapaciteit. Met het wetsvoorstel wordt een strafbaarstelling geïntroduceerd waarvan het blijkens de toelichting niet alleen de bedoeling is een norm te codificeren, maar om een bepaalde gedraging daadwerkelijk aan te pakken. Ook is – zoals in punt 2 van dit advies aangegeven – gekozen voor een strafbaarstelling met een ruim toepassingsbereik. In dergelijke gevallen geldt des te meer dat zorgvuldig een schatting gemaakt dient te worden van de omvang van de problematiek, de benodigde (opsporings)capaciteit en de prioritering in relatie tot andere strafbare gedragingen. De keuze om een brede vorm van doxing strafbaar te stellen en effectief te willen handhaven leidt met de beperkt beschikbare capaciteit immers tot een lagere prioritering en minder menskracht voor andere delicten.

De Afdeling begrijpt dat een kwantitatieve inschatting van de uitvoerings- en handavingslasten voor de nieuwe strafbaarstelling lastig is te maken, maar acht in dat geval een nadere motivering op zijn plaats om tot de conclusie te komen dat deze lasten beperkt zullen zijn. Hierbij wordt ook verwezen naar het advies van het College van procureurs-generaal dat, mede na een vergelijking met het aantal zaken van belaging, voorsnog uitgaat van 1500 zaken op jaarbasis.¹⁴ Verder gaat de toelichting maar zeer beperkt in op de benodigde capaciteit voor de nieuwe strafbaarstelling en de vraag hoe hierin wordt voorzien. In verband daarmee wordt ook niet ingegaan op de betekenis van het wetsvoorstel voor de wijze waarop de prioriteiten zullen worden gesteld, gelet op de doelstelling om ook andere vormen van (digitale) criminaliteit aan te pakken.

De Afdeling adviseert om, met inachtneming van het voorgaande, nader de uitvoerbaarheid en handhaafbaarheid van het voorstel te motiveren en daarbij in te gaan op de capaciteit en prioritering in de strafrechtketen. Ook wordt geadviseerd om, conform kabinetsbeleid,¹⁵ de invoeringstoets een jaar na inwerkingtreding van het wetsvoorstel uit te voeren.

3. Verwachte uitvoeringslasten

Naar aanleiding van het advies van de Afdeling om de uitvoerbaarheid en handhaafbaarheid van het voorstel nader te motiveren is de memorie van toelichting aangevuld.

Conform kabinetsbeleid zal de invoeringstoets worden uitgevoerd op het vroegst mogelijke moment waarop iets nuttigs gezegd kan worden over de werking van dit wetsvoorstel in de praktijk en in dit geval over de gevolgen daarvan voor politie en openbaar ministerie.¹⁶ Naar aanleiding van het advies van de Afdeling is de memorie van toelichting op dit punt aangepast. Als het na een jaar mogelijk is om te beoordelen of de aannames die zijn gehanteerd bij het beoordelen van de financiële consequenties van dit wetsvoorstel, zal de invoeringstoets na een jaar worden uitgevoerd. Mocht hiervoor meer tijd nodig zijn omdat binnen een jaar nog niet voldoende zaken zijn afgerond, dan zal de invoeringstoets zo snel mogelijk daarna worden uitgevoerd. De invoeringstoets zal in ieder geval uiterlijk twee jaar na inwerkingtreding van de wet worden uitgevoerd.

¹² Toelichting, paragrafen 1 en 6.

¹³ Kamerstukken II 2019/20, 28 684, nr. 621 en Kamerstukken II 2020/21, 26 643, nr. 768.

¹⁴ Openbaar Ministerie, 'Advies wetsvoorstel strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden', 10 augustus 2021.

¹⁵ Kamerstukken II 2020/21, 35 510, nr. 4, p. 6 en de brief van de Minister voor Rechtsbescherming van 21 april 2022 aan de Tweede Kamer over de inkleuring en stand van zaken invoeringstoets, kenmerk 3921364. Zie ook VVD, D66, CDA en ChristenUnie, 'Coalitieakkoord 2021–2025', 15 december 2021, p. 1.

¹⁶ Kamerstukken II 2021/22, 35 510, nr. 96, p. 5.

4. Strafbbaarstelling van 'zich verschaffen'

De voorgestelde strafbaarstelling van doxing ziet op drie gedragingen: het zich verschaffen, het verspreiden en het anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden. In de toelichting wordt uiteengezet dat onder 'zich verschaffen' gedragingen worden geschaard die zijn 'gericht op het in het bezit krijgen van de persoonsgegevens'. Hierbij wordt actief handelen verondersteld van degene die zich gegevens verschafft. Het maakt voor de strafbaarstelling niet uit of deze gegevens zelfstandig worden verzameld of worden verkregen van derden. Indien gegevens via een derde worden verkregen, kan er volgens de toelichting ook overlap zijn met het verspreiden of anderszins ter beschikking stellen van persoonsgegevens. Als voorbeeld wordt genoemd dat iemand via sociale media oproept tot het delen van persoonsgegevens en daarbij zelf ook persoonsgegevens verspreidt.¹⁷

Het bestanddeel 'zich verschaffen' geeft een ruime reikwijdte aan de strafbaarstelling. Een enkele zoekopdracht via een internetzoekmachine lijkt voldoende te zijn om te spreken van (een poging tot) het zich verschaffen van persoonsgegevens. Als deze gedraging én het oogmerk bewezen kunnen worden, is iemand strafbaar.¹⁸ Het verzamelen van persoonsgegevens hoeft dus niet op wederrechtelijke wijze plaats te vinden, zoals bij diefstal¹⁹ of hacken²⁰ het geval is. De informatie die wordt verkregen, hoeft naar haar aard evenmin strafwaardig te zijn.²¹ Zoals in de toelichting wordt erkend, dient het strafrecht te worden ingezet als ultimum remedium.²² Uit de toelichting blijkt in dat licht bezien onvoldoende waarom de voorgestelde delictsomschrijving zich ook uitstrekt tot het enkel 'zich verschaffen' van persoonsgegevens.

De Afdeling neemt daarbij in aanmerking dat de kern van het strafbare verwijt bij doxing betrekking heeft op het verspreiden van persoonsgegevens. Pas als iemand kenbaar maakt dat hij een persoonsgegeven zoekt, in bezit heeft of met anderen deelt, kunnen de schadelijke gevolgen optreden die de wetgever beoogt te voorkomen met dit wetsvoorstel. In de toelichting wordt opgemerkt dat dergelijke gedragingen in een aantal gevallen al onder bestaande strafbaarstellingen vallen.²³ In de overige gevallen zullen de gedragingen kunnen worden aangemerkt als 'verspreiden' of 'anderszins ter beschikking stellen' in de zin van de voorgestelde strafbaarstelling van doxing. Het opnemen van het delictsbestanddeel 'zich verschaffen' in deze strafbepaling draagt dus niet (direct) bij aan het doel van het wetsvoorstel.

In de afweging die gemaakt moet worden is ook de te verwachten bewijsproblematiek van belang. In de toelichting wordt erkend dat het geheel zelfstandig verzamelen van gegevens, bijvoorbeeld door te zoeken op internet, vrijwel niet op te sporen is. Tevens wordt erkend dat het oogmerk in dat geval waarschijnlijk 'niet eenvoudig' te bewijzen zal zijn.²⁴ Ook in de consultatiereacties wordt opgemerkt dat het oogmerk moeilijk te bewijzen zal zijn als de verdachte enkel persoonsgegevens verzameld heeft en deze vervolgens niet verspreidt.²⁵ Deze bewijsrechtelijke problematiek roept eens te meer de vraag op waarom het 'zich verschaffen' in de delictsomschrijving wordt opgenomen.

Gelet op het doel van het wetsvoorstel en de te verwachten bewijsproblematiek ziet de Afdeling onvoldoende meerwaarde van het opnemen van het bestanddeel 'zich verschaffen' in de strafbaarstelling van doxing. De Afdeling adviseert daarom hiervan af te zien en dit onderdeel van het voorstel te schrappen.

Als 'zich verschaffen' niet wordt opgenomen in de delictsomschrijving, wordt deze beperkt tot de handelingen 'verspreiden' en 'anderszins ter beschikking stellen'. Hoewel de Afdeling meent dat hiermee ook de situatie kan worden ondervangen waarin iemand oproept tot het delen van persoonsgegevens,²⁶ kan zij zich voorstellen dat het wenselijk is om expliciet tot uitdrukking te brengen dat een

¹⁷ Toelichting bij artikel I, eerste lid.

¹⁸ Toelichting, paragraaf 2.1 (De verhouding tot bestaande strafbaarstellingen) en bij artikel I, eerste lid. Zie Advies Raad voor de rechtspraak (15 september 2021), p. 2–3.

¹⁹ Artikel 310 Sr e.v.

²⁰ Artikel 138ab Sr.

²¹ Zie bijvoorbeeld vervalste documenten (artikel 226 lid 2 Sr), kinderporno (artikel 240b Sr) of instructiemateriaal ten behoeve van het plegen van terroristische misdrijven (artikel 134a Sr).

²² Toelichting, paragraaf 2.3.

²³ Toelichting, paragraaf 2.1 (De verhouding tot bestaande strafbaarstellingen).

²⁴ Toelichting bij Artikel I, eerste lid.

²⁵ Advies Raad voor de rechtspraak (15 september 2021), p. 2–3; advies Nederlandse Orde van Advocaten (2 september 2021), p. 5–6.

²⁶ Met deelnemingsvormen uitlokken, doen plegen en medeplegen en voorbereidingshandelingen zou het oproepen tot het delen van persoonsgegevens ook binnen het bereik van doxing kunnen worden gebracht. In de toelichting wordt niet op deze deelnemingsvormen ingegaan. Daarnaast kan gedacht worden aan andere strafbaarstellingen, zoals opruiing en bedreiging, waar een dergelijke oproep onder kan vallen.

dergelijke oproep strafbaar is gelet op de intimiderende werking die daarvan uit kan gaan. De Afdeling adviseert daarom de delictsomschrijving aan te vullen in de zin dat het verspreiden of anderszins ter beschikking stellen van persoonsgegevens, of het daartoe aanzetten, strafbaar is.

4. Strafbaarstelling van 'zich verschaffen'

Met de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden wordt beoogd de persoonlijke vrijheid te beschermen. De strafbaar te stellen gedragingen kunnen er immers toe leiden dat slachtoffers zich niet meer vrij voelen in hun dagelijkse doen en laten vanwege de vrees dat hun iets ernstigs zal worden aangedaan of vanwege het gevoel dat zij hebben dat hun iets ernstigs zal kunnen worden aangedaan vanwege de dreiging die van de beschikbaarheid van persoonsgegevens bij kwaadwillenden uit kan gaan.

Om persoonsgegevens te kunnen gebruiken om een ander te intimideren, zal degene die dit van plan is zich eerst deze gegevens moeten verschaffen. Het 'zich verschaffen' van gegevens zal dus vaak een voorfase voor een andere strafbare gedraging zijn, bijvoorbeeld het verspreiden van deze gegevens met het oogmerk degene van wie de gegevens zijn door anderen vrees aan te laten jagen of het bedreigen van diegene. Bij het 'zich verschaffen' van gegevens kunnen anderen worden betrokken, bijvoorbeeld door het doen van een oproep gegevens te delen op social media, maar het kan ook geheel zelfstandig gebeuren, bijvoorbeeld door het opzoeken van een telefoonnummer of adres in een (digitaal) telefoonboek. Beide vormen van het 'zich verschaffen' van deze gegevens zijn strafwaardig indien dit wordt gedaan met het oogmerk een ander te intimideren. Denk bijvoorbeeld aan de situatie dat iemand een lijst aanlegt van personen met een bepaalde overtuiging, met een bepaald beroep of die een bepaald strafbaar feit hebben gepleegd met dit oogmerk. De beoogde handeling richting het slachtoffer heeft misschien nog niet plaatsgevonden, maar de betrokkene was al wel de daarvoor benodigde informatie aan het verzamelen.

In sommige gevallen zal het 'zich verschaffen' van persoonsgegevens met het oogmerk een ander te intimideren ook strafbaar kunnen zijn indien deze gedraging niet in de delictsomschrijving wordt opgenomen. Bij het opvragen van persoonsgegevens zullen bijvoorbeeld vaak persoonsgegevens worden verspreid, 'wie weet waar X woont', maar dat hoeft niet het geval te zijn, als bijvoorbeeld wordt gevraagd naar gegevens van personen met bepaalde politieke overtuigingen of van personen met een bepaalde functie. Ook het 'zich verschaffen' van deze gegevens zonder zelf gegevens te verspreiden kan in sommige gevallen strafbaar zijn, als het 'zich verschaffen' zou worden geschrapt. In de situatie dat uiteindelijk geen strafbaar feit wordt gepleegd omdat niemand op een verzoek ingaat, zal er echter geen sprake kunnen zijn van uitlokken, doen plegen of medeplegen (artikel 47 Sr). Evenmin komt strafbare voorbereiding van het gebruik van persoonsgegevens voor intimiderende doeleinden in beeld omdat daarvoor een misdrijf met een strafmaximum van acht jaar gevangenisstraf vereist is terwijl de maximale gevangenisstraf die voor de strafbaar gestelde gedragingen kan worden opgelegd een jaar bedraagt (artikel 46 Sr). In uitzonderlijke gevallen zal mogelijk sprake kunnen zijn van een strafbare poging tot uitlokken, als zou worden gepoogd iemand door giften, beloften, misbruik van gezag, geweld, bedreiging, of misleiding of door het verschaffen van gelegenheid, middelen of inlichtingen te bewegen tot het verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander met het oogmerk die ander te intimideren (artikel 46a Sr), maar in dat geval zou de maximaal op te leggen straf met een derde worden verminderd. Als niet in het *openbaar* wordt opgeroepen tot het plegen van een strafbaar feit en niet wordt gedreigd met een strafbaar feit, is er geen sprake van opruiing (artikel 131 Sr) respectievelijk bedreiging (artikel 285 Sr). Er blijft dus een restcategorie gedragingen over waarvan het wel wenselijk is dat deze strafbaar is, maar die niet in alle gevallen 'gedekt' zal zijn als het 'zich verschaffen' uit de bepaling komt te vervallen. Daarom wordt het advies van de Afdeling om het 'zich verschaffen' niet op te nemen in de delictsomschrijving niet opgevolgd. In het verlengde daarvan is er ook geen aanleiding het advies van de Afdeling over te nemen om delictsomschrijving aan te vullen met het 'aanzetten tot het verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden'. Dergelijke gedragingen zullen immers worden bestreken door het 'zich verschaffen' voor zover het gaat om het verkrijgen van de persoonsgegevens voor hemzelf. Voor zover het gaat om het anderen aanzetten tot doxing kan worden volstaan met strafbaarheid onder het eerdergenoemde artikel 46a Sr (poging tot deelneming aan misdrijf) en de deelnemingsvorm uitlokking.

In voorkomende gevallen waarin een verdachte zich geheel zelfstandig persoonsgegevens verschaft zal het vaststellen en bewijzen van het oogmerk van de verdachte niet altijd eenvoudig zijn. Van het voor strafbaarheid vereiste oogmerk is bijvoorbeeld geen sprake in geval van het opzoeken van een telefoonnummer van een collega met wie je ruzie hebt om nog eens uit te leggen waarom je zo boos bent. Het oogmerk van de verdachte moet er echt op gericht zijn een ander te intimideren. In sommige gevallen zal uit de context moeten worden afgeleid of dat het geval is. Daarbij kan bijvoorbeeld gewicht worden toegekend aan de relatie tussen het slachtoffer en de verdachte en aan de manier waarop de verdachte zich de gegevens verschaft. Op dit punt is de memorie van toelichting aange-

vuld. Zoals daarin wordt erkend zal het geheel zelfstandig verzamelen van gegevens lastig op te sporen kunnen zijn omdat het verzamelen van de gegevens niet kenbaar is voor de omgeving, nog afgezien van het feit dat het oogmerk waarschijnlijk niet eenvoudig te bewijzen zal zijn. Er zullen zich echter ook situaties kunnen voordoen waarbij dit wel mogelijk is, bijvoorbeeld als een lijst met persoonsgegevens wordt aangetroffen tijdens een doorzoeking en de verdachte zich uitlaat over zijn intenties. De mogelijke bewijsproblematiek doet overigens ook geen afbreuk aan de strafwaardigheid van de gedraging.

5. Strafuitsluitingsgrond

Het tweede lid van het voorgestelde artikel 285d voorziet in een strafuitsluitingsgrond. Op basis van dit lid is iemand niet strafbaar als deze te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de persoonsgegevens vereiste. In de toelichting wordt uiteengezet dat deze strafuitsluitingsgrond is bedoeld voor journalisten, klokkenluiders en anderen die bijvoorbeeld maatschappelijke misstanden aan de kaak willen stellen. In dit verband wordt ook gewezen op onder andere artikel 7 van de Grondwet en artikel 10 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).²⁷

De Afdeling deelt de opvatting dat het verzamelen en verspreiden van persoonsgegevens niet strafbaar zou moeten zijn als iemand te goeder trouw aanneemt dat dit in het algemeen belang is. Dit laat onverlet dat de noodzaak van de bijzondere strafuitsluitingsgrond bij deze strafbaarstelling onvoldoende is aangetoond.²⁸ Op basis van de voorgestelde strafbaarstelling in het eerste lid dient iemand immers het oogmerk te hebben om een ander vrees aan te jagen, ernstig overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen. Als iemand te goeder trouw en met het oog op het algemeen belang persoonsgegevens verzamelt of verspreidt, zal niet voldaan zijn aan dit oogmerk en is doxing dus niet strafbaar. De rechter komt dan dus niet toe aan de toetsing van de strafuitsluitingsgrond in het tweede lid.

Hierin zit een belangrijk verschil met de andere strafbepalingen waarin een vergelijkbare strafuitsluitingsgrond is opgenomen en waar in de toelichting naar wordt verwezen.²⁹ Het betreft de delicten inzake het verwerven of openbaar maken van niet-openbare gegevens die afkomstig zijn uit een misdrijf,³⁰ smaad,³¹ en schending van bedrijfsgeheimen.³² Deze bepalingen omvatten geen oogmerk dat vergelijkbaar is met het voorgestelde oogmerk bij doxing. Deze delicten kunnen dus bewezen worden verklaard terwijl de verdachte ter goeder trouw en met het oog op het algemeen belang de informatie heeft verzameld of verspreid. De goedwillende journalist, klokkenluider of blogger heeft de bescherming van deze strafuitsluitingsgrond in die gevallen dus nodig om vrijuit te gaan. Voor het delict doxing geldt dit niet.

De strafuitsluitingsgrond kan de strafbepaling compliceren in die gevallen waarin niet eenduidig is wat de bedoeling van verdachte is geweest. In de toelichting wordt niet ingegaan op situaties waarin de motieven van de verdachte diffuus zijn. Sommige activisten gebruiken bijvoorbeeld intimiderende methodes, maar handelen wel uit een oprechte bezorgdheid over problemen in de samenleving. Moet de intentie van de activist dan worden behandeld in het licht van het oogmerk als bedoeld in het voorgestelde eerste lid of in het licht van de strafuitsluitingsgrond van het tweede lid? In dat laatste geval zou dit tot de situatie kunnen leiden dat de rechter vaststelt dat iemand handelde met het oogmerk een ander te intimideren, maar dat dit niet verwijtbaar is omdat iemand te goeder trouw en in het algemeen belang handelde. Intimidatie van personen, door middel van het verspreiden van persoonsgegevens, is in een dergelijk geval wellicht (onbedoeld) toch toegestaan. Dit lijkt op gespannen voet te staan met het doel van het wetsvoorstel.

In het licht van het voorgaande adviseert de Afdeling de strafuitsluitingsgrond in het tweede lid te schrappen. De positie van journalisten, klokkenluiders en goedwillende anderen kan voldoende worden gewaarborgd bij de toetsing van het oogmerk als bedoeld in het eerste lid. In de toelichting zou dit benadrukt kunnen worden, zodat hier bij de toepassing van het voorgestelde wetsartikel in de praktijk geen twijfel over kan bestaan.

²⁷ Toelichting, paragraaf 2.4 en bij Artikel I, tweede lid.

²⁸ Zie ook de adviezen van de Nederlandse Orde van Advocaten, de AP en het Openbaar Ministerie. De Raad voor de rechtspraak heeft juist begrip voor dit tweede lid, 'om twijfel te voorkomen'.

²⁹ Zie ook advies Openbaar Ministerie (10 augustus 2021), p. 11–12.

³⁰ Artikel 139g Sr.

³¹ Artikel 261 Sr.

³² Artikel 273 Sr.

5. Strafuitsluitingsgrond

Het voor strafbaarheid vereiste oogmerk ontbreekt bij degenen die te goeder trouw hebben kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander vereiste, zoals journalisten en klokkenluiders. Door het opnemen van een strafuitsluitingsgrond kan de indruk ontstaan dat ook deze personen met niet-kwaadaardige bedoelingen zich schuldig kunnen maken aan strafbare doxing. Het is geenszins de bedoeling dat dergelijke situaties binnen het bereik van deze strafbaarstelling vallen. Als het oogmerk er niet op is gericht een ander te intimideren is het gebruik van persoonsgegevens niet strafbaar op grond van de voorgestelde bepaling. Het opnemen van een strafuitsluitingsgrond in de strafbaarstelling kan ook de indruk wekken dat er situaties zijn waarin het gebruik van persoonsgegevens voor intimiderende doeleinden gerechtvaardigd is omdat het algemeen belang hiermee zou zijn gediend, dit terwijl het gebruik van persoonsgegevens voor intimiderende doeleinden in geen geval toelaatbaar wordt geacht. Daarom is naar aanleiding van het advies van de Afdeling over de strafuitsluitingsgrond die in het wetsvoorstel was opgenomen de strafuitsluitingsgrond geschrapt en de toelichting aangepast. Voor de volledigheid wordt opgemerkt dat onverkort blijft gelden dat dit wetsvoorstel journalisten, klokkenluiders en anderen die niet het oogmerk hebben een ander te intimideren op geen enkele wijze belet om nieuwsfeiten en misstanden openbaar te maken. Zij riskeren geen strafvervolgging en veroordeling omdat het voor strafbaarheid vereiste oogmerk in hun geval ontbreekt.

6. Weergave internetconsultatiereacties

De toelichting bij het wetsvoorstel bevat een paragraaf waarin wordt ingegaan op adviezen en consultatiereacties op een concept van het wetsvoorstel. Daarin wordt een weergave gegeven van opmerkingen van partijen die anders dan via de internetconsultatie hun visie hebben gegeven op het concept. Voor de reacties op de internetconsultatie en de respons daarop vanuit de regering wordt verwezen naar een verslag op de website van internetconsultatie.

Met het oog op de transparantie van het wetgevingsproces is het wenselijk dat in de toelichting bij een wetsvoorstel aandacht wordt besteed aan de opbrengst van een internetconsultatie en de verwerking daarvan in het wetsvoorstel of de toelichting. Dit is ook in lijn met het kabinetsbeleid op dit punt³³ en de Aanwijzingen voor de regelgeving.³⁴

De Afdeling adviseert in de toelichting de via internetconsultatie binnengekomen opmerkingen en de reactie daarop vanuit de regering weer te geven.

6. Weergave internetconsultatiereacties

Het advies van de Afdeling om in de toelichting de via internetconsultatie binnengekomen opmerkingen en de reactie daarop vanuit de regering weer te geven, is opgevolgd. Aan paragraaf 5 van de toelichting is een onderdeel toegevoegd waarin de – overwegend positieve – reacties uit de internetconsultatie alsmede de opvolging die daaraan is gegeven, zijn weergegeven.

7. Caribisch Nederland

Het wetsvoorstel regelt een nieuwe strafbaarstelling voor Europees Nederland en Caribisch Nederland. Een concept van het wetsvoorstel is onder meer naar de openbare lichamen in Caribisch Nederland en de Commissie toezicht bescherming persoonsgegevens BES ter consultatie gestuurd. Het Bestuurscollege van Bonaire heeft in reactie op de consultatie aangegeven dat het Korps Politie Caribisch Nederland en het openbaar ministerie BES positief hebben gereageerd op het wetsvoorstel. Daarbij is vermeld dat het goed is dat Caribisch Nederland qua strafrechtelijk instrumentarium niet achterblijft bij Europees Nederland.

In de toelichting wordt niet ingegaan op de problematiek van doxing in Caribisch Nederland, eventueel in vergelijking met de in de toelichting beschreven probleemschets in Europees Nederland. Er wordt dus ook niet stilgestaan bij de vraag of de lokale context aldaar in enige mate relevant is voor de voorgestelde strafbaarstelling of de handhaving daarvan.

Ook worden in de toelichting niet de relevante artikelen in het Wetboek van Strafrecht BES en het Wetboek van Strafvordering BES vermeld, zoals dat wel is gedaan voor bespreking van de overlap in strafbaarstellingen in Europees Nederland. Deze artikelen zijn grotendeels gebaseerd op de Europees

³³ Onder meer beschreven in Kamerstukken II 2010/11, 29 279, nr. 121, p. 2 en Kamerstukken II 2016/17, 33 009, nr. 39, p. 3–5.

³⁴ Aanwijzing 4.44, eerste lid, van de Aanwijzingen voor de regelgeving.



Nederlandse equivalenten, maar zijn niet volledig gelijk.³⁵ Daarnaast lijkt het ten behoeve van de kenbaarheid van de strafbaarstelling in Caribisch Nederland wenselijk om in het opschrift expliciet te benoemen dat dit wetsvoorstel het Wetboek van Strafrecht BES en Wetboek van Strafvordering BES wijzigt.³⁶

De Afdeling adviseert in de toelichting in te gaan op de strafbaarstelling van doxing in Caribisch Nederland, in de toelichting de relevante artikelen van het Wetboek van Strafrecht BES en Wetboek van Strafvordering BES te vermelden en in het opschrift aan te geven dat het wetsvoorstel deze wetboeken wijzigt.

7. Caribisch Nederland

Als uitgangspunt van het kabinetsbeleid geldt dat alle Nederlanders gelijkwaardig behandeld worden.³⁷ Hieruit volgt onder meer dat de burgers in Caribisch Nederland hetzelfde niveau van strafrechtelijke bescherming wordt geboden als de burgers in het Europese deel van Nederland. Daarom wordt in de openbare lichamen Bonaire, Sint Eustatius en Saba zoveel mogelijk aangesloten bij de materiële strafwetgeving van Nederland.

De voorgestelde strafbaarstelling is voorgelegd aan de openbare lichamen in Caribisch Nederland. Het Openbaar Lichaam Bonaire heeft in reactie op dit wetsvoorstel gemeld dat het Korps Politie Caribisch Nederland en het openbaar ministerie BES positief hebben gereageerd op het wetsvoorstel, en dat het goed is dat Caribisch Nederland qua strafrechtelijk instrumentarium niet achterblijft bij Europees Nederland. Er is voor zover bekend geen reden om in aangepaste strafbaarstelling voor Caribisch Nederland te voorzien. Bij doxing gaat het in veel gevallen om online gedragingen. Daders worden mogelijk niet gehinderd door de fysieke afstand tussen de verschillende delen van Nederland. Met een vergelijkbare strafbaarstelling in beide wetboeken kan worden voorkomen dat degenen die zich in Caribisch Nederland schuldig maken aan doxing straffeloos blijven.

Het advies om in de toelichting de relevante artikelen van het Wetboek van Strafrecht BES en Wetboek van Strafvordering BES te vermelden is opgevolgd. Dat geldt ook voor het advies om het opschrift van het wetsvoorstel aan te passen. Het opschrift van het wetsvoorstel luidt nu als volgt: 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.

Ik moge U hierbij verzoeken het gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

*De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius.*

³⁵ Zie bijvoorbeeld enerzijds 285 Sr en anderzijds 298 Sr BES, op grond waarvan bedreiging waarbij 'gemeen gevaar voor de verlening van diensten ontstaat' strafbaar is gesteld in Europees Nederland, maar niet in Caribisch Nederland. Ook kan gewezen op enerzijds artikel 318 Sr en anderzijds artikel 331 Sr BES, op grond waarvan in Europees Nederland sprake kan zijn van afdreiging indien wordt gedwongen tot het ter beschikking stellen van gegevens, hetgeen in Caribisch Nederland niet onder de strafbepaling valt.

³⁶ Dit geldt temeer omdat het wetsvoorstel niet een groot aantal regelingen wijzigt in de zin van Ar 4.3, op grond waarvan in het opschrift kan worden volstaan met een vermelding van de belangrijkste regeling(en) indien de regeling tot wijziging van een groot aantal regelingen strekt.

³⁷ Kamerstukken II 2019–20, 35 300 IV, p. 1.



Advies Raad van State

No. W16.22.0024/II

's-Gravenhage, 4 mei 2022

Aan de Koning

Bij Kabinetsmissive van 24 februari 2022, no.2022000452, heeft Uwe Majesteit, op voordracht van de Minister van Justitie en Veiligheid, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering en enige andere wetten 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), met memorie van toelichting.

Het wetsvoorstel introduceert de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden. Deze gedragingen maken inbreuk op de persoonlijke levenssfeer van slachtoffers en kunnen schadelijk zijn voor de democratische rechtsstaat en de instituties die daarvan deel uitmaken.

De Afdeling advisering van de Raad van State onderschrijft de wens van de regering om het gebruik van persoonsgegevens voor intimiderende doeleinden strafbaar te stellen. Mede in het licht van de ruime reikwijdte van de beoogde strafbaarstelling moeten de uitvoeringslasten nader worden gemotiveerd. De Afdeling adviseert verder af te zien van het bestanddeel 'zich verschaffen' in de delictomschrijving, alsmede van een bijzondere strafuitsluitingsgrond. Verder maakt zij een opmerking over verwerking van de internetconsultatie en vraagt zij aandacht voor Caribisch Nederland. In verband met deze opmerkingen adviseert de Afdeling het wetsvoorstel en de toelichting aan te passen.

1. Achtergrond en inhoud van het voorstel

Het wetsvoorstel heeft betrekking op het onderwerp 'doxing'. Dit woord is afgeleid van het Engelse 'docs' en ziet op het openbaar maken van iemands privé-informatie.¹ In het rapport 'Online ontspoord' van het Rathenau Instituut wordt doxing omschreven als 'het openbaar maken van iemands persoonlijke, sensitieve en privé-informatie zoals adres, telefoonnummer, paspoort, werkgever, gegevens van familie en foto's van iemands kinderen'.² Rond het jaar 2000 wordt voor het eerst doxing gesignaleerd, maar sinds de coronapandemie heeft dit fenomeen een vlucht genomen. Over de precieze omvang van doxing is echter nog weinig bekend.³

De redenen van mensen om aan doxing te doen, zijn niet eenduidig. Waar sommigen hieruit enkel plezier willen halen, zetten anderen doxing in als middel om politieke of maatschappelijke doelen te bereiken. Het Rathenau Instituut kwalificeert doxing als een vorm van 'digitaal vigilantisme', waarbij de drijfveer morele afkeuring en eigenrichting is. Doxing wordt schadelijk geacht omdat privé-informatie van slachtoffers online gemakkelijk misbruikt kan worden, bijvoorbeeld om iemand te bedreigen of diens werkgever lastig te vallen. Het kan bovendien leiden tot (online) zelfcensuur omdat personen bang zijn zelf slachtoffer te worden van doxing.⁴

Het wetsvoorstel beperkt zich tot doxing voor intimiderende doeleinden. Met het voorstel wordt het strafbaar om persoonsgegevens van een ander of een derde te verschaffen, verspreiden of anderszins ter beschikking stellen met het oogmerk 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. Op het misdrijf wordt een gevangenisstraf van ten hoogste een jaar of een geldboete van de derde categorie gesteld.⁵

Dit wetsvoorstel geeft uitvoering aan de breed gesteunde motie Michon-Derkzen c.s.⁶ In de motie

¹ De Van Dale geeft als omschrijving: mbt. een persoon op internet of de sociale media vertrouwelijke informatie verzamelen en publiceren over (...)

² Rathenau Instituut, *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland* (onderzoek in opdracht van het WODC), juli 2021, p. 15.

³ Rathenau Instituut, *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland* (onderzoek in opdracht van het WODC), juli 2021, p. 41.

⁴ Rathenau Instituut, *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland* (onderzoek in opdracht van het WODC), juli 2021, p. 40.

⁵ Voorgesteld artikel 285b Sr.

⁶ Kamerstukken II 2020/21, 35564, nr. 13.



wordt overwogen dat doxing in toenemende mate voorkomt richting onder meer hulpverleners, journalisten, wetenschappers en politici, en grote gevolgen heeft voor de veiligheid van deze personen.

In de toelichting bij het wetsvoorstel wordt vermeld dat doxing met intimiderende doeleinden een grote impact kan hebben op de slachtoffers en hun naasten, de groep waartoe zij behoren of de organisatie waarvoor zij werkzaam zijn. Het verspreiden van bijvoorbeeld het woonadres of de naam van de school van hun kinderen maakt de drempel lager om de slachtoffers of hun naasten fysiek te confronteren. Dit leidt ertoe dat personen vrezen voor hun eigen veiligheid en die van hun naasten, omdat zij niet kunnen voorzien hoe voor hen onbekenden met deze informatie zullen omgaan in de fysieke wereld. Daarom passen zij hun gedrag aan en voelen zij zich minder vrij in hun doen en laten.

In sommige gevallen leidt doxing daadwerkelijk tot anonieme, collectieve en gecoördineerde acties tegen het slachtoffer.⁷ Ook organisaties, en gedragszagers daarbinnen, kunnen zich door doxing gedwongen voelen om hun handelswijze aan te passen. Op die manier kan doxing met intimiderende doeleinden invloed uitoefenen op het functioneren van de democratische rechtsstaat en haar instituties.⁸

De Afdeling onderschrijft dat doxing met intimiderende doeleinden grote impact kan hebben op slachtoffers en hun naasten. Daarnaast kan doxing in bepaalde gevallen een potentiële bedreiging vormen voor het functioneren van de democratische rechtstaat. De Afdeling onderschrijft daarom de wens van de regering om te komen tot strafbaarstelling van het verspreiden of ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden. Niettemin heeft zij enkele opmerkingen over de voorgestelde strafbaarstelling.

2. Reikwijdte van de strafbaarstelling

Het wetsvoorstel heeft als doel doxing met intimiderende doeleinden strafbaar te stellen. De voorgestelde strafbaarstelling is ruim omschreven en omvat een gevarieerd palet aan situaties. In de toelichting worden voorbeelden aangehaald van politieagenten, journalisten, opiniemakers, wetenschappers, politici en bestuurders die vanwege hun werk of functie het slachtoffer van doxing worden.⁹ Deze voorbeelden zijn ook in lijn met de motie die de aanleiding vormt voor dit wetsvoorstel. In de toelichting wordt echter vermeld dat de strafbaarstelling, in tegenstelling tot in Frankrijk, niet is beperkt tot 'bepaalde beroepsgroepen of personen', omdat op voorhand niet goed is te bepalen welke beroepsgroepen hiermee zullen worden geconfronteerd en omdat het effect op slachtoffers niet samenhangt met hun beroep.¹⁰

Binnen de ruime strafbaarstelling zoals voorgesteld vallen dus situaties waarin personen niet vanwege hun ambt, beroep of maatschappelijke functie met doxing worden geïntimideerd. In de toelichting worden hiervan echter geen voorbeelden genoemd. Om beter zicht te krijgen op de situaties waar het hier om gaat, acht de Afdeling dat wel gewenst. Zij denkt hierbij aan iemand die een foto en telefoonnummer van een ex-partner op een online forum zet, een buurtbewoner die het adres van een zedendelinquent in de buurtapp rondstuurt of een slachtoffer dat de volledige naam van een verdachte in een strafzaak via sociale media verspreidt.

Het is evident dat voornoemde situaties bedreigend kunnen zijn voor de betrokkenen. De Afdeling begrijpt in dat licht gezien de wens om doxing ook in dergelijke situaties strafbaar te stellen. Deze situaties kunnen echter onderscheiden worden van situaties waarin personen geïntimideerd worden wegens hun ambt, beroep of maatschappelijke functie en die kunnen doorwerken in het functioneren van de democratische rechtsstaat en haar instituties. De strafbaarstelling van doxing in andere situaties behoeft daarom in de motivering zelfstandig aandacht. De Afdeling acht de toelichting op dit punt nog niet toereikend.

De ruime reikwijdte van de strafbepaling in het voorstel lijkt met name te zijn ingegeven doordat het moeilijk is tot afbakening te komen van beroepsgroepen die met doxing worden geconfronteerd. De Afdeling constateert dat het Wetboek van Strafrecht meer bepalingen bevat die specifiek gericht zijn op personen met een bepaald ambt, beroep of maatschappelijke functie.¹¹ Dit argument acht de Afdeling daarom niet overtuigend. Zij begrijpt het wetsvoorstel zo dat omdat doxing (ook) een bedreiging kan zijn voor personen die niet tot de in de toelichting genoemde beroepsgroepen

⁷ Toelichting, paragraaf 4.

⁸ Toelichting, paragraaf 1.

⁹ Toelichting, paragraaf 1 en 4.

¹⁰ Toelichting, paragraaf 3.

¹¹ Toelichting, paragraaf 2.1 (De verhouding tot bestaande strafbaarstellingen).

behoren, gekozen is voor een ruime strafbaarstelling.

De Afdeling adviseert in de toelichting nader in te gaan op de strafbaarstelling van doxing in gevallen waarin dit geen verband houdt met het ambt, beroep of de maatschappelijke functie van slachtoffer en hiervan voorbeelden te noemen in de toelichting.

3. Verwachte uitvoeringslasten

Gegeven de ruime strafbaarstelling zoals onder punt 2 is beschreven, is te meer van belang dat de gevolgen daarvan voor de uitvoering zorgvuldig worden gezien. De Afdeling vindt de toelichting in dat opzicht niet toereikend.

In de toelichting wordt aangegeven dat er weinig informatie is over de omvang van het fenomeen doxing in Nederland, maar dat er een toename van het gebruik van sociale media voor 'ontoelaatbare uitingen' is te zien.¹² In de uitvoeringsparagraaf wordt geconcludeerd dat de structurele gevolgen voor de uitvoering, en als gevolg daarvan de financiële consequenties, van het wetsvoorstel beperkt zullen zijn en kunnen worden opgevangen binnen de begrotingen van politie, openbaar ministerie en de rechtspraak. Dit wordt onder meer gebaseerd op de overweging dat een deel van de slachtoffers ook thans naar de politie stapt, waarbij ook nu een afweging van de strafwaardigheid moet worden gemaakt.

Verder is aangegeven dat slachtoffers ook via internettussenpersonen de gewraakte content ontoegankelijk kunnen maken. Daarnaast wordt opgemerkt dat uiterlijk twee jaar na de inwerkingtreding van de wet een invoeringstoets wordt uitgevoerd om te bezien of deze aanname van beperkte uitvoerings- en financiële gevolgen klopt.

De Afdeling acht deze toelichting onvoldoende. In algemene zin kan worden gesteld dat online criminaliteit toeneemt en complexer wordt, terwijl de digitale (opsporings)capaciteit bij politie en het OM beperkt is en onder druk staat.¹³ Dit noopt ertoe dat bij nieuwe strafbaarstellingen van (mede) in het digitaal domein gepleegde gedragingen in het bijzonder aandacht wordt besteed aan de uitvoerings- en handhavingcapaciteit. Met het wetsvoorstel wordt een strafbaarstelling geïntroduceerd waarvan het blijkens de toelichting niet alleen de bedoeling is een norm te codificeren, maar om een bepaalde gedraging daadwerkelijk aan te pakken. Ook is – zoals in punt 2 van dit advies aangegeven – gekozen voor een strafbaarstelling met een ruim toepassingsbereik. In dergelijke gevallen geldt des te meer dat zorgvuldig een schatting gemaakt dient te worden van de omvang van de problematiek, de benodigde (opsporings)capaciteit en de prioritering in relatie tot andere strafbare gedragingen. De keuze om een brede vorm van doxing strafbaar te stellen en effectief te willen handhaven leidt met de beperkt beschikbare capaciteit immers tot een lagere prioritering en minder menskracht voor andere delicten.

De Afdeling begrijpt dat een kwantitatieve inschatting van de uitvoerings- en handavingslasten voor de nieuwe strafbaarstelling lastig is te maken, maar acht in dat geval een nadere motivering op zijn plaats om tot de conclusie te komen dat deze lasten beperkt zullen zijn. Hierbij wordt ook verwezen naar het advies van het College van procureurs-generaal dat, mede na een vergelijking met het aantal zaken van belaging, vooralsnog uitgaat van 1500 zaken op jaarbasis.¹⁴ Verder gaat de toelichting maar zeer beperkt in op de benodigde capaciteit voor de nieuwe strafbaarstelling en de vraag hoe hierin wordt voorzien. In verband daarmee wordt ook niet ingegaan op de betekenis van het wetsvoorstel voor de wijze waarop de prioriteiten zullen worden gesteld, gelet op de doelstelling om ook andere vormen van (digitale) criminaliteit aan te pakken.

De Afdeling adviseert om, met inachtneming van het voorgaande, nader de uitvoerbaarheid en handhaafbaarheid van het voorstel te motiveren en daarbij in te gaan op de capaciteit en prioritering in de strafrechtketen. Ook wordt geadviseerd om, conform kabinetsbeleid,¹⁵ de invoeringstoets een jaar na inwerkingtreding van het wetsvoorstel uit te voeren.

4. Strafbarestelling van 'zich verschaffen'

De voorgestelde strafbarestelling van doxing ziet op drie gedragingen: het zich verschaffen, het

¹² Toelichting, paragrafen 1 en 6.

¹³ Kamerstukken II 2019/20, 28 684, nr. 621 en Kamerstukken II 2020/21, 26 643, nr. 768.

¹⁴ Openbaar Ministerie, 'Advies wetsvoorstel strafbarestelling gebruik persoonsgegevens voor intimiderende doeleinden', 10 augustus 2021.

¹⁵ Kamerstukken II 2020/21, 35 510, nr. 4, p. 6 en de brief van de Minister voor Rechtsbescherming van 21 april 2022 aan de Tweede Kamer over de inkleuring en stand van zaken invoeringstoets, kenmerk 3921364. Zie ook VVD, D66, CDA en ChristenUnie, 'Coalitieakkoord 2021–2025', 15 december 2021, p. 1.

verspreiden en het anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden. In de toelichting wordt uiteengezet dat onder 'zich verschaffen' gedragingen worden geschaard die zijn 'gericht op het in het bezit krijgen van de persoonsgegevens'. Hierbij wordt actief handelen verondersteld van degene die zich gegevens verschafft. Het maakt voor de strafbaarstelling niet uit of deze gegevens zelfstandig worden verzameld of worden verkregen van derden. Indien gegevens via een derde worden verkregen, kan er volgens de toelichting ook overlap zijn met het verspreiden of anderszins ter beschikking stellen van persoonsgegevens. Als voorbeeld wordt genoemd dat iemand via sociale media oproept tot het delen van persoonsgegevens en daarbij zelf ook persoonsgegevens verspreidt.¹⁶

Het bestanddeel 'zich verschaffen' geeft een ruime reikwijdte aan de strafbaarstelling. Een enkele zoekopdracht via een internetzoekmachine lijkt voldoende te zijn om te spreken van (een poging tot) het zich verschaffen van persoonsgegevens. Als deze gedraging én het oogmerk bewezen kunnen worden, is iemand strafbaar.¹⁷ Het verzamelen van persoonsgegevens hoeft dus niet op wederrechtelijke wijze plaats te vinden, zoals bij diefstal¹⁸ of hacken¹⁹ het geval is. De informatie die wordt verkregen, hoeft naar haar aard evenmin strafwaardig te zijn.²⁰ Zoals in de toelichting wordt erkend, dient het strafrecht te worden ingezet als ultimum remedium.²¹ Uit de toelichting blijkt in dat licht bezien onvoldoende waarom de voorgestelde delictsomschrijving zich ook uitstrekt tot het enkel 'zich verschaffen' van persoonsgegevens.

De Afdeling neemt daarbij in aanmerking dat de kern van het strafbare verwijt bij doxing betrekking heeft op het verspreiden van persoonsgegevens. Pas als iemand kenbaar maakt dat hij een persoonsgegeven zoekt, in bezit heeft of met anderen deelt, kunnen de schadelijke gevolgen optreden die de wetgever beoogt te voorkomen met dit wetsvoorstel. In de toelichting wordt opgemerkt dat dergelijke gedragingen in een aantal gevallen al onder bestaande strafbaarstellingen vallen.²² In de overige gevallen zullen de gedragingen kunnen worden aangemerkt als 'verspreiden' of 'anderszins ter beschikking stellen' in de zin van de voorgestelde strafbaarstelling van doxing. Het opnemen van het delictsbestanddeel 'zich verschaffen' in deze strafbepaling draagt dus niet (direct) bij aan het doel van het wetsvoorstel.

In de afweging die gemaakt moet worden is ook de te verwachten bewijsproblematiek van belang. In de toelichting wordt erkend dat het geheel zelfstandig verzamelen van gegevens, bijvoorbeeld door te zoeken op internet, vrijwel niet op te sporen is. Tevens wordt erkend dat het oogmerk in dat geval waarschijnlijk 'niet eenvoudig' te bewijzen zal zijn.²³ Ook in de consultatiereacties wordt opgemerkt dat het oogmerk moeilijk te bewijzen zal zijn als de verdachte enkel persoonsgegevens verzameld heeft en deze vervolgens niet verspreidt.²⁴ Deze bewijsrechtelijke problematiek roept eens te meer de vraag op waarom het 'zich verschaffen' in de delictsomschrijving wordt opgenomen.

Gelet op het doel van het wetsvoorstel en de te verwachten bewijsproblematiek ziet de Afdeling onvoldoende meerwaarde van het opnemen van het bestanddeel 'zich verschaffen' in de strafbaarstelling van doxing. De Afdeling adviseert daarom hiervan af te zien en dit onderdeel van het voorstel te schrappen.

Als 'zich verschaffen' niet wordt opgenomen in de delictsomschrijving, wordt deze beperkt tot de handelingen 'verspreiden' en 'anderszins ter beschikking stellen'. Hoewel de Afdeling meent dat hiermee ook de situatie kan worden ondervangen waarin iemand oproept tot het delen van persoonsgegevens,²⁵ kan zij zich voorstellen dat het wenselijk is om expliciet tot uitdrukking te brengen dat een dergelijke oproep strafbaar is gelet op de intimiderende werking die daarvan uit kan gaan. De Afdeling adviseert daarom de delictsomschrijving aan te vullen in de zin dat het verspreiden of anderszins ter beschikking stellen van persoonsgegevens, of het daartoe aanzetten, strafbaar is.

¹⁶ Toelichting bij artikel I, eerste lid.

¹⁷ Toelichting, paragraaf 2.1 (De verhouding tot bestaande strafbaarstellingen) en bij artikel I, eerste lid. Zie Advies Raad voor de rechtspraak (15 september 2021), p. 2–3.

¹⁸ Artikel 310 Sr e.v.

¹⁹ Artikel 138ab Sr.

²⁰ Zie bijvoorbeeld vervalste documenten (artikel 226 lid 2 Sr), kinderporno (artikel 240b Sr) of instructiemateriaal ten behoeve van het plegen van terroristische misdrijven (artikel 134a Sr).

²¹ Toelichting, paragraaf 2.3.

²² Toelichting, paragraaf 2.1 (De verhouding tot bestaande strafbaarstellingen).

²³ Toelichting bij Artikel I, eerste lid.

²⁴ Advies Raad voor de rechtspraak (15 september 2021), p. 2–3; advies Nederlandse Orde van Advocaten (2 september 2021), p. 5–6.

²⁵ Met deelnemingsvormen uitlokken, doen plegen en medeplegen en voorbereidingshandelingen zou het oproepen tot het delen van persoonsgegevens ook binnen het bereik van doxing kunnen worden gebracht. In de toelichting wordt niet op deze deelnemingsvormen ingegaan. Daarnaast kan gedacht worden aan andere strafbaarstellingen, zoals opruiing en bedreiging, waar een dergelijke oproep onder kan vallen.

5. Strafuitsluitingsgrond

Het tweede lid van het voorgestelde artikel 285d voorziet in een strafuitsluitingsgrond. Op basis van dit lid is iemand niet strafbaar als deze te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de persoonsgegevens vereiste. In de toelichting wordt uiteengezet dat deze strafuitsluitingsgrond is bedoeld voor journalisten, klokkenluiders en anderen die bijvoorbeeld maatschappelijke misstanden aan de kaak willen stellen. In dit verband wordt ook gewezen op onder andere artikel 7 van de Grondwet en artikel 10 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).²⁶

De Afdeling deelt de opvatting dat het verzamelen en verspreiden van persoonsgegevens niet strafbaar zou moeten zijn als iemand te goeder trouw aanneemt dat dit in het algemeen belang is. Dit laat onverlet dat de noodzaak van de bijzondere strafuitsluitingsgrond bij deze strafbaarstelling onvoldoende is aangetoond.²⁷ Op basis van de voorgestelde strafbaarstelling in het eerste lid dient iemand immers het oogmerk te hebben om een ander vrees aan te jagen, ernstig overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen. Als iemand te goeder trouw en met het oog op het algemeen belang persoonsgegevens verzamelt of verspreidt, zal niet voldaan zijn aan dit oogmerk en is doxing dus niet strafbaar. De rechter komt dan dus niet toe aan de toetsing van de strafuitsluitingsgrond in het tweede lid.

Hierin zit een belangrijk verschil met de andere strafbepalingen waarin een vergelijkbare strafuitsluitingsgrond is opgenomen en waar in de toelichting naar wordt verwezen.²⁸ Het betreft de delicten inzake het verwerven of openbaar maken van niet-openbare gegevens die afkomstig zijn uit een misdrijf,²⁹ smaad,³⁰ en schending van bedrijfsgeheimen.³¹ Deze bepalingen omvatten geen oogmerk dat vergelijkbaar is met het voorgestelde oogmerk bij doxing. Deze delicten kunnen dus bewezen worden verklaard terwijl de verdachte te goeder trouw en met het oog op het algemeen belang de informatie heeft verzameld of verspreid. De goedwillende journalist, klokkenluider of blogger heeft de bescherming van deze strafuitsluitingsgrond in die gevallen dus nodig om vrijuit te gaan. Voor het delict doxing geldt dit niet.

De strafuitsluitingsgrond kan de strafbepaling compliceren in die gevallen waarin niet eenduidig is wat de bedoeling van verdachte is geweest. In de toelichting wordt niet ingegaan op situaties waarin de motieven van de verdachte diffuus zijn. Sommige activisten gebruiken bijvoorbeeld intimiderende methodes, maar handelen wel uit een oprechte bezorgdheid over problemen in de samenleving. Moet de intentie van de activist dan worden behandeld in het licht van het oogmerk als bedoeld in het voorgestelde eerste lid of in het licht van de strafuitsluitingsgrond van het tweede lid? In dat laatste geval zou dit tot de situatie kunnen leiden dat de rechter vaststelt dat iemand handelde met het oogmerk een ander te intimideren, maar dat dit niet verwijtbaar is omdat iemand te goeder trouw en in het algemeen belang handelde. Intimidatie van personen, door middel van het verspreiden van persoonsgegevens, is in een dergelijk geval wellicht (onbedoeld) toch toegestaan. Dit lijkt op gespannen voet te staan met het doel van het wetsvoorstel.

In het licht van het voorgaande adviseert de Afdeling de strafuitsluitingsgrond in het tweede lid te schrappen. De positie van journalisten, klokkenluiders en goedwillende anderen kan voldoende worden gewaarborgd bij de toetsing van het oogmerk als bedoeld in het eerste lid. In de toelichting zou dit benadrukt kunnen worden, zodat hier bij de toepassing van het voorgestelde wetsartikel in de praktijk geen twijfel over kan bestaan.

6. Weergave internetconsultatiereacties

De toelichting bij het wetsvoorstel bevat een paragraaf waarin wordt ingegaan op adviezen en consultatiereacties op een concept van het wetsvoorstel. Daarin wordt een weergave gegeven van opmerkingen van partijen die anders dan via de internetconsultatie hun visie hebben gegeven op het concept. Voor de reacties op de internetconsultatie en de respons daarop vanuit de regering wordt verwezen naar een verslag op de website van internetconsultatie.

Met het oog op de transparantie van het wetgevingsproces is het wenselijk dat in de toelichting bij een

²⁶ Toelichting, paragraaf 2.4 en bij Artikel I, tweede lid.

²⁷ Zie ook de adviezen van de Nederlandse Orde van Advocaten, de AP en het Openbaar Ministerie. De Raad voor de rechtspraak heeft juist begrip voor dit tweede lid, 'om twijfel te voorkomen'.

²⁸ Zie ook advies Openbaar Ministerie (10 augustus 2021), p. 11–12.

²⁹ Artikel 139g Sr.

³⁰ Artikel 261 Sr.

³¹ Artikel 273 Sr.



wetsvoorstel aandacht wordt besteed aan de opbrengst van een internetconsultatie en de verwerking daarvan in het wetsvoorstel of de toelichting. Dit is ook in lijn met het kabinetsbeleid op dit punt³² en de Aanwijzingen voor de regelgeving.³³

De Afdeling adviseert in de toelichting de via internetconsultatie binnengekomen opmerkingen en de reactie daarop vanuit de regering weer te geven.

7. Caribisch Nederland

Het wetsvoorstel regelt een nieuwe strafbaarstelling voor Europees Nederland en Caribisch Nederland. Een concept van het wetsvoorstel is onder meer naar de openbare lichamen in Caribisch Nederland en de Commissie toezicht bescherming persoonsgegevens BES ter consultatie gestuurd. Het Bestuurscollege van Bonaire heeft in reactie op de consultatie aangegeven dat het Korps Politie Caribisch Nederland en het openbaar ministerie BES positief hebben gereageerd op het wetsvoorstel. Daarbij is vermeld dat het goed is dat Caribisch Nederland qua strafrechtelijk instrumentarium niet achterblijft bij Europees Nederland.

In de toelichting wordt niet ingegaan op de problematiek van doxing in Caribisch Nederland, eventueel in vergelijking met de in de toelichting beschreven probleemschets in Europees Nederland. Er wordt dus ook niet stilgestaan bij de vraag of de lokale context aldaar in enige mate relevant is voor de voorgestelde strafbaarstelling of de handhaving daarvan.

Ook worden in de toelichting niet de relevante artikelen in het Wetboek van Strafrecht BES en het Wetboek van Strafvordering BES vermeld, zoals dat wel is gedaan voor bespreking van de overlap in strafbaarstellingen in Europees Nederland. Deze artikelen zijn grotendeels gebaseerd op de Europees Nederlandse equivalenten, maar zijn niet volledig gelijk.³⁴ Daarnaast lijkt het ten behoeve van de kenbaarheid van de strafbaarstelling in Caribisch Nederland wenselijk om in het opschrift expliciet te benoemen dat dit wetsvoorstel het Wetboek van Strafrecht BES en Wetboek van Strafvordering BES wijzigt.³⁵

De Afdeling adviseert in de toelichting in te gaan op de strafbaarstelling van doxing in Caribisch Nederland, in de toelichting de relevante artikelen van het Wetboek van Strafrecht BES en Wetboek van Strafvordering BES te vermelden en in het opschrift aan te geven dat het wetsvoorstel deze wetboeken wijzigt.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

*De vice-president van de Raad van State,
Th.C. de Graaf.*

³² Onder meer beschreven in Kamerstukken II 2010/11, 29 279, nr. 121, p. 2 en Kamerstukken II 2016/17, 33 009, nr. 39, p. 3–5.

³³ Aanwijzing 4.44, eerste lid, van de Aanwijzingen voor de regelgeving.

³⁴ Zie bijvoorbeeld enerzijds 285 Sr en anderzijds 298 Sr BES, op grond waarvan bedreiging waarbij 'gemeen gevaar voor de verlening van diensten ontstaat' strafbaar is gesteld in Europees Nederland, maar niet in Caribisch Nederland. Ook kan gewezen op enerzijds artikel 318 Sr en anderzijds artikel 331 Sr BES, op grond waarvan in Europees Nederland sprake kan zijn van afdreiging indien wordt gedwongen tot het ter beschikking stellen van gegevens, hetgeen in Caribisch Nederland niet onder de strafbepaling valt.

³⁵ Dit geldt temeer omdat het wetsvoorstel niet een groot aantal regelingen wijzigt in de zin van Ar 4.3, op grond waarvan in het opschrift kan worden volstaan met een vermelding van de belangrijkste regeling(en) indien de regeling tot wijziging van een groot aantal regelingen strekt.



Tekst zoals toegezonden aan de Raad van State: Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering en enige andere wetten 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)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden strafbaar te stellen;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

Na artikel 285c van het Wetboek van Strafrecht wordt een artikel ingevoegd, luidende:

Artikel 285d

1. Degene die zich persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk 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 te laten hinderen, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.
2. Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de gegevens, bedoeld in het eerste lid, vereiste.

ARTIKEL II

Na artikel 298a van het Wetboek van Strafrecht BES wordt een artikel ingevoegd, luidende:

Artikel 298b

1. Degene die zich persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk 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 door te laten hinderen, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.
2. Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de gegevens, bedoeld in het eerste lid, vereiste.

ARTIKEL III

In artikel 67, eerste lid, van het Wetboek van Strafvordering wordt in onderdeel b na '285c, ' ingevoegd '285d, '.

ARTIKEL IV

In artikel 100, eerste lid, van het Wetboek van Strafvordering BES wordt in onderdeel b na '298, eerste lid, ' ingevoegd '298b, '.

ARTIKEL V

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

De Minister van Justitie en Veiligheid,



MEMORIE VAN TOELICHTING

I. Algemeen deel

1. Inleiding

Het is betrekkelijk eenvoudig om via internetbronnen persoonlijke informatie van individuele personen te achterhalen. Enige basiskennis van het internet volstaat om via een zoekopdracht persoonsgegevens boven water te krijgen. De publieke toegankelijkheid van het internet en de bereikbaarheid van anderen door middel van sociale media bieden kwaadwillenden de mogelijkheid om deze persoonsgegevens te gebruiken om mensen vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in hun dagelijks leven. Dit kan leiden tot gedragingen die een dusdanige inbreuk op iemands persoonlijke levenssfeer maken dat deze gedragingen naar de huidige in de maatschappij levende opvattingen als uiterst onwenselijk en strafwaardig worden gezien. Een onwenselijke en strafwaardige gedraging is het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden, een gedraging die nauw aansluit bij dat wat wordt aangeduid als doxing (ook wel: *doxxing*). Met dit wetsvoorstel wordt uitvoering gegeven aan de motie die de regering verzoekt om doxing strafbaar te stellen (Kamerstukken II 2020/21, 35 564, nr. 13).

In opdracht van het WODC heeft het Rathenau Instituut onderzoek verricht naar schadelijk en immoreel gedrag online. Het rapport getiteld *Online ontspoord*¹ bevat de uitkomsten van onderzoek naar de aard en de omvang van online schadelijk en immoreel gedrag in Nederland, de onderliggende mechanismen en oorzaken, en de handelingsperspectieven voor de overheid voor het beperken van schadelijk en immoreel gedrag op internet. De fenomenen die binnen het bereik van het onderzoek vallen, zijn ondergebracht in zes categorieën (online informatie manipulatie, digitaal vigilantisme, online haat, online pesterij en geweld, cyberbedrag en online zelfbeschadiging) en in totaal 22 fenomenen van schadelijk en immoreel gedrag online, 17 onderliggende mechanismen en een agenda voor de overheid aan de hand van vier strategische thema's. In het rapport van het Rathenau Instituut wordt het fenomeen doxing belicht als onderdeel van de categorie digitaal vigilantisme oftewel digitale eigenrichting. Het begrip doxing wordt omschreven als het openbaar maken van iemands persoonlijke, sensitieve en privé-informatie zoals adres, telefoonnummer, paspoort, werkgever, gegevens van familie en foto's van iemands kinderen. Opgemerkt wordt dat doxing juridisch complex is. In de wetenschappelijke literatuur zijn er weinig internationale, empirische studies gevonden over doxing – laat staan over de omvang van het fenomeen in Nederland. Doxing wordt sinds begin jaren 2000 gesignaleerd. Tijdens de coronapandemie is het fenomeen een stuk zichtbaarder geworden.

Doxing met als doel een bepaald persoon te intimideren kan grote impact hebben op de beoogde slachtoffers en hun naasten, op de groep waartoe zij behoren of van wie wordt verondersteld dat zij daartoe behoren, of op de organisatie waarvoor zij werkzaam zijn. Het slachtofferschap is daarbij niet voorbehouden aan bepaalde groepen: eenieder kan ermee te maken krijgen. Het gevolg is dat personen vrezen voor hun eigen veiligheid en die van hun naasten en niet meer zichzelf durven te zijn, of dat organisaties, en gezagsdragers daarbinnen, zich gedwongen voelen hun handelwijze aan te passen. Het ontregelende karakter van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden heeft op die manier, direct of indirect, tevens invloed op het functioneren van onze democratische rechtsstaat en de instituties die daarvan deel uitmaken.

De gevolgen van doxing in de fysieke wereld zijn uiteenlopend van aard. Onlangs is in de nationale media aandacht geschonken aan gevallen van doxing waarbij persoonsgegevens werden gebruikt voor intimiderende doeleinden, en aan de effecten daarvan op slachtoffers. Zo vonden mensen die actief zijn op het online berichtenplatform Twitter en daar een progressief politiek geluid laten horen een sticker van 'Vizier op Links' op hun voordeur en werden zij slachtoffer van online treitercampagnes. Ook politieagenten, opiniemakers, journalisten en politici hebben in toenemende mate te maken met online intimidatie en bedreiging. Uit de jaarcijfers GTPA (Geweld Tegen Politie Ambtenaren) komt een stijging van het aantal online intimiderende uitingen gericht tot politieambtenaren naar voren.² Zo is een tijd lang getracht om de identiteit van undercoveragenten te onthullen. Het is de wens van de politie om het fenomeen doxing strafbaar te stellen. Door de strafbaarstelling kan de politie in een eerder stadium van (ervaren) bedreiging haar strafvorderlijke bevoegdheden inzetten en sneller optreden. Daarnaast wil de politie – als werkgever – ook met het uiten van deze wens een signaal

¹ *Online ontspoord* – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen).

² <https://www.politie.nl/binaries/content/assets/politie/onderwerpen/geweld-tegen-politieambtenaren/gtpa-cijfers-2017-tot-en-met-2020.pdf>

afgegeven dat dit in haar ogen normoverschrijdend gedrag is. Doxing heeft voor de politie als organisatie een grote impact op medewerkers (weerbaarheid en inzetbaarheid).

De politie heeft in haar advies opgemerkt dat het online delen van dergelijke berichten en persoonsgegevens tot een groot en snel bereik leidt. Dit betekent dat ook een podium is ontstaan voor kwaadwillenden die vaak anoniem escaleren met uitingen van een soms zeer intimiderend karakter. Met dergelijke (oproepen tot) inbreuken op de persoonlijke levenssfeer genereert men ernstige dreigingen of zelfs daaruit voortvloeiende incidenten. De politie constateert een toename van de omvang van dit fenomeen. Daarmee zijn ook de ernst, impact en de gevolgen hiervan meer zichtbaar geworden. Doxing heeft zich volgens de politie ontwikkeld tot een (digitale) klopjacht naar en het online publiceren en onderling delen van zeer persoonlijke gegevens van anderen.

De politie ziet dat doxing uiteenlopende groepen slachtoffers kent. Zo werden uit onvrede met het vaccinatiebeleid tijdens de coronacrisis in Telegramgroepen rondom de 'avondklokrellen' lijsten met namen en adresgegevens geopenbaard van leden van de Tweede Kamer en van medewerkers van het RIVM en van de GGD die werkzaam zijn op priklocaties. In chatgroepen werden oproepen gedaan om persoonsgegevens zoals een woonadres te achterhalen van overheidsfunctionarissen, journalisten en wetenschappers, bestuurders en politici, of van medewerkers van bepaalde bedrijven. Deze gegevens werden vervolgens via sociale media verder verspreid, veelal gecombineerd met het plaatsen van een herkenbare foto, en een oproep om de betrokkene thuis een bezoek te brengen. Ook is het voorgekomen dat op sociale media door personen die zich intimiderend uitlaten richting een burgemeester een oproep werd gedaan om bij zijn ambtswoning op een bepaald tijdstip 'koffie te gaan drinken'.³

De bovenbeschreven uitingsvormen die zich niet concreet openbaren in bijvoorbeeld bedreiging, belediging en dwang zijn niet altijd te kwalificeren als een strafbaar feit. Dit terwijl de consequenties ervan voor het leven en het welzijn van de betrokkenen ernstig kunnen zijn. Slachtoffers worden geïntimideerd en voelen zich niet meer veilig in hun dagelijkse omgeving. Dit kan ertoe leiden dat zij zich gedwongen voelen zich anders te gedragen en niet meer naar buiten durven te treden, noch in de fysieke wereld, noch online. Deze ontwikkeling is zeer kwalijk. De vrijheid van meningsuiting mag niet worden gebruikt om de grondrechten en persoonlijke vrijheden van anderen aan te tasten. De overheid kan niet tolereren dat persoonsgegevens van burgers worden verspreid met het doel anderen vrees aan te jagen of ernstige overlast aan te doen. Daarom wordt voorgesteld het gebruik van persoonsgegevens voor intimiderende doeleinden zelfstandig strafbaar te stellen. Hiermee wordt een duidelijke norm gesteld: het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens met het doel een ander te intimideren (hierna ook: strafbare doxing) is onacceptabel en wordt onder de reikwijdte van de strafwet gebracht. Daarbij is niet van belang of de gedragingen al dan niet online plaatsvinden.

2. Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden

2.1 De verhouding tot bestaande strafbbaarstellingen

Strafbaar wordt gesteld het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde met het oogmerk 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 te laten hinderen. Hiermee wordt beoogd de persoonlijke vrijheid te beschermen. Het voorgestelde strafbaar te stellen gedrag – het gebruik van persoonsgegevens voor intimiderende doeleinden of strafbare doxing – brengt immers tweevoudig dat slachtoffers zich niet meer vrij voelen in hun dagelijkse doen en laten vanwege de vrees dat hen iets ernstigs zal worden aangedaan of vanwege het gevoel dat zij hebben dat hen iets ernstigs zal kunnen worden aangedaan vanwege de dreiging die van de beschikbaarheid van persoonsgegevens bij kwaadwillenden uit kan gaan. De terughoudendheid waar dit bij het slachtoffer toe kan leiden kan zich zowel in zijn privésfeer openbaren als het professioneel handelen raken. Bij personen die vanwege hun (publieke) functie slachtoffer worden van strafbare doxing, kan dit tot gevolg hebben dat zij zowel in de privésfeer als in de uitoefening van hun beroep consequenties ervaren. Voor de strafbaarheid is essentieel dat de gedragingen zijn gericht op het aanjagen van vrees, het veroorzaken van ernstige overlast voor de betrokkene of het ernstig hinderen in de uitoefening van zijn ambt of beroep.

Hoewel onder omstandigheden sprake kan zijn van overlap met reeds strafbare gedragingen, zoals belaging, bedreiging of (ambts)dwang, is dat zeker niet altijd het geval. Voor strafbare bedreiging (artikel 285 Sr) is vereist dat iemand wordt bedreigd met bepaalde ernstige misdrijven. De dader van dit delict kan worden bestraft met gevangenisstraf van ten hoogste twee jaren. De wet van 4 novem-

³ 'Razzia bij Moeke, Nijmegen. Personeel meegenomen voor verhoor. De nieuwe 'wet' staat dit echter niet toe. Bruls begaat een misdrijf in zijn rol als mini-dictator. Wederom ambtsmisdrijf. Morgen koffie drinken bij de ambtswoning.'

ber 2021 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering en enige andere wetten in verband met versterking van de strafrechtelijke aanpak van ondermijnende criminaliteit (Stb. 2021, 544) verhoogt dit strafmaximum tot drie jaar gevangenisstraf, waarbij een extra strafverhogingsgrond geldt voor de bedreiging van ambts-, gezags- en togadragers, journalisten en publicisten, ambtenaren van politie en buitengewoon opsporingsambtenaren. Voor strafbare doxing is evenwel niet vereist dat het slachtoffer wordt bedreigd met een bepaald ernstig misdrijf. Voor strafbare belaging (artikel 285b Sr) is vereist dat opzettelijk inbreuk wordt gemaakt op de persoonlijke levenssfeer van een ander met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen. De dader van dit delict kan worden gestraft met gevangenisstraf van ten hoogste drie jaren. Hoewel het voor belaging vereiste oogmerk deels overeenkomt met dat voor strafbare doxing, namelijk voor zover het gaat om het oogmerk de ander vrees aan te jagen, betreft het andersoortige gedragingen. Een belangrijk verschil is dat het bij belaging gaat om het herhaaldelijk – stelselmatig – lastigvallen van een bepaald persoon waardoor een inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkene, het gaat bijvoorbeeld om het voortdurend achtervolgen of steeds berichten sturen. Bij strafbare doxing ligt het zwaartepunt wat betreft de strafwaardigheid niet in de stelselmatigheid van de inbreuk op de persoonlijke levenssfeer maar in de ernst van de inbreuk op de persoonlijke levenssfeer, die het gevolg is van het gebruik van persoonsgegevens om een ander vrees aan te (laten) jagen dan wel ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de uitoefening van ambt of beroep. Het eenmalig zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens is – als wordt voldaan aan de overige delictsbestanddelen – voldoende voor strafbaarheid.

In het geval het slachtoffer door een ander wordt gedwongen iets te doen, niet te doen of te dulden kan er sprake zijn van dwang. Voor strafbare dwang (artikel 284 Sr) is vereist dat het slachtoffer door geweld of enige andere feitelijkheid of door bedreiging met geweld of enige andere feitelijkheid, gericht tegen het slachtoffer of een derde, of door bedreiging met smaad of smaadschrift wordt gedwongen iets te doen, niet te doen of te dulden. Als een ambtenaar, bijvoorbeeld een ambtenaar van politie, wordt gedwongen tot het volvoeren van een ambtsverrichting of het nalaten van een rechtmatige ambtsverrichting, kan dit kwalificeren als ambtsdwang (artikel 179 Sr). De dader van dit delict kan worden gestraft met gevangenisstraf van ten hoogste vier jaren. Dwang gericht op de afgifte van een goed, tot het aangaan van een schuld, het teniet doen van een inschuld of het ter beschikking stellen van gegevens is strafbaar als afpersing als dit gebeurt door middel van geweld of bedreiging met geweld (artikel 317 Sr) of afdreiging als dit gebeurt door bedreiging met smaad, smaadschrift of openbaring van een geheim (artikel 318 Sr), waarvoor de dader kan worden gestraft met gevangenisstraf van ten hoogste negen respectievelijk vier jaren. Voor strafbaarheid wegens dwang, ambtsdwang, afdreiging of afpersing is vereist dat het slachtoffer ergens toe wordt gedwongen.⁴ De voorgestelde strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden onderscheidt zich van deze strafbaarstellingen doordat strafrechtelijke aansprakelijkheid reeds ontstaat bij het oogmerk dat de dader heeft bij het zich verschaffen, verspreiden of anderszins ter beschikking stellen van gegevens. Daarmee beoogt hij om het slachtoffer 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. Ook als het slachtoffer (nog) niet is gedwongen tot een bepaald handelen of nalaten, zal er sprake kunnen zijn van strafbare doxing als de dader heeft gehandeld met voormeld oogmerk. Kenmerk van de strafbaarstelling is dat de bovenbeschreven gedragingen strafbaar worden gesteld ongeacht het resultaat ervan; het gebruik van persoonsgegevens voor intimiderende doeleinden is een formeel omschreven delict.

Als in het openbaar persoonsgegevens worden gepubliceerd met een oproep om tegen het openbaar gezag een strafbaar feit te plegen, is dit strafbaar als opruiing (artikel 131 Sr). Voor strafbare opruiing is vereist dat in het openbaar wordt opgeruid tot enig strafbaar feit of tot gewelddadig optreden tegen het openbaar gezag. De dader van dit delict kan worden gestraft met gevangenisstraf van ten hoogste vijf jaren. Hoewel het oproepen tot het plegen van een strafbaar feit tegen iemand een manier kan zijn om die ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de uitoefening van zijn ambt of beroep, is dit voor strafbaarheid wegens het gebruik van persoonsgegevens voor intimiderende doeleinden niet vereist. Het gebruik van persoonsgegevens voor intimiderende doeleinden betreft dan ook geen vorm van opruiing. In situaties waarin sprake is van zowel opruiing als van gebruik van persoonsgegevens voor intimiderende doeleinden is het aan

⁴ Zie bijvoorbeeld rechtbank Rotterdam 28 januari 2021 (ECLI:NL:RBROT:2021:547) waarin een veroordeling wegens poging tot ambtsdwang is uitgesproken in een zaak waarin de verdachten een foto van twee undercoveragenten op Twitter hadden geplaatst met daarbij onder andere de tekst 'meer dan 1100 mensen hebben naar deze foto gekeken, straks met andere foto's worden de undercoveragents bekend in heel NL'. De rechtbank oordeelde dat de verdachten hiermee willens en wetens de aanmerkelijke kans hebben aanvaard dat de identiteit van de undercoveragenten zou kunnen worden achterhaald dan wel onthuld en dat zij hierdoor gedwongen konden worden hun (undercover)werkzaamheden na te laten. Dat agenten van wie de identiteit publiek gemaakt is geen undercoverwerkzaamheden meer kunnen verrichten, achtte de rechtbank dermate evident, dat de verdachte dit heeft geweten.

het openbaar ministerie om te beslissen of vervolging wordt ingesteld en welk specifieke strafbare verwijt de dader wordt gemaakt. In voorkomende gevallen lijkt het, vanwege de ernst van de gedraging en de strafbedreiging, echter aangewezen dat een verdachte die anderen heeft opgeroepen een strafbaar feit te plegen tegen het openbaar gezag primair wordt vervolgd vanwege opruiing.

Als de persoonsgegevens die voor intimiderende doeleinden worden gebruikt zijn verkregen door middel van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk, en het vervolgens overnemen, aftappen of opnemen van de gegevens, dan is tevens sprake van computervredebreuk (artikel 138ab Sr). De dader van computervredebreuk kan worden gestraft met gevangenisstraf van ten hoogste vier jaren. Uit het eerdergenoemde rapport 'Online ontspoord' komt echter naar voren dat voor doxing vaak informatie wordt gebruikt die openbaar online beschikbaar is, zonder dat opzettelijk en wederrechtelijk een computer wordt binnengedrongen ('hacken'). Verwezen wordt naar het voorbeeld dat iemand zijn werkgever op LinkedIn heeft vermeld. Dit kan in combinatie met informatie uit andere publieke bronnen gebruikt worden voor een haatcampagne. In relatie tot het misdrijf computervredebreuk onderscheidt de voorgestelde strafbaarstelling zich doordat strafrechtelijke aansprakelijkheid vanwege het zich verschaffen van persoonsgegevens voor intimiderende doeleinden ontstaat zonder dat sprake is van het hacken van een computer om deze gegevens te verkrijgen. Voor strafbaarheid wegens het verspreiden of anderszins ter beschikking stellen van dergelijke gegevens voor intimiderende doeleinden is de wijze van verkrijging van deze gegevens niet relevant. Evenwel ligt strafvervolging terzake van computervredebreuk voor de hand als sprake is van hacken.

2.2 De noodzaak van strafbaarstelling

Het gebruik van persoonsgegevens voor intimiderende doeleinden wordt strafbaar gesteld omdat bestaande strafbaarstellingen niet altijd toereikend zijn terwijl strafrechtelijk optreden wel wenselijk is. Vanwege de mate van impact van strafbare doxing op de slachtoffers, de inbreuk op fundamentele rechten van burgers en de invloed op het functioneren van onze democratische rechtsstaat en de instituties die daarvan deel uitmaken, is een zelfstandige strafbaarstelling noodzakelijk. Deze strafbaarstelling voorziet in een aanvulling op de bestaande strafbaarstellingen, en is bedoeld voor de situaties waarin de bestaande strafbaarstellingen tekortschieten voor de strafrechtelijke bescherming van burgers die slachtoffer zijn van het gebruik van persoonsgegevens voor intimiderende doeleinden. Dit kan aan de hand van een voorbeeld worden geïllustreerd. In de inleiding is melding gemaakt van het in chatgroepen oproepen om persoonsgegevens te achterhalen van overheidsfunctionarissen, journalisten en wetenschappers, bestuurders en politici, of van medewerkers van bepaalde bedrijven, om deze gegevens vervolgens via sociale media verder te verspreiden met een oproep om de betrokkene thuis een bezoek te brengen. Dergelijk handelen levert geen strafbare bedreiging op, omdat er geen sprake is van bedreiging met een bepaald ernstig misdrijf, als bedoeld in het eerste lid van artikel 285 Sr. Dergelijk handelen levert geen strafbare belaging op, omdat er geen sprake is van het stelselmatig lastigvallen van het slachtoffer waardoor een inbreuk wordt gemaakt op diens persoonlijke levenssfeer. Dergelijk handelen levert geen strafbare dwang op, omdat er geen sprake is van het met geweld of enige andere feitelijkheid of door bedreiging met geweld of enige andere feitelijkheid, of door bedreiging met smaad of smaadschrift dwingen van het slachtoffer om iets te doen, niet te doen of te dulden. Er is evenmin sprake van strafbare opruiing, omdat niet in het openbaar wordt opgeruid tot enig strafbaar feit of tot gewelddadig optreden tegen het openbaar gezag. Met de voorgestelde strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden wordt in deze lacune voorzien.

Het openbaar ministerie kan op basis van het opportuniteitsbeginsel een strafrechtelijk onderzoek starten naar aanleiding van een verdenking van strafbare doxing. Doorgaans zal dit na een melding of aangifte van het slachtoffer zijn. Een klacht van het slachtoffer is echter niet vereist. Dan zou het slachtoffer, dat mogelijk vreest voor zijn of andermans veiligheid of vrijheid, altijd de beslissing moeten nemen of hij het wenselijk acht dat de dader wordt vervolgd. Voorkomen moet worden dat het slachtoffer voor een dergelijke keuze wordt gesteld. Bij strafbare doxing gaat het om een gevaarzettingsdelict, waarvoor geldt dat de samenleving er als geheel belang bij heeft dat hiertegen kan worden opgetreden. Dit is anders dan bijvoorbeeld bij belaging (artikel 285b Sr) waarbij er een relatie kan zijn tussen slachtoffer en dader, en waarbij het persoonlijke belang van het slachtoffer niet te worden geconfronteerd met eventuele negatieve gevolgen van een strafvervolging zwaarder kan wegen dan het algemene belang van strafvervolging. Bij strafbare doxing kan het algemeen belang in het bijzonder strekken tot strafvervolging als persoonsgegevens van grote groepen gelijktijdig worden verspreid (bijvoorbeeld een 'vijandelijke lijst') of als de intimidatie van het slachtoffer samenhangt met de functie die hij uitoefent en de intimidatie daardoor tevens gevolgen kan hebben voor het functioneren van een beroepsgroep of een organisatie als geheel.

Bij het begaan van de strafbaar gestelde gedragingen zal veelal gebruik worden gemaakt van het internet, meer bepaald van sociale media en online berichtendiensten. De snelheid waarmee het internet en sociale media veranderen, maakt het voor het strafrechtelijk onderzoek noodzakelijk om

relevante informatie zo snel mogelijk vast te leggen. Dit vraagt deels om een andere aanpak van de opsporing dan bij gedragingen in de fysieke wereld. Ook het identificeren van verdachten vraagt om een andere inzet van opsporing. Door het gebruik van persoonsgegevens voor intimiderende doeleinden aan te merken als een feit waarvoor voorlopige hechtenis is toegelaten, komen extra opsporingsbevoegdheden beschikbaar. Berichten op internet en sociale media worden vaak onder een accountnaam of «nickname» geplaatst. Voor het achterhalen van het IP-adres van de plaatser en de bijbehorende metadata moeten bij een aanbieder verkeersgegevens kunnen worden gevorderd, gericht op het identificeren van de plaatser. Voor het opsporingsonderzoek is vastlegging van de volgende informatie van belang: de accountnaam en bijbehorend IP-adres waar het bericht mee is geplaatst, de periode waarin het bericht online heeft gestaan, de plaatsingsdatum van het bericht, de datum waarop het bericht is vastgelegd ten behoeve van het proces-verbaal en de samenhang en context van het bericht. Voor het vorderen van verkeersgegevens is vereist de verdenking van een misdrijf als bedoeld in artikel 67, eerste lid, Sv (artikel 126n/u Sv). Belangrijk is dat persoonsgegevens die online zijn geplaatst zo snel mogelijk kunnen worden verwijderd, om te voorkomen dat deze gegevens door anderen worden bewaard, gebruikt of verder verspreid. In situaties waarin de desbetreffende persoonsgegevens nog niet zijn verwijderd via zelfregulering van IT-bedrijven, bijvoorbeeld doordat de partij die de gegevens beheert niet is aangesloten bij de Notice and Take Down (NTD) gedragscode (zie ook paragraaf 2.3), kan de officier van justitie met een machtiging van de rechter-commissaris, die enkel wordt afgegeven ingeval van verdenking van een strafbaar feit als bedoeld in artikel 67, eerste lid, Sv, bevelen om gegevens ontoegankelijk te maken (artikel 125p Sv). De rechtbank kan vervolgens gelasten dat de ontoegankelijk gemaakte gegevens worden vernietigd indien het gegevens betreft met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan, voor zover de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten (artikel 354, eerste en tweede lid, Sv).

Voor politie en openbaar ministerie wordt het met een op de specifieke gedraging toegesneden strafbaarstelling mogelijk om het gebruik van persoonsgegevens voor intimiderende doeleinden gericht op te sporen, te vervolgen en te bewijzen.

2.3 Het belang van preventieve en niet-strafrechtelijke maatregelen

Bij de aanpak van strafbare doxing is het noodzakelijk om eerst en vooral in te zetten op andere (preventieve) maatregelen. Daarvoor is de inzet van partners buiten het domein van justitie en veiligheid essentieel.

In het eerdergenoemde rapport 'Online ontspoord' worden vier strategische thema's geïdentificeerd waarop de Rijksoverheid een sturende, coördinerende en faciliterende rol kan vervullen. Het thema 'Herinrichting van de online omgeving' bevat handvatten voor de Rijksoverheid om de mechanismen die kenmerkend zijn voor het internet ten goede te keren. Het thema 'Verhelderen van online normen' formuleert aanbevelingen om maatschappelijke afspraken over normen en waarden online te vernieuwen. Het thema 'Mensen beschermen en slachtoffers bijstaan' bevat suggesties voor de Rijksoverheid en haar uitvoeringsinstanties om beter te reageren op schadelijk en immoreel gedrag online en de schade daarvan. Het thema 'Adaptief vermogen versterken' bevat suggesties voor de Rijksoverheid om grip te krijgen en te houden op schadelijk en immoreel gedrag online dat continu in beweging is, en is gericht op het toekomstbestendig maken van de strategische agenda. Zo kan de Rijksoverheid in samenwerking met actoren uit de markt en maatschappij, schadelijk en immoreel gedrag online aanpakken en een veilige online omgeving bevorderen. Mogelijke concrete initiatieven die in het rapport worden genoemd zijn de oprichting van een nationaal meldpunt waar slachtoffers van online immoreel en schadelijk gedrag terecht kunnen, het bevorderen van de ontwikkeling van onderzoeksprogramma's en samenwerking met onderzoeksinstituten om de mechanismen en fenomenen beter te doorgronden en slachtoffers en daders beter in beeld te krijgen, en het coördineren van de samenwerking tussen toezichthouders om het toezicht op fenomenen en mechanismen van schadelijk en immoreel gedrag online te versterken en verbeteren. De aanpak van schadelijk en immoreel onlinegedrag verdient aandacht. Daarom verken ik de mogelijkheden tot het vergroten van de bewustwording en het weten hoe te handelen, het ontwikkelen van een beoordelingskader voor online normstelling, het inrichten van een infrastructuur voor het melden en ontoegankelijk maken van illegale content. Voor preventief niet strafrechtelijk optreden kan ook worden gedacht aan bewustwordings- en voorlichtingscampagnes.

Tussenpersonen als hosting providers en online platformen zijn in beginsel niet strafbaar op grond van het voorgestelde artikel 285d als strafbare doxing plaatsvindt via hun netwerk of platform. Wel hebben zij een verantwoordelijkheid om op te treden indien zij ervan op de hoogte zijn dat op hun platformen of servers strafbare of onrechtmatige content staat. Indien zij niet adequaat optreden kunnen ze civielrechtelijk of strafrechtelijk aansprakelijk worden gesteld. De NTD-gedragscode bevat heldere afspraken over hoe te handelen bij meldingen van onrechtmatige en strafbare inhoud op internet. Het deelnemen van tussenpersonen aan deze gedragscode dient om in een dergelijk geval snel de geëigende maatregelen te kunnen nemen. De nieuwe strafbaarstelling kan behulpzaam zijn in deze procedure omdat hiermee het verboden karakter van het gebruik van persoonsgegevens voor

intimiderende doeleinden tot uitdrukking wordt gebracht. In de gevallen waarin de NTD-gedragscodes niet afdoende is voor de verwijdering van de gegevens, bijvoorbeeld omdat verschil van inzicht bestaat over de onrechtmatigheid van de berichten, of wanneer sprake is van een aanbieder die de gedragscodes niet heeft ondertekend, staat eveneens de gang naar de civiele rechter open. Het slachtoffer kan een dergelijke civiele procedure starten. Dan kan het offline halen van de onrechtmatige content worden gevorderd en/of de NAW-gegevens van degene die de gewraakte content online heeft geplaatst. Indien bekend is wie dit is, kan het slachtoffer een civiele procedure tegen diegene starten en een schadevergoeding eisen.

In aanvulling hierop kan het strafrechtelijk optreden van meerwaarde zijn. Dit optreden is gericht op degene die door het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens bij de ander vrees wil (laten) teweegbrengen, hem ernstige overlast wil (laten) aandoen of ernstig wil (laten) hinderen in de uitoefening van zijn ambt of beroep. Het strafrecht is en blijft het ultimum remedium. In minder ernstige gevallen van strafbare doxing, waarbij het slachtoffer bijvoorbeeld vooral wil dat berichten worden verwijderd, kan een andere, niet-strafrechtelijke procedure aangewezen zijn om het laakbare gedrag te beëindigen, de dreiging weg te nemen en de dader op zijn gedrag aan te spreken.

2.4 Uitzonderingsgrond

Het samenbrengen en publiceren van persoonsgegevens kan een gerechtvaardigd belang opleveren, bijvoorbeeld wanneer de intentie van de openbaarmaking is gelegen in het aan de kaak stellen van misstanden. Het deelnemen aan het maatschappelijk debat, waarbij wordt gereageerd op andermans stellingen en posities, kan slechts binnen het bereik van de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden vallen indien persoonsgegevens worden verschaft, verspreid of ter beschikking gesteld en degene die dit doet 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 te laten hinderen. Bij het geven van een mening over een bepaald onderwerp zal daarvan geen sprake zijn. Bij dit soort publicaties zal er dan ook geen sprake zijn van een oogmerk in de zin van het eerste lid van het voorgestelde artikel 285d, zodat er geen strafbare gedraging is. Om hierover iedere twijfel uit te sluiten is aanvullend een expliciete strafuitsluitingsgrond opgenomen. In het tweede lid van het voorgestelde artikel 285d is vastgelegd dat niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de persoonsgegevens vereiste. Met deze strafuitsluitingsgrond wordt aangesloten bij soortgelijke bepalingen in het Wetboek van Strafrecht (artikelen 139g, tweede lid, en 273, tweede lid, Sr). Dit wetsvoorstel belet daarmee journalisten, klokkenluiders en anderen op geen enkele wijze om nieuwsfeiten en misstanden openbaar te maken. Voorwaarde voor het van toepassing zijn van deze strafuitsluitingsgrond is dat te goeder trouw wordt gehandeld, dat wil zeggen dat de betrokkene niet het oogmerk heeft tot het aanjagen van vrees en er overigens in redelijkheid van mocht uitgaan dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de gegevens, bedoeld in het eerste lid, vereiste. Journalisten kunnen in beginsel niet op basis van de hun door artikel 10 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) gegeven bescherming worden ontslagen van hun verplichting de door de strafwet getrokken grenzen in acht te nemen. Het door artikel 10 EVRM gewaarborgde recht op vrijheid van meningsuiting kan echter dwingen tot het maken van een uitzondering op dit uitgangspunt. Daarbij dient de ernst van de inbreuk op de rechtsorde door overtreding van de strafrechtelijke norm, gelet op het belang van het geschonden voorschrift, te worden afgewogen tegen het maatschappelijk belang van openbaarmaking, het daadwerkelijke nadeel dat door de openbaarmaking is ontstaan en de mate waarin de openbaarmaking daadwerkelijk op andere wijze had kunnen worden voorbereid (HR 26 maart 2013, LJN BY3752).⁵ Aldus wordt bereikt dat bij de beslissing of vervolging moet worden ingesteld en bij de beslissing van de rechter of van strafbaarheid sprake is, op basis van een expliciete bepaling rekening kan worden gehouden met conflicterende belangen: aan de ene kant het recht op een vrije nieuwsgaring en aan de andere kant het recht op bescherming van de persoonlijke levenssfeer van burgers.

3. De situatie in andere landen

Strafwaardige gedragingen die samenhangen met doxing zijn geen typisch Nederlands verschijnsel. Ook andere landen, zowel binnen als buiten Europa, worden ermee geconfronteerd. In verschillende landen zijn initiatieven genomen om gedragingen strafbaar te stellen, waarbij de strekking en reikwijdte van de betreffende strafbepalingen per land verschillen. Zo is recent in Duitsland een wetsvoorstel in consultatie gebracht om de verspreiding van zogenoemde ‘vijandelijke lijsten’ tegen te

⁵ Zie voor de toetsing van proportionaliteit en subsidiariteit in dit kader ook de uitspraak van de Rechtbank Oost-Brabant van 15 februari 2013, ECLI:NL:ROBR:2013:BZ115.

gaan.⁶ Met dit conceptwetsvoorstel zou strafbaar worden gesteld de verspreiding van persoonsgegevens van een ander op een manier die geschikt is om die ander of een persoon in zijn nabijheid in gevaar te brengen door het plegen van een strafbaar feit of een onrechtmatige daad. In Frankrijk is op 25 mei 2021 de Wet nr. 2021-646 van 25 mei 2021 op de algemene veiligheid uitgevaardigd. Deze wet voorziet onder meer in strafbaarstelling van het creëren van computerbestanden voor kwaadaardige identificatiedoeleinden van ambtenaren. Ook in verschillende staten van de Verenigde Staten zijn vormen van doxing strafbaar gesteld of voorstellen daartoe gedaan.⁷

De strafbaarstellingen in deze landen hebben gemeen dat zij steeds betrekking hebben op het verspreiden en/of verzamelen van persoonsgegevens. De overige voorwaarden verschillen per land. De in dit wetsvoorstel opgenomen strafbaarstelling vergt voor strafbaarheid een bepaald oogmerk bij de dader. Het oogmerk dient te zijn gericht op het (laten) aanjagen van vrees, het (laten) aandoen van ernstige overlast of het ernstig (laten) hinderen van de uitoefening van ambt of beroep. In tegenstelling tot bijvoorbeeld Frankrijk is niet gekozen voor een beperking tot bepaalde beroepsgroepen of personen, omdat op voorhand niet goed is te bepalen welke beroepsgroepen hiermee zullen worden geconfronteerd en omdat het effect op slachtoffers niet noodzakelijkwijs samenhangt met het beroep dat zij beoefenen. Wel is hiermee rekening gehouden in de formulering van het vereiste oogmerk, door hierin expliciet op te nemen 'het ernstig hinderen in de uitoefening van ambt of beroep'. Als bijvoorbeeld persoonsgegevens van politieambtenaren worden verspreid dan is degene die de gegevens verspreid strafbaar indien hij hiermee beoogt die politieambtenaren ernstig te hinderen in het uitoefenen van de functie.

4. Verhouding met fundamentele rechten

De strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden impliceert een beperking van de vrijheid van meningsuiting. De vrijheid van meningsuiting wordt gewaarborgd in artikel 7 van de Grondwet en in artikel 10 EVRM. Op grond van artikel 10 EVRM heeft eenieder recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van een zwaarwegend maatschappelijk belang, zoals het voorkomen van wanordelijkheden en strafbare feiten of de bescherming van de goede naam of de rechten van anderen. Artikel 10, eerste lid, EVRM heeft ook betrekking op uitingen op internet.⁸ Op grond van artikel 7 van de Grondwet heeft niemand voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet. Bij dit laatste kan worden gedacht aan de mogelijkheid van veroordeling wegens een strafbaar feit als smaad of laster (artikelen 261 en 268 Sr).

De vrijheid van meningsuiting is geen absoluut recht. Zoals hierboven aangegeven, kan dit grondrecht worden beperkt in het belang van een zwaarwegend maatschappelijk belang, en ieders verantwoordelijkheid voor de wet.

Op grond van de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) is een bij de wet voorziene beperking van de vrijheid van meningsuiting niet in strijd met artikel 10 EVRM indien zij een gerechtvaardigd doel dient als genoemd in het tweede lid van deze verdragsbepaling en zij noodzakelijk is in een democratische samenleving, bij de beoordeling waarvan aan de nationale autoriteiten een zekere beoordelingsmarge ('margin of appreciation') toekomt. De noodzaak tot de inzet van een bevoegdheid waarmee dit recht kan worden beperkt, wordt mede bepaald aan de hand van de beginselen van proportionaliteit en subsidiariteit.

De in dit wetsvoorstel voorgestelde strafbaarstelling voldoet aan deze eisen. De eis dat de inmenging bij de wet is voorzien, houdt in dat de regeling daarvan is opgenomen in het nationale recht ('prescribed by law') en dat deze voor de burger voorzienbaar moet zijn. Dit brengt met zich mee dat de regeling voldoende precies moet zijn geformuleerd en dat zij waarborgen biedt tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger. Met het oog op deze eis kan worden vooropgesteld dat de inmengingen in het privéleven welke bij de vigerende strafbaarstellingen die tegen doxing kunnen worden ingezet alsook bij de voorgestelde strafbaarstelling aan de orde zijn, en de voorwaarden en waarborgen die daarbij aan de orde zijn, worden omschreven in de wet en

⁶ Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Verbesserung des strafrechtlichen Schutzes gegen sogenannte Feindeslisten (Drucksache 19/28678).

⁷ Waaronder Alabama, Colorado, Oklahoma en Utah.

⁸ EHRM 1 december 2015, Cengiz e.a. t. Turkije, nrs. 48226/10 en 14027/11, ECLI:CE:ECHR:2015:1201JUD004822610. Zie ook EHRM 18 december 2012, Ahmet Yildirim t. Turkije, nr. 3111/10, ECLI:CE:ECHR:2012:1218JUD000311110 en EHRM 18 oktober 2005, Perrin t. Verenigd Koninkrijk, nr. 5446/03, ECLI:CE:ECHR:2005:1018DEC000544603.

dit wetsvoorstel. Met de voorgestelde strafbaarstelling wordt een maatschappelijke norm gesteld waardoor voor burgers duidelijk is dat deze gedragingen onacceptabel zijn en zij hun gedrag hierop kunnen afstemmen. De rechten van verdachten worden gewaarborgd door de waarborgen die de strafrechtelijke procedure biedt. De beslissing over de strafbaarheid van een verdachte en over de op te leggen straf of maatregel is voorbehouden aan een onafhankelijke rechter. Daarbij gelden de nodige waarborgen voor de verdachte, zoals de onschuldpresumptie, het recht op bijstand van een raadsman en de mogelijkheid van het instellen van rechtsmiddelen tegen een veroordelend vonnis. Aldus is voldaan aan de eis dat de wettelijke regeling voldoende precies is en dat zij een zorgvuldige toepassing waarborgt. Artikel 7 van de Grondwet gaat in dit opzicht overigens verder, maar ook aan de door het eerste lid gestelde eisen – geen voorafgaand verlot, uitsluitend wet in formele zin – voldoet de voorgestelde regeling.

Voor de beoordeling of een beperking van de vrijheid van meningsuiting noodzakelijk is in een democratische samenleving, is van belang of daartoe een dringende maatschappelijke noodzaak ('pressing social need') bestaat. In het onderhavige geval is die maatschappelijke noodzaak gelegen in de ingrijpende en schadelijke effecten die het strafbare doxing kan hebben op het persoonlijke leven van slachtoffers. In de eerste plaats betreft dit een rechtstreekse aantasting van het veiligheidsgevoel. Slachtoffers maken melding van het online delen van hun adres, het kenteken van hun auto, de route en tijden waarop zij met hun hond wandelen, de sportvereniging van hun kinderen en zelfs de koosnamen van hun geliefden. Het verspreiden van deze gegevens onder onbekenden maakt ernstig inbreuk op het veiligheidsgevoel van de slachtoffers, omdat zij niet kunnen voorzien tot welke gevolgen dit zal leiden in de fysieke wereld, en vormt een ernstige inbreuk op hun persoonlijke levenssfeer. In de tweede plaats leidt strafbare doxing vaak tot anonieme, collectieve en gecoördineerde acties richting het slachtoffer, louter om het feit dat het slachtoffer behoort tot een bepaalde (beroeps)groep. In situaties waarbij de werkomgeving van het slachtoffer gevaar met zich brengt, kan dit het persoonlijke leven van het slachtoffer raken. Bij collectieve gecoördineerde acties kan ook sprake zijn van het aanspreken van een klaarblijkelijk willekeurig uitgekozen individu als representant van een (beroeps)groep als geheel of vanwege het vervullen van een bepaalde maatschappelijke rol. In de derde plaats treft strafbare doxing niet alleen de slachtoffers zelf, maar ook de personen in hun directe omgeving. Daardoor is het voor hen vaak lastig om het risico in te schatten dat zij – of iemand in hun naaste omgeving – worden geconfronteerd met strafbare feiten, ernstige overlast of ernstige hinder in de uitoefening van hun beroep en waarvoor ze in een dergelijk geval dienen te vrezen. Dit wordt nog versterkt als de persoonsgegevens zijn verspreid binnen een grote groep (bijvoorbeeld door het delen ervan in een app-groep of op sociale media), waardoor door slachtoffers noch door de politie kan worden ingeschat wie met behulp van die gegevens wanneer welke actie zou kunnen ondernemen. Met de voorgestelde strafbaarstelling wordt een strafrechtelijke norm gesteld die tot uitdrukking brengt dat een grens wordt overschreden bij het gebruik van persoonsgegevens voor intimiderende doeleinden, gezien de ernstige inbreuk op het persoonlijk leven van slachtoffers. Het gebruik van de vrijheid van meningsuiting mag geen instrument zijn om met kwaadwillende bedoelingen de vrijheid van een ander te beperken. Eenieder heeft immers ook recht op eerbiediging van zijn persoonlijke levenssfeer, zoals gewaarborgd in artikel 8 EVRM en artikel 10 van de Grondwet. Behalve dat de voorgestelde strafbaarstelling in het licht van artikel 10 EVRM noodzakelijk moet zijn in een democratische samenleving moet de met de strafbaarstelling gepaarde inbreuk op dit verdragsartikel proportioneel zijn aan het nagestreefde doel. Hierboven is reeds ingegaan op de noodzaak van de strafbaarstelling, in aanvulling op preventieve en niet-strafrechtelijke maatregelen en bestaande strafbaarstellingen voor gedragingen die raakvlakken hebben met de strafbare doxing. De staat komt een rol toe bij het reguleren van het maatschappelijk verkeer, en het beschermen van burgers tegen de aantasting van hun rechten en vrijheden, waar nodig ook door het stellen van duidelijke normen die raken aan de uitoefening van de vrijheid van meningsuiting. Hierbij past een zorgvuldige afweging over de wijze waarop aan de interventie door de overheid invulling wordt gegeven om het evenwicht in de bescherming van de betrokken belangen te waarborgen. Daarbij geeft het EHRM de nationale staten als gezegd een zekere beoordelingsvrijheid. Er is alle reden om aan te nemen dat de afweging die aan dit wetsvoorstel ten grondslag ligt, binnen de kaders valt die het EHRM in het kader van artikel 10 EVRM heeft gesteld en zou kunnen stellen. De voorgestelde strafbaarstelling is proportioneel omdat deze niet verder gaat dan strikt noodzakelijk; de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden is beperkt tot gevallen waarin het oogmerk aanwezig is om een ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de uitoefening van ambt of beroep. Hierbij is tevens van belang dat het wetsvoorstel geen afbreuk beoogt te doen aan de positie van journalisten en de bescherming van de persvrijheid, mede gebaseerd op artikel 7 van de Grondwet. Dit is in paragraaf 2.4 aan de orde gekomen. Voorts geldt dat het met deze strafbaarstelling beoogde doel niet kan worden bereikt met een andere maatregel die minder ingrijpend is voor de grondrechten van burgers. Zoals hiervoor in deze toelichting is uiteengezet kan onder omstandigheden sprake kan van overlap met reeds strafbare gedragingen. Niettemin is het gebruik van persoonsgegevens voor intimiderende doeleinden op dit moment zeker niet in alle gevallen waarin daaraan dringend behoefte bestaat, strafbaar. De mogelijkheid van de inzet van het

strafrecht is daarbij wenselijk voor gevallen waarin het gedrag dermate laakbaar is dat strafrechtelijk optreden is geïndiceerd.

5. Adviezen

Het conceptwetsvoorstel is in consultatie gegeven aan het College van procureurs-generaal (tevens in Caribisch Nederland), de politie (tevens in Caribisch Nederland), de Nederlandse Orde van Advocaten, de Raad voor de rechtspraak (tevens in Caribisch Nederland), de Nederlandse Vereniging voor Rechtspraak, de Autoriteit persoonsgegevens, de Commissie toezicht bescherming persoonsgegevens BES, de Nederlandse Vereniging van Journalisten en de openbare lichamen in Caribisch Nederland.

Over het conceptwetsvoorstel is advies ontvangen van het College van procureurs-generaal, de korpschef van de politie, de Nederlandse Orde van Advocaten (NOvA), de Raad voor de rechtspraak (Rvdr), de Autoriteit persoonsgegevens (AP), de Commissie toezicht bescherming persoonsgegevens BES (CBP BES), de Nederlandse Vereniging voor Rechtspraak (NVvR) en de Nederlandse Vereniging van Journalisten (NVJ) en de openbare lichamen in Caribisch Nederland. Het CBP BES en de openbare lichamen in Caribisch Nederland hebben geadviseerd over de voorgestelde strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden binnen de grenzen van de openbare lichamen Bonaire, Sint Eustatius en Saba, door middel van wijziging van het Wetboek van Strafrecht BES en het Wetboek van Strafvordering BES. Daarnaast is het conceptwetsvoorstel op internet gepubliceerd (www.internetconsultatie.nl) zodat een ieder in de gelegenheid is gesteld hierop te reageren. Een aantal respondenten heeft hiervan gebruik gemaakt om aan te geven dat de noodzaak van dit wetsvoorstel wordt herkend omdat dit aansluit bij de maatschappelijke ontwikkelingen.

Hieronder wordt de inhoud van de adviezen op hoofdlijnen besproken. Voor de inhoud van de reacties op de internetconsultatie en de verwerking daarvan wordt verwezen naar het verslag van de internetconsultatie.

** Het College van procureurs-generaal*

Het College schaart zich achter de (in de motie benoemde) wens van de politie om doxing als zodanig strafbaar te stellen in het Wetboek van Strafrecht. Wel vraagt het College aandacht voor de grote spoed waarmee het wetsvoorstel wordt vervaardigd. In dit verband wijst het College in het bijzonder op het eerdergenoemde rapport van het Rathenau instituut, getiteld Online ontspoord, en pleit het voor een bredere benadering van doxing in het licht van andere te nemen maatregelen tegen schadelijk en immoreel onlinegedrag. Naar aanleiding van dit pleidooi van het College wordt opgemerkt dat het Rathenau onderzoek een verkennend, exploratief onderzoek betreft met een breed onderzoeksveld over schadelijk en immoreel gedrag in relatie tot het internet. In het rapport ligt de nadruk op beschrijving, inventarisatie en het formuleren van thema's en opgaven om meer gericht actie te ondernemen tegen ontsporingen en moreel en wenselijk gedrag te bevorderen. Het fenomeen doxing moet inderdaad worden gezien in samenhang met andere fenomenen die zijn te scharen onder de noemer van schadelijk en immoreel onlinegedrag. In paragraaf 2.3 zijn enkele relevante actielijnen benoemd. Met deze strafbaarstelling wordt de norm gesteld dat het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden onacceptabel is en daarom onder de reikwijdte van de strafwet wordt gebracht. Gelet op de aard en opzet van voornoemd onderzoek, lijkt het weinig waarschijnlijk dat er met het huidige voorstel voor strafbaarstelling van persoonsgegevens voor intimiderende doeleinden wegen worden ingeslagen die niet aansluiten op latere beleids- of wetgevingsinitiatieven.

Het College benadrukt het ultimum remedium-karakter van het strafrecht omdat maatschappelijke problemen niet in de eerste plaats worden opgelost door het strafrecht. Het College meent dat nader uitgelegd dient te worden aan welke preventieve niet-strafrechtelijke maatregelen wordt gedacht en welke gevallen van doxing zich lenen voor deze aangestipte andere niet strafrechtelijke maatregelen. Naar aanleiding van dit advies is in de toelichting een nieuwe paragraaf 2.3 opgenomen, waarin wordt ingegaan op het belang van preventieve en niet-strafrechtelijke maatregelen.

Verder maakt het College enkele inhoudelijke opmerkingen over de begrippen 'doxing' en 'identificerende persoonsgegevens', de verhouding tussen het zich verschaffen en het verspreiden van persoonsgegevens, het bewijs van het oogmerk en de uitzonderingsgrond van het tweede lid. Naar aanleiding van deze opmerkingen is de toelichting op het voorgestelde artikel 285d, eerste lid en tweede lid, aangevuld. Overigens is het begrip 'identificerende persoonsgegevens', zoals in de reactie op het advies van de AP aan de orde zal komen, gewijzigd in 'persoonsgegevens'.

** De politie*

De korpschef van de politie constateert met instemming dat wordt voorgesteld de politie de mogelijk-

heid te bieden tot een al langer bepleite strafrechtelijke aanpak van doxing. Als maatschappelijk fenomeen uit doxing zich in verschillende verschijningsvormen. De politie ziet een groeiende ontwikkeling van het (oproepen tot) het verzamelen, delen en/of gebruiken van privégegevens van anderen met kennelijk als doel op die wijze hun doen en laten te beïnvloeden. Dit baart de politie grote zorgen die de korpschef eerder dit jaar heeft kenbaar gemaakt. De politie hecht vanuit een daadkrachtig strafrechtelijk optreden aan een heldere, handhaafbare strafbepaling, die de genoemde ernstige gevallen binnen de reikwijdte van het Wetboek van Strafrecht brengen en afbakenen van overige delicten. Het huidige ontwerp biedt met de gekozen vormgeving volgens de politie goede aanknopingspunten.

De politie geeft in overweging het voorstel aan te vullen met een strafverzwaringsgrond voor de gevallen dat doxing zich richt tegen de publieke functionaris gedurende of in verband met de uitoefening van zijn ambt of beroep. Daarbij gaat de korpschef er in ieder geval van uit dat ook voor de strafbedreiging van doxing de bestaande strafvorderingsrichtlijnen en landelijke afspraken ten aanzien van de opsporing en vervolging conform het beleid Veilige Publieke Taak (VPT) van toepassing worden, met een verhoogde strafeis bij vervolging van doxing gericht tegen een publieke functionaris gedurende of in verband met de uitoefening van zijn ambt of beroep. Naar aanleiding van dit advies wordt opgemerkt dat is gebleken dat niet alleen publieke functionarissen slachtoffer worden van strafbare doxing. Deze gedragingen worden ook gericht tegen anderen, zoals journalisten, winkeliers en sporters. Daarom heb ik niet gekozen voor een strafverzwaringsgrond die beperkt is tot bepaalde beroepsgroepen. Daarbij geldt dat het voorgestelde strafmaximum naar mijn mening voldoende toereikend is voor de bijzondere kwalijke verschijningsvormen zoals strafbare doxing die zich richt tegen publieke functionarissen gedurende of in verband met de uitoefening van ambt of beroep. In de strafvorderingsrichtlijnen van het openbaar ministerie is reeds vastgelegd dat de strafeis met 200% wordt verhoogd bij incidenten van agressie en geweld tegen werknemers met een publieke taak – conform het beleid Veilige Publieke Taak – en andere functionarissen werkzaam in het publieke domein (zie paragraaf 6 van de Aanwijzing kader voor strafvordering meerderjarigen (2019A003)).

De politie adviseert de term persoonsgegevens in de memorie van toelichting duidelijk en toekomstbestendig toe te lichten, en aan de vermelding van de accountnaam ook het bijbehorend ID-nummer toe te voegen. Aan dit advies is gevolg gegeven, hiervoor wordt verwezen naar de toelichting op het voorgestelde artikel 285d, eerste lid.

Daarnaast adviseert de politie in de memorie van toelichting te verduidelijken in welke gevallen sprake is van een voltooid delict, en daarbij ook de strafbare poging en de deelnemingsvormen zoals uitlokking op te nemen. Naar aanleiding van dit advies is de toelichting op het voorgestelde artikel 285d, eerste lid, aangevuld.

Tenslotte is het advies in de memorie van toelichting helder af te bakenen wat de reikwijdte is van de termen klokkenluiders en journalisten. Dit advies is niet overgenomen omdat met een nadere inkadering van deze begrippen ten onrechte de indruk zou worden gewekt dat uitsluitend journalisten en klokkenluiders een beroep kunnen doen op de in het tweede lid voorgestelde strafuitsluitingsgrond. Deze uitsluitingsgrond is echter van toepassing op degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het strafbaar gestelde handelen vereiste; dit kan ook een publicist, blogger, vlogger of influencer zijn.

** De Nederlandse Orde van Advocaten*

De NOvA adviseert een nadere afweging te maken van de noodzaak om tot deze strafbaarstelling te komen, waarvoor de onderbouwing volgens de NOvA te summier is, en een nadere toelichting te geven met betrekking tot de reikwijdte van een aantal delictsbestanddelen en deze zo nodig aan te passen in verband met de voorzienbaarheid van strafbaar gedrag. De NOvA merkt op dat in de toelichting ten onrechte geen aandacht wordt geschonken aan de overlap met bijvoorbeeld computervredebreuk (artikel 138ab Sr). Die vergelijking dient wel te worden gemaakt omdat privéadressen veelal niet op de voor het publiek toegankelijke websites te vinden zijn. Mede gelet op de strafbaarstelling van belaging (art. 285b Sr) blijkt een grote mate van overlap met de bestaande strafbare feiten, hetgeen de vraag rechtvaardigt voor welke gevallen een aparte strafbaarstelling noodzakelijk is. Het gegeven dat voorlopige hechtenis mogelijk is in combinatie met de opmerking dat het strafrecht echter het ultimum remedium is en blijft vraagt om een nadere motivering van de noodzaak van de voorgestelde strafbepaling. Naar aanleiding van deze opmerkingen is in paragraaf 2.2 de noodzaak van de strafbaarstelling nader toegelicht, in aanvulling op de bestaande strafbaarstellingen zoals de belaging en de computervredebreuk.

Ten aanzien van de reikwijdte en voorzienbaarheid acht de NOvA de strafbaarstelling minder duidelijk. Dit betreft onderdelen als het 'zich verschaffen' in combinatie met het oogmerk, de precieze meerwaarde van de uitzonderingsgrond voor journalisten en klokkenluiders in het voorgestelde tweede lid

en het onderscheid tussen 'een ander' en 'een derde'. Naar aanleiding van deze opmerkingen zijn de verschillende onderdelen van de strafbaarstelling verhelderd in de toelichting op het voorgestelde artikel 285d, eerste en tweede lid.

** De Raad voor de rechtspraak*

De Rvdr onderkent het belang van het wetsvoorstel. De Rvdr heeft geen zwaarwegende bezwaren tegen het wetsvoorstel, maar geeft in overweging om de noodzaak voor het wetsvoorstel nader te onderbouwen en het wetsvoorstel op enkele onderdelen te verduidelijken en toe te lichten.

De Rvdr acht een verdere toelichting van de noodzaak van het wetsvoorstel wenselijk omdat de toelichting geen inzicht biedt in de vraag of zich situaties hebben voorgedaan waarvoor de bestaande strafbaarstellingen ontoereikend waren, geen voorbeelden worden genoemd waaruit de toegevoegde waarde van de nieuwe strafbaarstelling blijkt en opgemerkt wordt dat bij de aanpak van doxing eerst en vooral moet worden ingezet op andere maatregelen. Naar aanleiding van deze opmerking is in de inleiding nader ingegaan op de noodzaak van strafbaarstelling, in aanvulling op de bestaande strafbaarstellingen, en zijn de nieuwe paragrafen 2.2 en 2.3 opgenomen, waarin wordt ingegaan op respectievelijk de noodzaak van strafbaarstelling en het belang van preventie / strafrecht als ultimum remedium.

Bij de term 'zich verschaffen' dringt zich bij de Rvdr de vraag op welke gedragingen hier precies onder vallen, wat de noodzaak is van strafbaarstelling daarvan en hoe eventueel het voor strafbaarheid vereiste oogmerk uit de context kan worden afgeleid. De vraag rijst of, en zo ja, waarom ook het zich verschaffen van persoonsgegevens strafbaar wordt gesteld en hoe de wetgever de mogelijkheden ziet om het bewijs van het oogmerk op dit punt uit de context af te leiden. Deze vragen hebben geleid tot aanvulling van de toelichting op het voorgestelde artikel 285, eerste lid.

Met betrekking tot het aanjagen van vrees wordt de vraag opgeworpen of het voor de hand ligt van de emotie van de – meer geobjectiveerde – normale mens uit te gaan in plaats van te beoordelen of de persoon in kwestie (de ander) vrees zou worden aangejaagd. Ook mist de Rvdr in de toelichting een verduidelijking waar de vrees betrekking op moet hebben. Verder vraagt de Rvdr naar de precieze inhoud van de begrippen 'ernstige overlast' en 'ernstige hinder', en het onderscheid tussen ernstige overlast of hinder en overlast of hinder. Hierbij is ook de vraag aan de orde of de persoon die de hinder of overlast ondervindt of moet ondervinden bij deze beoordeling moet worden betrokken of dat – meer geobjectiveerd – moet worden beoordeeld wat de gevolgen voor 'ieder normaal mens' zouden zijn. Voorts verzoekt de Rvdr om verduidelijking van de begrippen 'een ander' en een 'derde'. Tenslotte beveelt de Rvdr aan om in de toelichting aandacht te besteden aan de poging tot overtreding van het voorgestelde artikel 285d en aan de verschillende deelnemingsvormen.

Naar aanleiding van de vragen en opmerkingen van de Rvdr is de toelichting op het voorgestelde artikel, 285d, eerste lid, aangevuld.

** De Nederlandse Vereniging voor Rechtspraak*

De NVvR meent dat er van strafbaarstelling pas sprake hoort te zijn als door het gebruik van de gegevens gevreesd mag worden dat het in de memorie van toelichting bedoelde (zeer) belastende gedrag zal gaan optreden, en vraagt zich af of deze materie binnen de grenzen van het strafrecht moet worden gebracht. Het zou naar het oordeel van de NVvR steeds (ten minste) moeten gaan om het verzamelen/verspreiden van gegevens die in redelijkheid de in de toelichting bedoelde vrees kunnen oproepen. De NVvR adviseert daarom de bestaande uitgangspunten te verduidelijken en scherper dan tot nu toe de grenzen aan te geven van deze nieuwe strafbepaling. Naar aanleiding van dit advies zijn de grenzen van de voorgestelde strafbepaling in de toelichting verduidelijkt. Hierbij moet worden opgemerkt dat strafbaarheid ontstaat door het handelen (verzamelen, verspreiden of anderszins ter beschikking stellen) met persoonsgegevens, gekoppeld aan het oogmerk van het aanjagen van vrees of het (laten) aandoen van ernstige overlast of ernstige hinder. De overlast of hinder moet van zodanige aard zijn dat het slachtoffer hierdoor redelijkerwijs kan worden geacht ernstige overlast aan te worden gedaan of in de uitoefening van zijn ambt of beroep ernstig te worden gehinderd. Dit is uiteindelijk aan de rechter ter beoordeling.

Naar aanleiding van de uitnodiging van de NVvR om te onderbouwen dat strafbare doxing vaak leidt tot anonieme, collectieve en gecoördineerde acties richting het slachtoffer, louter omdat deze behoort tot een bepaalde beroepsgroep, wijs ik op de in de inleiding aangehaalde voorbeelden van intimidatie van burgemeesters, journalisten en politieambtenaren. En ook artsen hebben te maken gekregen met intimidatie vanwege hun adviezen inzake de aanpak van het COVID-19 virus.

Verder vraagt de NVvR om verduidelijking van een volzin in paragraaf 4 die luidt als volgt: 'In het

huidige maatschappelijke klimaat waarin sprake is van verharding van de uitingen op internet, eist de democratische samenleving dat terughoudend wordt omgegaan met de vrijheid van meningsuiting als met die uitingen angst wordt aangejaagd aan anderen.' Met deze zin is beoogd tot uitdrukking te brengen dat de bescherming van het grondrecht van de vrijheid van meningsuiting niet ten koste mag gaan van de bescherming van andere (grond)rechten, zoals de bescherming van de persoonlijke levenssfeer. Overigens is de tekst van paragraaf 4 na de consultatie herzien; daarbij is de betreffende zin geschrapt.

De NVvR wijst erop dat het voorbeeld van het gooien van een vuurwerkbom in de tuin al strafbaar is op grond van de artikelen 157 Sr (het opzettelijk veroorzaken van een ontploffing, waardoor gemeen gevaar voor goederen ontstaat) of 350 Sr (vernietiging/beschadiging) en/of de Wet Wapens en Munitie. Naar aanleiding hiervan wordt opgemerkt dat het desbetreffende voorbeeld is geschrapt.

De NVvR merkt op dat het bewijzen van het oogmerk om, kort gezegd, die ander te (laten) intimideren, meestal niet eenvoudig zal zijn omdat het bij oogmerk gaat om de zwaarste vorm van opzet, maar meent dat de keuze voor dit bestanddeel juist is als de voorgestelde, ruime delictsomschrijving wordt gehandhaafd.

De NVvR acht de bijzondere opsporingsbevoegdheden proportioneel in relatie tot het beschermde belang. Het vorderen van verkeersgegevens en/of de identificerende gegevens van een IP-adres ligt immers voor de hand in een strafrechtelijk onderzoek naar dit type gedragingen. Om deze bevoegdheden te kunnen toepassen is nodig dat voor het feit voorlopige hechtenis kan worden toegepast. Aan die voorwaarde wordt in het wetsvoorstel voldaan.

De NVvR vraagt zich af of is voorzien in een adequate uitbreiding van de digitale opsporingscapaciteit van de politie en verzoekt mij nader in te gaan op de beperkte opsporingscapaciteit bij de politie, om teleurstelling te voorkomen bij aanmelders die rekenen op een serieus onderzoek naar aanleiding van hun aangifte. Naar aanleiding hiervan wordt opgemerkt dat in de uitvoerings- en financieringsparagraaf de impact van dit wetsvoorstel is opgenomen. In het algemeen geldt dat opsporingscapaciteit schaars is. Het Openbaar Ministerie prioriteert de zaken in afstemming met de politie. De politie is verantwoordelijk voor het bij de tijd houden van het vakmanschap van haar mensen.

Tenslotte vraagt de NVvR of ik voornemens ben gerichte actie te ondernemen met betrekking tot de effectiviteit van de regeling voor de tussenkomst van de host, zodat inschakeling van de civiele rechter door het slachtoffer in de regel niet nodig is. Naar aanleiding van deze vraag kan worden opgemerkt dat ik voornemens ben om bij de aanpak van schadelijk en immoreel online gedrag onder meer in te zetten op laagdrempelige mogelijkheden om gericht actie te ondernemen tegen illegale content.

** De Autoriteit persoonsgegevens*

De AP onderschrijft de noodzaak van een strafbaarstelling van doxing omdat de voorgestelde gedraging doxing ernstige schade kan toebrengen, strafwaardig is, en bestaande relevante strafbepalingen veelal niet voldoende zijn toegesneden op diverse gevallen van doxing.

De AP vraagt aandacht voor de openbaarheid van bronnen van gegevens die voor doxing kunnen worden gebruikt en adviseert in de toelichting aandacht te besteden aan het kabinetsbeleid op het punt van beschikbaarheid van persoonsgegevens uit wettelijk vormgegeven registers, waaronder het Handelsregister en het Kadaster. Naar aanleiding van dit advies wordt opgemerkt dat bij algemene registers, die van belang zijn voor het vrije handelsverkeer of voor het uitvoeren van publieke taken, het uitgangspunt is dat gegevens openbaar, dan wel opvraagbaar zijn. Tegelijkertijd is die openbaarheid onderhevig aan wet- en regelgeving ten aanzien van gegevensbescherming. In de praktijk kunnen geregistreerden de vrije beschikbaarheid van hun persoonsgegevens beperken tot gebruik door partijen voor wie de gegevens noodzakelijk zijn om tot een civielrechtelijke overeenkomst te komen, dan wel om hun publieke taken uit te kunnen voeren. Dit wetsvoorstel heeft betrekking op de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden. Voor strafbaarheid is de wijze van verkrijging van deze gegevens niet relevant, het oogmerk waarmee de dader zich persoonsgegevens verschafft is bepalend. Dat neemt niet weg dat het beperken van de toegang tot andermans persoonsgegevens het begaan van de strafbaar gestelde gedraging kan bemoeilijken.

De AP wijst erop dat de in de toelichting op de term 'identificerende persoonsgegevens' niet wordt ingegaan op de verhouding tot het begrip persoonsgegevens in de Algemene verordening gegevensbescherming (AVG) en adviseert deze afwijking van de AVG beter te motiveren of het voorstel en overige bepalingen in het Wetboek van Strafrecht waarin deze formulering voorkomt aan te passen aan de AVG. Mede naar aanleiding van deze opmerking van de AP is de voorgestelde strafbaarstelling gewijzigd. De term 'identificerende persoonsgegevens' is vervangen door de term 'persoonsgege-

vens'. Hiermee wordt aangesloten bij de AVG. De artikelsgewijze toelichting bij het voorgestelde artikel 285, eerste lid, is aangevuld om dit te verduidelijken. Het begrip identificerende persoonsgegevens komt voor in een aantal reeds bestaande strafbepalingen in het Wetboek van Strafrecht (onder andere de artikelen 231b en 435 Sr). In die bepalingen is de term 'identificerend' nodig om te verduidelijken dat het direct identificerende persoonsgegevens betreft, zoals de NAW-gegevens. In deze strafbepaling kan het ook om andere persoonsgegevens gaan, zoals eerdergenoemd de sportvereniging van de kinderen van het slachtoffer en de koosnamen van zijn geliefden. Om die reden zijn de overige bepalingen niet aangepast.

De AP merkt op dat de geconsulteerde versie van de toelichting de indruk wekte dat foto's in veel gevallen geen persoonsgegevens zijn terwijl in het geval dat een foto die is geplaatst zonder verdere gegevens veelal sprake zal zijn van een persoonsgegeven in de zin van de AVG omdat bekenden van de geportretteerde de identiteit van betrokkene aan de hand van uitsluitend de foto kunnen vaststellen en omdat de AVG uitgaat van directe of indirecte herleidbaarheid. Dit is een terechte opmerking, naar aanleiding waarvan de desbetreffende zin is geschrapt.

Naar het oordeel van de AP is de in het voorstel opgenomen strafuitsluitingsgrond overbodig omdat in geval van te goeder trouw verrichte gerechtvaardigde activiteiten van 'journalisten en klokkenluiders', maar ook van anderen, niet voldaan zal zijn aan het voor strafbaarheid vereiste oogmerk. Ik erken dat in deze gevallen het voor strafbaarheid vereiste oogmerk doorgaans zal ontbreken. De toelichting heb ik op dit punt aangevuld om dit te verduidelijken (paragraaf 2.4 en artikelsgewijs). Desalniettemin heb ik besloten de strafuitsluitingsgrond te handhaven zodat voor eenieder duidelijk is dat degenen die te goeder trouw hebben aangenomen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de persoonsgegevens vereiste niet strafbaar zijn.

De AP wijst er op dat ook anderen dan journalisten en klokkenluiders onder omstandigheden een beroep op vrijheid van meningsuiting toekomt. De strafuitsluitingsgrond is inderdaad niet beperkt tot een bepaalde beroepsgroep of een bepaalde kring van personen. In paragraaf 4 van deze toelichting is nader uiteengezet hoe het recht op vrijheid van meningsuiting zich verhoudt tot de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden.

De AP merkt op dat het vervullen van de delictomschrijving tevens een inbreuk op de AVG zal opleveren. De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, 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 dus situaties waarin de AVG van toepassing is en de AP bij niet naleving van deze verordening handhavend kan optreden, terwijl er ook sprake is van strafbare doxing waarvoor het openbaar ministerie vervolging in kan stellen. De strafrechtelijke aanpak van doxing betreft het gebruik van persoonsgegevens voor intimiderende doeleinden. De ernst van deze gedraging en de impact op de slachtoffers zijn aanleiding dit zelfstandig strafbaar te stellen. In voorkomende gevallen zal de AP in overleg moeten treden met het openbaar ministerie alvorens een boete op te leggen (artikel 5:44 Awb).

De wijzigingen van het Wetboek van Strafrecht BES en het Wetboek van Strafvordering BES komen niet in het opschrift van het wetsvoorstel tot uitdrukking, constateert de AP. Daarnaast adviseert de AP het concept ter advisering aan te bieden aan de Commissie toezicht bescherming persoonsgegevens BES. Vanwege het aantal regelingen dat dit wetsvoorstel wijzigt is er voor gekozen om te volstaan met een vermelding van het Wetboek van Strafrecht en het Wetboek van Strafvordering, gevolgd door 'en enige andere wetten' (Ar. 4.3). Het wetsvoorstel is voor advisering aangeboden aan de Commissie toezicht bescherming persoonsgegevens BES.

** De Commissie toezicht bescherming persoonsgegevens BES*

De CBP BES onderschrijft eveneens de noodzaak van de strafbaarstelling van doxing, omdat misbruik van persoonsgegevens voor intimiderende doeleinden ernstige schade kan toebrengen. De CBP BES merkt op dat in de memorie van toelichting bij de uitleg van 'identificerende persoonsgegevens' wordt aangehaakt bij bestaande strafbepalingen in het Wetboek van Strafrecht in het Europees deel van Nederland, maar dat niet wordt verwezen naar strafbepalingen uit het Wetboek van Strafrecht BES en de Wet bescherming persoonsgegevens BES (Wbp BES). De CBP BES adviseert om in de MvT met betrekking tot het begrip 'identificerende persoonsgegevens' in te gaan op de verhouding tot het begrip persoonsgegevens in de Wbp BES, en in het bijzonder aandacht te geven aan de biometrische gegevens bij de kwalificatie van persoonsgegevens voor doxing. Ook adviseert de CBP BES de passage in de MvT over foto's aan te passen, zeker gelet op de context waarbinnen de verwerking plaatsvindt. In reactie op dit advies wordt opgemerkt, dat zoals in reactie op het advies van de AP is toegelicht, de term 'identificerende persoonsgegevens' is vervangen door de term 'persoonsgegevens'. Hiermee wordt niet alleen bij de AVG aangesloten, maar ook bij de Wbp BES. De term persoonsgegevens omvat ook biometrische gegevens. De artikelsgewijze toelichting bij het voorge-

stelde artikel 298b Sr BES is aangevuld om dit te verduidelijken. Zoals is aangegeven in reactie op het advies van de AP is de zin uit de geconsulteerde versie van de toelichting die de indruk wekte dat foto's in veel gevallen geen persoonsgegevens zijn, geschrapt.

De CBP BES merkt op dat openbare registers, zoals het Handelsregister en het Kadaster, snel en voor iedereen toegankelijk zijn en adviseert om in de memorie van toelichting aandacht te besteden aan de beschikbaarheid van gegevens uit bij wet gestelde openbare registers. Zoals ik ook in de reactie op een vergelijkbare opmerking van de AP heb aangegeven, heeft dit wetsvoorstel betrekking op de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden. De wijze van verkrijging van deze gegevens is voor strafbaarheid niet relevant. Voor een uitgebreidere reactie op dit advies verwijs ik graag naar hetgeen ik hierover in reactie van het advies van de AP heb opgemerkt.

Voor het effectief optreden van autoriteiten acht de CBP BES het belangrijk dat vrij en integer persoonsgegevens kunnen worden uitgewisseld tussen Europees Nederland en het Caribisch deel van Nederland. De CBP BES wijst er echter op dat de Wbp BES niet de in artikel 46 AVG vereiste passende waarborgen voor de doorgifte van persoonsgegevens naar een derde land biedt. Daarom acht de CBP BES het wenselijk het beschermingsniveau voor persoonsgegevens in Europa als leidraad te volgen en na te streven voor Caribisch Nederland. In mijn reactie op deze opmerking beperk ik mij tot de context van dit wetsvoorstel, waarin het gebruik van persoonsgegevens voor intimiderende doeleinden strafbaar wordt gesteld in Europees Nederland en in de openbare lichamen Bonaire, Sint Eustatius en Saba. Voor de opsporing van deze strafbare gedragingen is het van belang dat opsporingsinstanties in Europees Nederland en in de openbare lichamen Bonaire, Sint Eustatius en Saba persoonsgegevens kunnen uitwisselen. De Wet politiegegevens (Wpg), die ook van toepassing is in de openbare lichamen Bonaire, Sint Eustatius en Saba (artikel 36b Wpg), biedt een uitgebreid wettelijk kader voor de uitwisseling van politiegegevens tussen Nederland en de openbare lichamen.

** De Nederlandse Vereniging van Journalisten*

De NVJ acht het van groot belang dat (strafrechtelijk) wordt opgetreden tegen het verspreiden van persoonsgegevens vanuit het oogpunt van intimidatie en vergelding. Voor de strafbaarstelling daarvan lijkt het onderhavige wetsvoorstel geschikt. De NVJ onderschrijft het belang dat wordt voorkomen dat het wetsvoorstel journalisten en klokkenluiders belet om misstanden en nieuwsfeiten openbaar te maken maar vraagt zich af of de vrijheid van meningsuiting en nieuwsgaring van journalisten in het wetsvoorstel daadwerkelijk voldoende is gewaarborgd. In het bijzonder wil de NVJ de volgende punten voor het voetlicht brengen.

De NVJ vindt onvoldoende duidelijk wat wordt bedoeld met 'identificerende persoonsgegevens', en vraagt of het wetsvoorstel aanknoopt bij het ruime begrip 'persoonsgegevens' in de AVG of dat het begrip in het wetsvoorstel beperkter is bedoeld. In reactie op een opmerking met dezelfde strekking van de AP is in het voorgaande aangegeven dat de toelichting op dit punt is aangevuld en dat de term identificerend is geschrapt. De NJV merkt op dat het oogmerk van een journalist bij de verspreiding van persoonsgegevens doorgaans het informeren van het publiek zal zijn en niet het aanjagen van vrees of aandoen van ernstige overlast. Omdat een goede controleur van macht machthebbers hindert in de uitoefening van hun beroep met kritische berichtgeving valt discussie te verwachten over het oogmerk 'hinderen in de uitoefening van ambt of beroep'. De NVJ zou graag bevestigd zien dat het 'hinderen' door journalistieke uitingen niet onder het eerste lid van het voorgestelde nieuwe artikel 298b Sr valt (kennelijk wordt hier artikel 285d Sr bedoeld) en is van mening dat de in het wetsvoorstel genoemde oogmerken in dit kader nadere verduidelijking behoeven. In reactie op de vraag van de NJV kan worden bevestigd dat een journalist die in het kader van zijn beroepsuitoefening persoonsgegevens verspreidt geen oogmerk zal hebben om de ander in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel te laten hinderen maar er op gericht zal zijn een misstand aan de kaak te stellen, zodat er geen sprake is van strafbare doxing. Dit is in de toelichting verhelderd.

De mogelijkheid van een beroep op het algemeen belang bij de verspreiding van persoonsgegevens roept bij de NVJ de nodige vragen op. De NJV zou graag zien dat nader wordt gespecificeerd in hoeverre de uitzondering op andere (journalistieke) uitingen dan het in de toelichting genoemde voorbeeld van toepassing is. De NVJ vraagt zich af of niet beter aansluiting zou kunnen worden gezocht bij de (ruime) 'journalistieke exceptie' die van toepassing is op de AVG en de aan deze uitzondering gerelateerde jurisprudentie van het Europees Hof voor de Rechten van de Mens. Naar aanleiding hiervan wordt opgemerkt dat de strafuitsluitingsgrond niet beperkt is tot journalisten. De formulering van de strafuitsluitingsgrond sluit aan bij de formulering van de artikelen 139g, tweede lid, en 273, tweede lid, Sr. De reikwijdte van de strafuitsluitingsgrond is in paragraaf 2.4 en het artikelsgewijs deel nader toegelicht.

Tenslotte vreest de NJV voor veel aangiftes vanwege journalistieke uitingen wanneer deze uitingen (te) snel onder het eerste lid van het voorgestelde nieuwe artikel kunnen worden geschaard, vanwege

een ruime toepassing van dit lid of vanwege onvoldoende duidelijkheid over de gehanteerde termen. Als gevolg van de dreiging van een aangifte zullen journalisten terughoudender worden in hun informatiegaring en berichtgeving; dat dient vanzelfsprekend te worden voorkomen. In reactie hierop moet worden opgemerkt dat deze vrees door mij niet wordt gedeeld. Het wetsvoorstel beoogt op geen enkele wijze afbreuk te doen aan de persvrijheid, dit komt tot uitdrukking in de opzet van de strafbaarstelling – waarin het oogmerk van het aanjagen van vrees een cruciale rol vervult – en het aanvullend opnemen van de strafuitsluitingsgrond van het algemeen belang. Hier komt nog bij dat het oordeel over de strafbaarheid uiteindelijk aan de rechter is.

** De openbare lichamen in Caribisch Nederland*

Het Openbaar Lichaam Bonaire heeft gemeld dat het Korps Politie Caribisch Nederland en het openbaar ministerie BES positief hebben gereageerd op het wetsvoorstel, en dat het goed is dat Caribisch Nederland qua strafrechtelijk instrumentarium niet achterblijft bij Europees Nederland. Het Openbaar Lichaam Bonaire kan dan ook instemmen met het voorstel.

6. Uitvoerings- en financiële consequenties

Strafbare doxing is een nieuw fenomeen, dat zich in korte tijd in verschillende vormen heeft gemanifesteerd. Het wetsvoorstel codificeert de breed gevoelde maatschappelijke norm dat het gebruik van persoonsgegevens voor intimiderende doeleinden onacceptabel is.

Van de politie, het openbaar ministerie en de rechterlijke macht is een reactie ontvangen met betrekking tot de gevolgen voor de uitvoering en de financiële consequenties die de voorgenomen wetwijziging met zich meebrengt. Voor de berekening daarvan zijn door politie, openbaar ministerie en rechterlijke macht verschillende methodes gehanteerd, waardoor de inschattingen onderling variëren. Met betrekking tot het maken van een inschatting van het aantal extra strafzaken dat het gevolg is van dit wetsvoorstel, overweegt het kabinet dat het wetsvoorstel de drempel om strafrechtelijk in te kunnen grijpen bij online intimidatie en bedreiging verlaagt. Daarbij dient echter overwogen te worden, dat ten minste een gedeelte van de slachtoffers zich nu ook al tot de politie wendt, en het openbaar ministerie in die gevallen ook nu reeds een afweging maakt of de aangifte strafwaardig is. Wel zal vaker dan op dit moment het geval is een strafrechtelijk onderzoek worden uitgevoerd en worden besloten tot strafrechtelijke vervolging. Zeker nu de ontwikkelingen laten zien dat er sprake is van een toename van het gebruik van sociale media voor ontoelaatbare uitingen.

Daarnaast geldt dat slachtoffers een beroep kunnen doen op internettussenpersonen om op grond van hun gebruiksvoorwaarden de gewraakte online content ontoegankelijk te maken. De nieuwe strafbaarstelling kan behulpzaam zijn in deze procedure omdat hiermee het verboden karakter van het gebruik van persoonsgegevens voor intimiderende doeleinden tot uitdrukking wordt gebracht. Verder geldt dat de nationale en Europese wetgeving met betrekking tot de aansprakelijkheid van internettussenpersonen in ontwikkeling is. Hierdoor wordt het voor burgers mogelijk om laagdrempelig melding te maken van dergelijke content.

Aanvullend hierop geldt dat het Coalitieakkoord 2021–2022 *Omzien naar elkaar, vooruitkijken naar de toekomst* in brede zin aandacht vraagt voor online bejegening. Dat betekent dat het fenomeen doxing de komende jaren ook in een bredere context van het reguleren van bepaalde vormen van online content zal worden gezien. Hierbij zal ook nadrukkelijk aandacht worden besteed aan de rol van het strafrecht daarbij, en daarmee aan de benodigde inzet van politie en openbaar ministerie ten aanzien van deze fenomenen.

Dit alles overwegend schat het kabinet in dat de structurele gevolgen voor de uitvoering en dientengevolge de financiële consequenties van dit wetsvoorstel beperkt zullen zijn en kunnen worden opgevangen binnen de begrotingen van politie, openbaar ministerie en de rechtspraak. De door politie geschatte incidentele kosten met betrekking tot het aanpassen van de IV-voorzieningen, opleidingen en het actualiseren van de kennis van politiemedewerkers, zullen worden opgenomen in de politiebegroting.

Ik zal in samenwerking met politie en openbaar ministerie uiterlijk twee jaar na de inwerkingtreding van de wet een invoeringstoets uitvoeren, met als doel te bezien of de hierboven gehanteerde aannames zich inderdaad hebben gemanifesteerd. Mocht blijken dat de aannames niet helemaal juist waren of dat de structurele uitvoeringsconsequenties anders zijn, dan wordt dit gewogen door middel van het reguliere traject van het vaststellen van de begrotingen van politie, openbaar ministerie en de rechtspraak.

II. Artikelsgewijze toelichting

Artikel I (Wijziging Wetboek van Strafrecht)

Eerste lid

In dit lid wordt strafbaar gesteld het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde met het oogmerk 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 te laten hinderen. Hieronder worden de verschillende onderdelen van de delictsomschrijving nader toegelicht.

‘Zich verschaffen’ betreft gedragingen die zijn gericht op het in het bezit krijgen van de persoonsgegevens (Kamerstukken 2002/03, 29 025, 3, blz. 1 en 5/6). Het handelt om het zich doen toekomen van gegevens, hieronder kan met andere woorden worden verstaan het verzamelen van gegevens. Hierbij kan onderscheid worden gemaakt tussen het geheel zelfstandig verzamelen van gegevens en het verkrijgen van de gegevens van derden. In beide gevallen is het zich verschaffen van persoonsgegevens van een ander of een derde, bijvoorbeeld door het gebruik van internet, strafbaar als deze handelingen worden verricht met het oogmerk van het (laten) aanjagen van vrees of het (laten) aandoen van ernstige overlast die een ander of het (laten) hinderen van die ander in de uitoefening van zijn ambt of beroep. In de praktijk zal het geheel zelfstandig verzamelen van gegevens zonder enige betrokkenheid van anderen, zoals bij het zoeken op het internet, vrijwel niet op te sporen zijn omdat het verzamelen van de gegevens niet kenbaar is voor de omgeving, nog afgezien van het feit dat het oogmerk waarschijnlijk niet eenvoudig te bewijzen zal zijn. In geval van het zich verschaffen van de persoonsgegevens van de derde doordat deze worden verkregen van een andere persoon, bijvoorbeeld nadat via sociale media is opgeroepen om het adres van een bepaalde persoon toe te zenden, zal er ook sprake kunnen zijn van het verspreiden of anderszins ter beschikking stellen van persoonsgegevens, namelijk door de oproep via sociale media, en kan er sprake zijn van overlap in de delictsomschrijving tussen het zich verschaffen en verspreiden van gegevens.

Het zich verschaffen veronderstelt een actief handelen van degene die zich de gegevens verschafft. Degene die tegen zijn wil andermans persoonsgegevens toegezonden krijgt is niet bezig met het ‘verschaffen’ ervan, en heeft overigens ook niet het voor strafbaarheid vereiste oogmerk.

‘Verspreiden of anderszins ter beschikking stellen’ ziet op het distribueren of toezenden van gegevens. Dit handelen is niet beperkt tot de door de dader gekende of beoogde ontvangers van de informatie. Anders dan bij opruiing (art. 131 Sr) hoeft dit niet in het openbaar te gebeuren. De voorgestelde strafbaarstelling is niet beperkt tot voor het publiek toegankelijke plaatsen of tot het verspreiden of ter beschikking stellen onder zodanige omstandigheden en op zodanige wijze dat zij door het publiek kunnen worden verkregen, omdat ook het verspreiden van persoonsgegevens op niet openbare plaatsen – zoals in besloten chatgroepen – een geschikt instrument kan zijn om een ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de uitoefening van ambt of beroep. Daarom omvat de strafbaarstelling ook die verspreidingswijzen.

Met ‘een ander’ wordt bedoeld op het slachtoffer; de persoon die vrees kan worden aangejaagd, ernstige overlast kan worden aangedaan of in de uitoefening van zijn functie ernstig kan worden gehinderd. Met ‘een derde’ wordt bedoeld op een persoon die in een bepaalde relatie staat tot het slachtoffer, en van wie de verdachte zich de persoonsgegevens verschafft teneinde het slachtoffer te intimideren, zoals de familieleden van het slachtoffer.

Met het gebruik van de term ‘persoonsgegevens’ wordt aangesloten bij de AVG. Het begrip persoonsgegevens betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, onderdeel 1, AVG). Persoonsgegevens zijn bijvoorbeeld naam, adres, woonplaats, postadres, telefoonnummers, IP-adressen of geboortedatum. Om te bepalen of een natuurlijke persoon identificeerbaar is moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen (AVG, punt 26, Richtlijn politiegegevens, punt 21).

Voor strafbaarheid is vereist dat degene die zich de persoonsgegevens verschafft, deze gegevens verspreidt of anderszins ter beschikking stelt het oogmerk heeft 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. Het gaat om het beoogde effect van de gedraging: aan de oogmerkeis is voldaan

wanneer de verdachte ten tijde van die gedraging de bedoeling heeft om het slachtoffer vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in zijn beroepsuitoefening. Aan de oogmerkeis is tevens voldaan in het geval van noodzakelijkheidsbewustzijn (vgl. de arresten van de Hoge Raad van 5 januari 1982, NJ 1982/232, m.nt. Van Veen (Gevangenis-voedsel II) en 21 april 1998, NJ 1998/610). Daarvan is sprake indien het niet anders kan zijn dan dat de verdachte heeft beseft dat het noodzakelijke gevolg van zijn handelen is dat – kort gezegd – het slachtoffer vrees zal worden aangejaagd, ernstige overlast zal worden aangedaan of in de uitoefening van zijn ambt of beroep ernstig zal worden gehinderd. Het oogmerk kan er ook op zijn gericht het tweewegbrengen van vrees, ernstige overlast of hinder door een ander te laten bewerkstelligen. Dit wordt tot uitdrukking gebracht met de woorden vrees aan te laten jagen, ernstige overlast aan te laten doen of in de uitoefening van zijn ambt of beroep ernstig te laten hinderen. Bij strafbare doxing kan het immers juist ook gaan om het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van het beoogde slachtoffer, zoals zijn adres, zodat anderen hiermee in de richting van diegene kunnen handelen.

De hiervoor genoemde arresten illustreren dat bij het bewijs van het oogmerk gebruik kan worden gemaakt van een objectiverende bewijsvoering. Voor het bewijs van het oogmerk kan de rechter acht slaan op onder meer gedragingen en uitlatingen van de verdachte voor, tijdens of na het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van de ander. Het oogmerk zal ook uit de context kunnen worden afgeleid, dat wil zeggen de omstandigheden waaronder de persoonsgegevens zijn verzameld, verspreid of anderszins ter beschikking zijn gesteld. Als de verdachte het strafbare oogmerk ontkent dan kan voor het bewijs van het oogmerk de context van het handelen van belang zijn, bijvoorbeeld het feit dat de verdachte heeft deelgenomen aan een chatgroep waarin negatief is gesproken over het slachtoffer of de kring van personen waartoe het slachtoffer behoort. Ook als de verdachte verklaart een positieve intentie te hebben gehad – ‘ik wilde hem bedanken’ – zal in sommige gevallen uit de omstandigheden kunnen worden afgeleid dat het oogmerk van de verdachte erop gericht moet zijn geweest om de betrokkene vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of hem in te uitoefening van zijn functie ernstig te (laten) hinderen. Bijvoorbeeld omdat adresgegevens worden gedeeld in een groep die bestaat uit personen die zich verontwaardigd of beledigend uitlaten over het slachtoffer of een groep waartoe hij behoort. Als door anderen gehoor wordt gegeven aan de oproep van degene die de persoonsgegevens verspreidt om deze persoonsgegevens te gebruiken, op een wijze die door een normaal mens onder vergelijkbare omstandigheden zou worden opgevat als het (laten) aanjagen van vrees, het (laten) aandoen van ernstige overlast of het ernstig (laten) hinderen in de uitoefening van ambt of beroep, dan kan het strafbare oogmerk worden bewezen als de verdachte beseft of moet hebben beseft dat zijn handelen dit door hem gewilde gevolg met zich mee zou brengen.

Zoals in paragraaf 2.1 reeds is opgemerkt, is het gebruik van persoonsgegevens voor intimiderende doeleinden een formeel omschreven delict; de gedragingen worden strafbaar gesteld ongeacht het resultaat ervan. Niet hoeft te worden bewezen dat het slachtoffer ten gevolge van de gedraging daadwerkelijk vrees is aangejaagd, dat betrokkene daadwerkelijk ernstige overlast heeft ervaren of in de uitoefening van zijn functie daadwerkelijk ernstig is gehinderd. Het volstaat dat het oogmerk van de verdachte hierop is gericht. Of dit op het slachtoffer het beoogde effect heeft gehad is strafrechtelijk niet relevant, al maakt dat de bewijsvoering wel eenvoudiger.

Met ‘vrees’ wordt, evenals in de delictomschrijving van belaging (artikel 285b Sr), een emotie bedoeld, die ieder normaal mens onder vergelijkbare omstandigheden ook zou hebben. Van belang is of een andere persoon, redelijkerwijs te vergelijken of gelijk te stellen met het slachtoffer in kwestie, in vergelijkbare omstandigheden eveneens deze emotie zou ervaren. Uitgegaan wordt van de – meer geobjectiveerde – emotie van de normale mens om te voorkomen dat de strafbaarheid van de verdachte afhankelijk zou zijn van de beleving van het slachtoffer, waarmee de strafbaarstelling een zeer subjectief karakter zou verkrijgen. In de memorie van toelichting bij artikel 285b Sr (Kamerstukken II 1997/98, 25 768 nr. 5, p. 116) is hierover het volgende opgemerkt: ‘Het oogmerk van de dader is gericht op (...) het ontstaan van zo’n emotie.’ Het werkwoord ‘aanjagen’ veronderstelt bij ‘vrees aanjagen’ dat de dader met een kwalijke opzet handelt (Kamerstukken II 1997/98, 25 768 nr. 7), de dader heeft daadwerkelijk het oogmerk om het slachtoffer bang te maken. Het voorafgaande impliceert dat de maatschappelijke positie van het slachtoffer, zoals het zijn van burgemeester of ambtenaar van politie, als zodanig niet van invloed is op de beoordeling van de vraag of sprake is van het aanjagen van vrees; zoals hierboven aangegeven betreft dit een geobjectiveerde beoordeling, waarbij wordt uitgegaan van ieder normaal mens in vergelijkbare omstandigheden. De aan te jagen vrees is niet beperkt tot een bepaalde strekking, zoals vrees voor de veiligheid. Een nadere inkadering van deze strekking, zoals in het advies van de Rvdr aan de orde gesteld, draagt het risico van een te vergaande beperking van de bescherming van de voorgestelde strafbaarstelling voor de slachtoffers. Met de woorden ‘*ernstige overlast*’ of ‘*ernstige hinder*’ wordt tot uitdrukking gebracht dat dit van zodanige aard moet zijn dat het slachtoffer hierdoor redelijkerwijs kan worden geacht ernstige overlast aan te worden gedaan of in de uitoefening van zijn ambt of beroep ernstig te worden gehinderd. Van

‘ernstige overlast’ en ‘ernstige hinder van de uitoefening van ambt of beroep’ kan sprake zijn in die gevallen waarin een slachtoffer – doordat zijn persoonsgegevens bekend zijn bij anderen – zijn reguliere (privé)activiteiten of werkzaamheden niet meer ongestoord kan voortzetten, bijvoorbeeld omdat hij wordt lastiggevallen of omdat het risico dat dit gebeurt zeer groot is. Ook kan hierbij worden gedacht aan personen die alleen in relatieve onbekendheid hun functie kunnen vervullen, zoals undercoveragenten, van wie de identiteit door de verspreiding van persoonsgegevens bekend is geworden. De gevallen waarin het oogmerk van de verdachte niet kan worden aangemerkt als te zijn gericht op het (laten) aanjagen van ernstige overlast of het (laten) aandoen van ernstige hinder in de uitoefening van ambt of beroep vallen buiten de reikwijdte van de delictsomschrijving en zullen voor de opsporings- en vervolgingsinstanties geen aanleiding behoeven te geven tot inspanningen gericht op opsporing en vervolging.

In verschillende adviezen is aandacht gevraagd voor de reikwijdte van de voorgestelde strafbaarstelling. Daarbij is gesuggereerd te komen tot nadere inkadering aan de hand van praktijkvoorbeelden of typologieën van strafbare gedragingen of strafbare situaties. Hierboven is uiteengezet dat de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden bestaat uit een bepaald handelen, te weten het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde, met een bepaald oogmerk, te weten het die ander (laten) aanjagen van vrees, (laten) aandoen van ernstige overlast of ernstig te (laten) hinderen in de uitoefening van zijn ambt of beroep. Zoals hierboven aan de orde is gekomen, wordt voor de beoordeling of het oogmerk van de dader is gericht op het aanjagen van vrees of het aandoen van ernstige hinder of overlast uitgegaan van ieder normaal mens in vergelijkbare omstandigheden. In een concrete situatie kan voor het bewijs van het oogmerk de context van het handelen van belang zijn, zeker als de verdachte het oogmerk van de intimidatie ontkent. Als bijvoorbeeld wordt opgeroepen tot een samenkomst in de tuin van de woning van een burgemeester van een gemeente op een bepaalde datum of tijdstip om daar gezamenlijk ‘een kop koffie te drinken’, en met het oog op een dergelijke samenkomst bij anderen wordt gevraagd naar het adres van de woning van de burgemeester, of het adres van die woning wordt verspreid, dan kan een dergelijke oproep onder omstandigheden – in het licht van de context – worden aangemerkt als het aanjagen van vrees, bijvoorbeeld omdat de oproep wordt gedaan door personen die zich intimiderend of bedreigend uitlaten of hebben uitgelaten richting de betrokkene of doordat de oproep wordt gedaan in een kring van personen waarin dergelijke uitlatingen zijn of worden gedaan. In het licht van de context kan de samenkomst van een aantal personen bij de ambtswoning worden aangemerkt als het aanjagen van vrees. Een dergelijke samenkomst kan onder omstandigheden ook als ernstige overlast worden aangemerkt, bijvoorbeeld als deze personen zich zonder toestemming ophouden in de tuin van de woning en/of de toegang tot de woning versperren. Het vragen bij anderen naar het woonadres van een politicus om hem een taart aan te bieden kan, afhankelijk van de context, eveneens als het aanjagen van vrees worden aangemerkt, bijvoorbeeld onder de omstandigheden als hierboven vermeld (oproep gedaan door personen die zich intimiderend of bedreigend uitlaten of hebben uitgelaten richting de betrokkene of oproep gedaan in een kring van personen waarin dergelijke uitlatingen zijn of worden gedaan). Ditzelfde geldt voor het bekend maken van de personalia of het adres van een verdachte of veroordeelde (‘ontanonimiseren’): mede afhankelijk van de context van het handelen kan worden geoordeeld dat sprake is van het oogmerk van het aanjagen van vrees, het (laten) aandoen van ernstige overlast of het ernstig (laten) hinderen in de ambts- of beroepsuitoefening, waardoor dit handelen kan worden gekwalificeerd als gebruik van persoonsgegevens voor intimiderende doeleinden.

Op grond van de voorgestelde delictsomschrijving is als pleger strafbaar degene die zich de persoonsgegevens van een ander of een derde verschafft, verspreidt of anderszins ter beschikking stelt met het bovenbeschreven oogmerk. De delictsomschrijving strekt zich niet uit tot degene die na een oproep daartoe van een ander daadwerkelijk de vrees aanjaagt, ernstige overlast aandoet of de uitoefening van ambt of beroep ernstig hindert, hoewel diegene zich uiteraard ook schuldig kan maken aan het zich verschaffen van persoonsgegevens met dit oogmerk. Poging tot het plegen van het strafbare feit van gebruik van persoonsgegevens voor intimiderende doeleinden is mogelijk als het feit niet wordt voltooid vanwege een van de wil van de pleger onafhankelijke omstandigheid, bijvoorbeeld doordat het zich verschaffen of verspreiden van de persoonsgegevens niet is gelukt omdat de gegevens niet beschikbaar bleken. Overigens is het – zo bleek hiervoor al – niet uitgesloten dat de verdachte bij het oproepen tot het verstrekken van persoonsgegevens zelf een dergelijk gegeven verspreidt, zodat er dan tevens sprake kan zijn van een voltooid delict. Medeplichtigheid aan het strafbare feit van het gebruik van persoonsgegevens voor intimiderende doeleinden is mogelijk als opzettelijk gelegenheid, middelen of inlichtingen worden verschafft, bijvoorbeeld doordat een geautomatiseerd werk (pc, tablet of smartphone) beschikbaar wordt gesteld, tot het plegen van dit misdrijf.

Het strafmaximum bedraagt een jaar gevangenisstraf of geldboete van de derde categorie. De voorgestelde strafbaarstelling betreft handelingen die vooraf kunnen gaan aan reeds strafbare gedragingen, zoals bedreiging (artikel 285 Sr), belaging (artikel 285b Sr) of mishandeling (artikel 300

e.v. Sr). Voor strafbaarheid is echter niet vereist dat deze gedragingen hierop volgen. In dat licht dient deze strafmaat, die lager is dan de maximumstraf voor voornoemde gedragingen, passend te worden geacht. Ter vergelijking wordt gewezen op artikel 133 Sr waarin strafbaar is gesteld het in het openbaar aanbieden inlichtingen, gelegenheid of middelen te verschaffen om enig strafbaar feit te plegen. Hiervoor geldt een strafmaximum van ten hoogste zes maanden gevangenisstraf of een geldboete van de derde categorie.

Tweede lid

Van strafbaarheid is geen sprake als de betrokkene te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de persoonsgegevens vereiste. In dit verband kan worden gewezen op het recht op vrije nieuwsgaring dat voortvloeit uit onder andere de artikelen 7 van de Grondwet en 10 van het EVRM. Het wetsvoorstel beoogt nadrukkelijk niet te voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders. Het voor strafbaarheid vereiste oogmerk – 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 te laten hinderen – zal bij journalisten en klokkenluiders in nagenoeg alle gevallen ontbreken. Om hierover geen twijfel te laten bestaan wordt voorgesteld in dit lid een zelfstandige uitzondering in de wet op te nemen voor degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens vereiste. Hiervoor is aangesloten bij de regeling in de artikelen 139g, tweede lid, en 273, tweede lid, Sr. Deze uitzondering is overigens niet beperkt tot een bepaalde beroepsgroep of een bepaalde kring van personen, zodat iedere burger die te goeder trouw bijvoorbeeld een maatschappelijke misstand aan de kaak wil stellen in voorkomend geval hierop een beroep kan doen. In paragraaf 2.4 is toegelicht dat het samenbrengen en publiceren van persoonsgegevens een gerechtvaardigd belang kan dienen, bijvoorbeeld wanneer het gaat om het aan de kaak stellen van misstanden.

De in het voorgestelde tweede lid opgenomen strafuitsluitingsgrond strekt zich uit tot de in het voorgestelde eerste lid strafbaar gestelde handelingen.

Artikel II (Wijziging Wetboek van Strafrecht BES)

In de openbare lichamen Bonaire, Sint Eustatius en Saba wordt zoveel mogelijk aangesloten bij de materiële strafwetgeving van Nederland. Om die reden wordt thans ook voorgesteld de strafbaarstelling van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens met het oogmerk vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of de ander in de uitoefening van zijn ambt of beroep ernstig te (laten) hinderen in het Wetboek van Strafrecht BES in te voeren. Dit gebeurt door invoeging van een nieuw artikel 298b. Voor een toelichting op deze strafbaarstelling wordt verwezen naar de toelichting op Artikel I. Ten aanzien van de term ‘persoonsgegevens’ wordt in aanvulling op de toelichting bij Artikel I opgemerkt dat met deze term eveneens wordt aangesloten bij de Wbp BES. Het begrip persoonsgegevens wordt in artikel 1, tweede lid, onder a, Wbp BES gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit omvat ook biometrische gegevens.

Artikel III (Wijziging van het Wetboek van Strafvordering)

Artikel 67 Sv bevat de gevallen waarin een bevel tot voorlopige hechtenis kan worden gegeven, te weten een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaar of meer is gesteld of een aantal specifiek opgesomde misdrijven. Dwangmiddelen als de aanhouding buiten heterdaad en de in verzekeringstelling en de inzet van bijzondere opsporingsbevoegdheden als het vorderen van gegevens zullen noodzakelijk zijn bij de bestrijding van het gebruik van persoonsgegevens voor intimiderende doeleinden. Gelet op het op dit misdrijf gestelde wettelijke strafmaximum – dat ten hoogste gevangenisstraf van een jaar bedraagt – wordt in artikel III voorgesteld het gebruik van persoonsgegevens voor intimiderende doeleinden in artikel 67, eerste lid, onderdeel b, Sv afzonderlijk te noemen als een misdrijf bij verdenking waarvan een bevel tot voorlopige hechtenis kan worden gegeven.

Artikel IV (Wijziging van het Wetboek van Strafvordering BES)

Ook voor de openbare lichamen Bonaire, Sint Eustatius en Saba geldt dat dwangmiddelen en opsporingsbevoegdheden nodig kunnen zijn bij de bestrijding van het gebruik van persoonsgegevens voor intimiderende doeleinden. In artikel IV wordt daarom voorgesteld het gebruik van persoonsgegevens voor intimiderende doeleinden in artikel 100, eerste lid, onderdeel b, van het Wetboek van Strafvordering BES afzonderlijk te noemen als een misdrijf bij verdenking waarvan een bevel tot voorlopige hechtenis kan worden gegeven. Zie ook de toelichting bij Artikel III.



Artikel V (Inwerkingtreding)

Voor de inwerkingtredingsbepaling is aangesloten bij het model van de Aanwijzingen voor de regelgeving (Ar. 4.21).

De Minister van Justitie en Veiligheid,