36 171 **Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafrecht BES, het Wetboek van Strafvordering en het Wetboek van Strafvordering BES in verband met de strafbaarstelling van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden (strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden)**

Memorie van antwoord

1. Inleiding

Met belangstelling heb ik kennisgenomen van het voorlopig verslag over het onderhavige wetsvoorstel dat voorziet in strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden. De leden van de fracties van **GroenLinks** en de **PvdA** hebben aangegeven met belangstelling te hebben kennisgenomen van het wetsvoorstel. Het stemt deze leden positief dat voor de invulling van het begrip persoonsgegevens is aangesloten bij de Algemene verordening gegevensbescherming. Ook waarderen ze de gegeven duidelijkheid omtrent de positie van journalisten, klokkenluiders en betrokken burgers die maatschappelijke misstanden aan de kaak willen stellen. Zij hebben over het wetsvoorstel nog enkele vragen gesteld. Ook de **D66**-fractieleden hebben over het wetsvoorstel enkele vragen gesteld. De leden van de **SGP**-fractie hebben eveneens met belangstelling kennisgenomen van het wetsvoorstel. Zij hebben de noodzaak van de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden onderschreven. Deze leden hebben over het wetsvoorstel enkele vragen gesteld. De leden van **50PLUS**-fractie hebben zich aangesloten bij de vragen gesteld door de leden van de fracties van GroenLinks, de PvdA en de SGP.

Ik dank de leden van deze fracties voor hun inbreng over het wetsvoorstel. Graag ben ik bereid de gestelde vragen te beantwoorden. Bij de beantwoording wordt zoveel mogelijk de volgorde van het voorlopig verslag aangehouden.

2. Dwangmiddelen en strafmaxima

De leden van de fracties van **GroenLinks** en de **PvdA** hebben gevraagd wat de gevolgen van de twee in de Tweede Kamer aangenomen amendementen (Kamerstukken II 2022/23, 36171, nr. 8; Kamerstukken II 2022/23, 36171, 10) zijn voor de mogelijke inzet van dwangmiddelen.

De twee door de Tweede Kamer aangenomen amendementen hebben tot gevolg dat het strafmaximum voor het strafbaar gestelde gebruik van persoonsgegevens voor intimiderende doeleinden (hierna ook te noemen: strafbare doxing) is verhoogd tot een gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie (Kamerstukken II 2022/23, 36171, nr. 8). Daarnaast is aan de voorgestelde bepaling een bijzondere strafverhogingsgrond toegevoegd voor het geval de strafbaar gestelde gedraging wordt gepleegd tegen personen in een bepaalde hoedanigheid (Kamerstukken II 2022/23, 36171, nr. 10), namelijk die van minister, staatssecretaris, commissaris van de Koning, gedeputeerde, burgemeester, wethouder, lid van een algemeen vertegenwoordigend orgaan, rechterlijk ambtenaar, advocaat, journalist of publicist in het kader van nieuwsgaring, ambtenaar van politie of buitengewoon opsporingsambtenaar. Als deze strafverhogingsgrond van toepassing is, wordt de op het feit gestelde gevangenisstraf met een derde verhoogd, deze bedraagt daardoor maximaal twee jaar en acht maanden.

De twee amendementen hebben geen gevolgen voor de mogelijke inzet van dwangmiddelen. In het wetsvoorstel was namelijk al voorzien in aanpassing van artikel 67 Sv en artikel 100 Sv BES waardoor strafbare doxing wordt aangemerkt als een misdrijf waarvoor een bevel tot voorlopige hechtenis kan worden gegeven. Daarmee kunnen dwangmiddelen - als de aanhouding buiten heterdaad en de inverzekeringstelling – en bijzondere opsporingsbevoegdheden - als het vorderen van gegevens - reeds worden toegepast.

Voorts hebben de leden van deze fracties gevraagd hoe de regering de twee amendementen waardeert die elkaar in strafmaximumverhogende werking versterken, wat het oordeel is over de intrinsieke strafwaardigheid van dit gedrag en hoe het geamendeerde strafmaximum zich verhoudt tot dat van vergelijkbare strafbare feiten.

Het in het wetsvoorstel voorgestelde strafmaximum van één jaar gevangenisstraf of geldboete van de derde categorie werd passend geacht voor het misdrijf gebruik van persoonsgegevens voor intimiderende doeleinden. In de verhouding tot de wettelijke strafmaxima voor andere misdrijven meende ik dat bij die voorgestelde maximale strafhoogte sprake was van evenredigheid en dat de rechter voldoende ruimte zou hebben om een straf te bepalen die recht doet aan de specifieke feiten en omstandigheden van het geval. Dat neemt niet weg dat ik begrip had voor de door leden van verschillende fracties in de Tweede Kamer geuite wens om het mogelijk te maken dat in heel

ernstige gevallen een fikse straf kan worden opgelegd. Daarbij speelt ook mee dat het bij het bepalen van het strafmaximum in essentie gaat om de waardering van de ernst van een strafbaar feit. Dat oordeel is niet alleen aan mij. Van belang is ook hoe vanuit de samenleving naar een fenomeen wordt gekeken. Het amendement dat strekte tot verhoging van het strafmaximum tot twee jaar gevangenisstraf heb ik daarom tijdens de behandeling van dit wetsvoorstel in de Tweede Kamer aan het oordeel van de Kamer gelaten. Het amendement dat strekte tot invoering van de bijzondere strafverhogingsgrond heb ik daarentegen ontraden omdat ik een afzonderlijke wettelijke strafverzwaringsgrond met een derde niet nodig achtte omdat het strafmaximum van twee jaar de strafrechter voldoende ruimte bood om de meest ernstige gevallen van strafbare doxing passend te kunnen bestraffen. Ik heb erop gewezen dat als deze amendementen gecombineerd zouden worden het strafmaximum enigszins uit evenwicht zou raken in verhouding tot de strafmaxima van andere delicten die qua strafwaardigheid tot op zekere hoogte op dezelfde lijn zijn te stellen. Het nu geldende strafmaximum van twee jaar gevangenisstraf is bijvoorbeeld gelijk aan dat voor strafbare dwang (artikel 284 Sr) maar nog wel lager dan dat voor bedreiging (artikel 285 Sr) waarop een maximale gevangenisstraf van drie jaar gevangenisstraf is gesteld. Tegelijk is het strafmaximum van twee jaren gevangenisstraf weer aanzienlijk hoger dan het strafmaximum voor het in het openbaar aanbieden inlichtingen, gelegenheid of middelen te verschaffen om enig strafbaar feit te plegen (artikel 133 Sr), waarop een gevangenisstraf van ten hoogste zes maanden is gesteld, maar fors lager dan dat voor opruiing waarvoor een gevangenisstraf van maximaal vijf jaren kan worden opgelegd (artikel 131 Sr). Al met al concludeer ik dan ook dat de hoogte van het strafmaximum in relatie tot de strafhoogtes voor soortgelijke delicten nog steeds verdedigbaar is en daarmee op passende wijze uiting geeft aan de meest ernstige verschijningsvorm van doxing.

De leden van de fracties van **GroenLinks** en de **PvdA** hebben daarnaast gevraagd of het met het amendement gecreëerde onderscheid tussen de groep functionarissen waarvoor de bijzondere strafverhogingsgrond geldt en andere functionarissen, zoals wetenschappers, medici, leden van het OMT of anderen die niet tot de in het amendement genoemde beroepsgroepen behoren en ook een relevant belang hebben om publiekelijk stelling te nemen of een beroep uit te oefenen, te rechtvaardigen is. Daarbij hebben zij gevraagd het onderscheid in ernst van het delict dan wel te beschermen belang te motiveren.

Ik stel voorop dat ik het gebruik van persoonsgegevens voor intimiderende doeleinden onacceptabel vind, ongeacht wie het slachtoffer is. Extra kwalijk zijn de gevallen waarin een journalist of iemand vanwege zijn of haar publieke functie slachtoffer wordt van deze gedraging. Doxing kan grote gevolgen hebben voor slachtoffers en hun gezinsleden en kan ertoe leiden dat mensen bepaalde functies niet meer kunnen, willen of durven te vervullen. Dit kan direct raken aan het functioneren van de democratische rechtstaat. In gevallen van strafbare doxing die verband houden met de uitvoering van de publieke taak zal het openbaar ministerie de strafeis aanzienlijk naar boven bijstellen, conform het uitgangspunt voor agressie en geweld tegen werknemers met een publieke taak en andere functionarissen werkzaam in het publieke domein (zie paragraaf 6 van de Aanwijzing kader voor strafvordering meerderjarigen (2019A003)). De strafeis wordt in deze gevallen met 200% verhoogd. Dit geldt overigens ook ten aanzien van publieke functies die niet in de strafverhogingsgrond zijn opgenomen. De indieners van het amendement hebben toegelicht dat aan de publieke functie die de in de strafverzwaringsgrond genoemde ambts- en gezagsdragers en functionarissen werkzaam in het veiligheidsdomein vervullen een bepaalde positie is verbonden. Zij worden gezien als vertegenwoordiger van een publiek orgaan dat een essentiële functie vervult in het democratisch bestel of als functionaris vanuit het veiligheidsdomein. Van personen in deze posities wordt een hoge mate van loyaliteit en inzet voor de publieke zaak verwacht. Het beeld van deze functionarissen als representant van het openbaar orgaan of veiligheidsdomein maakt deze functionarissen volgens de indieners van het amendement een aantrekkelijk doelwit voor 'doxers'. Daardoor kunnen zij in hun functie worden geconfronteerd met gedrag van burgers die het goed uitoefenen van hun functie bemoeilijken en de persoonlijke vrijheid beperkt. Ik deel de opvatting van de indieners van het amendement dat veel wordt verwacht van deze functionarissen en dat zij, en hun gezinsleden, in de praktijk – helaas - een groot risico lopen slachtoffer te worden van intimidatie vanwege de functie die zij vervullen. Dit bemoeilijkt niet alleen de vervulling van hun belangrijke taak, maar raakt direct aan hun privéleven. Dat rechtvaardigt dat daartegen stevig kan worden opgetreden. Van de strafverhogingsgrond kan ook een afschrikwekkende werking uitgaan naar potentiële daders voor wie echt duidelijk moet zijn dat het ontoelaatbaar is dat personen die een publieke functie vervullen en hun naasten om die reden worden geïntimideerd. Het nu voorziene strafmaximum dat - zoals hierboven besproken - op een fors hogere positie is uitgekomen, biedt in elk geval ook voldoende ruimte om de ernstige gevallen van strafbare doxing tegen andere functionarissen - die niet in de strafverzwaringsgrond zijn genoemd - stevig te kunnen bestraffen.

3. Opzet en bewijs

De leden van de fracties van **GroenLinks** en de **PvdA** vragen vervolgens twee concrete voorbeelden te geven van feitelijkheden die als voldoende bewijs kunnen dienen van het voor strafbaarheid vereiste oogmerk.

Strafbaar is de dader die zich persoonsgegevens van een ander verschaft, deze verspreidt of anderszins ter beschikking stelt met oogmerk om die ander vrees aan te jagen, ernstige overlast aan te doen of ernstig te hinderen in de uitoefening van zijn ambt of beroep. Voor het bewijs van het oogmerk kan de rechter acht slaan op onder meer uiterlijk kenbare 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 in sommige gevallen ook uit de context kunnen worden afgeleid. Dat de verdachte heeft deelgenomen aan een chatgroep waarin uiterst negatief is gesproken over het slachtoffer of de kring van personen waartoe het slachtoffer behoort, kan voor het bewijs van het oogmerk bijvoorbeeld van belang zijn als de verdachte het strafbare oogmerk ontkent. In dit voorbeeld kunnen berichten uit de chatgroep waarin kwaad wordt gesproken over het slachtoffer als bewijsmateriaal dienen, tezamen met gegevens waaruit blijkt dat de dader lid is van de chatgroep (bijvoorbeeld berichten die hij daar achterlaat) en een bericht van de dader waarin hij persoonsgegevens van het slachtoffer deelt. Het oogmerk van de dader kan ook worden bewezen met behulp van verklaringen van getuigen aan wie de dader heeft verteld wat hij van plan was met de persoonsgegevens van een ander, uit aantekeningen in een dagboek of in een document waarin de dader persoonsgegevens heeft opgeslagen of berichten van de dader aan derden (bijvoorbeeld "ik heb eindelijk het adres gevonden van X, als ze mij bij haar huis ziet zal ze wel inzien dat ze haar standpunt moet herzien"). Veel hangt derhalve af van hetgeen uit objectieve feiten en omstandigheden blijkt over het oogmerk van de dader.

Deze leden vragen vervolgens hoe het oogmerk zich verhoudt tot 'opzet' of 'voorwaardelijk opzet'.

Om strafbaar te zijn moet de verdachte de bedoeling hebben – het oogmerk – om het slachtoffer vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in zijn beroepsuitoefening. Aan het oogmerkvereiste kan zijn voldaan als de verdachte het gevolg van zijn gedraging heeft beseft en (mede) heeft beoogd. Het is niet voldoende dat hij daarmee eventueel rekening heeft gehouden en dat op de koop heeft toegenomen. Voorwaardelijk opzet is dus niet voldoende voor strafbaarheid van het gebruik van persoonsgegevens voor intimiderende doeleinden.

Ook vragen deze leden wanneer een journalist in de uitoefening van zijn of haar beroep of een klokkenluider het oogmerk heeft een ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in zijn beroepsuitoefening. Zij vragen daarbij welke criteria de rechter moet aanhouden om te beoordelen of iemand handelt vanuit journalistieke motieven.

De strafbaarstelling heeft uitsluitend betrekking op personen die persoonsgegevens verzamelen en verspreiden met kwaadaardige bedoelingen. Bij het bepalen of iemand die persoonsgegevens van een ander verzamelt of verspreidt zich schuldig heeft gemaakt aan strafbare doxing staat het oogmerk van diegene centraal, niet de hoedanigheid van de verdachte. Bij journalisten en klokkenluiders die nieuwsfeiten en misstanden openbaar maken – wat doorgaans eenvoudig zal kunnen worden opgemaakt uit de aard van een publicatie – zal van strafbaarheid geen sprake zijn. Als de intentie bij het vergaren, samenbrengen en publiceren van persoonsgegevens is gericht op nieuwsgaring of op het aan de kaak stellen van misstanden, is het oogmerk immers niet gericht op vrees aanjagen, ernstige overlast aandoen of ernstig hinderen in de beroepsuitoefening en is de betrokkene dus niet strafbaar op grond van het voorgestelde artikel 285d Sr. Het openbaar ministerie zal in dergelijke gevallen dan ook geen vervolging instellen en de rechter zal deze ook niet hoeven te beoordelen.

Voorts hebben de leden van de fracties van **GroenLinks** en de **PvdA** gevraagd of het retweeten of anderszins verder verspreiden van persoonsgegevens een zelfstandig strafbaar feit oplevert, welke rol de omvang van de verspreiding (bijvoorbeeld het aantal volgers) daarbij speelt en hoe de impact van de verspreiding meegenomen wordt in de strafbepaling.

Het verspreiden van persoonsgegevens, ook het verder verspreiden van gegevens nadat een ander die gegevens openbaar heeft gemaakt, is strafbaar op grond van het voorgestelde artikel 285d Sr als degene die dit doet daarbij het oogmerk heeft de ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de beroepsuitoefening. Voor strafbaarheid is het niet van belang hoeveel personen kennis hebben genomen of kennis kunnen hebben nemen van de persoonsgegevens. In voorkomende gevallen kan de kring van personen aan wie persoonsgegevens van een ander worden verstrekt wel worden betrokken bij de

beoordeling van het oogmerk van de betrokkene bij de verstrekking, bijvoorbeeld bij het bepalen of het oogmerk was gericht op het veroorzaken van ernstige overlast of ernstige hinder. Bij een verzoek tot het plegen van een telefoontje kan het bijvoorbeeld uitmaken of dit aan een persoon wordt gestuurd of aan een grote groep. De omvang van de verspreiding van de gegevens zal daarnaast van belang kunnen zijn bij de beslissing of vervolging wordt ingesteld, bij het bepalen van de strafeis en bij de strafoplegging.

Ten aanzien van het oogmerkvereiste vragen deze leden met het oog op de rechtspraktijk een voorbeeld te geven van zowel vrees, ernstige overlast en ernstige hinder in de uitoefening van ambt of beroep en van gedragingen die (net) niet zijn bedoeld te vallen onder vrees, ernstige hinder of ernstige overlast.

Graag verduidelijk ik wat onder vrees, ernstige overlast en ernstige hinder in de beroepsuitoefening kan worden verstaan. Daarbij merk ik op dat zich in de praktijk situaties zullen voordoen die nu niet zijn te voorzien. Op basis van de concrete feiten en omstandigheden van een geval zal moeten worden bepaald of sprake is van strafbare doxing. Ik kan uiteraard wel enkele voorbeelden van gedragingen noemen. Bij een gedraging die vreesaanjagend is kan in dit verband bijvoorbeeld worden gedacht aan het aan een slachtoffer laten weten dat wordt beschikt over zeer persoonlijke gegevens van diegene of diens naasten, bijvoorbeeld de school van de kinderen en het tijdstip waarop ze in de ochtend naar school gaan. Van ernstige overlast kan bijvoorbeeld sprake zijn als een adres wordt gedeeld met de oproep aan velen om daar op een bepaald tijdstip te verzamelen met zoveel mogelijk hooibalen. Dat kan er immers toe leiden dat de betrokkene de woning niet meer (ongestoord) kan verlaten. Een gedraging die ernstige hinder in de uitoefening van de functie veroorzaakt is het publiceren van functieaanduidingen en foto's van personen die hun functie alleen in anonimiteit kunnen verrichten, zoals bij een undercoveragent het geval is. Het is niet uitgesloten dat een gedraging zowel vreesaanjagend als ernstig overlastgevend is of ernstige hinder veroorzaakt. In het geval van de undercoveragent kan bijvoorbeeld ook sprake zijn van het aanjagen van vrees als hierdoor een dreiging kan ontstaan vanuit een bepaalde criminele groepering richting de agent. Bij gedragingen die niet voldoende ernstig zijn om vrees aan te jagen, ernstige overlast te veroorzaken of ernstig te hinderen in de uitoefening van ambt of beroep kan worden gedacht aan het voor de werklocatie aanspreken van een persoon met een publieke functie, een enkel irritant telefoontje of onaardig kaartje, of het eenmalig bestellen en bij het slachtoffer laten bezorgen van een ongewenst artikel. Dergelijke gedragingen kunnen vervelend zijn, maar daarbij zal niet bij voorbaat sprake behoeven te zijn van vrees, ernstige overlast of ernstige hinder in de uitoefening in ambt of beroep. Als de betrokkene zich persoonsgegevens verschaft of aan iemand anders persoonsgegevens van een ander stuurt, ten behoeve van het begaan van deze gedragingen, zal dat in die gevallen geen strafbare doxing opleveren.

De leden van de **D66**-fractie hebben gevraagd waarom in de delictsomschrijving de afbakening is gemaakt bij 'ernstige' overlast en 'ernstige' hinder. Zij vragen of de rechter niet met een lastige afweging wordt opgezadeld als de verdachte zich er in de rechtszaal op beroept dat hij slechts geringe overlast of geringe hinder wilde veroorzaken.

In de omschrijving van het voor strafbaarheid vereiste oogmerk is een grens getrokken tussen gedragingen die naar de maatstaven van fatsoen als onbehoorlijk moeten worden beschouwd en gedragingen die vallen onder de voorgestelde strafbaarstelling. Strafwaardig zijn de gedragingen waarbij uit het oogmerk blijkt van een gerichte wil om anderen te intimideren. Daarvan hoeft nog geen sprake te zijn in gevallen van 'gewone' hinder en overlast. Of in een specifiek geval het oogmerk aanwezig is om iemand ernstige overlast aan te doen of iemand ernstig te hinderen in de uitoefening van ambt of beroep, zal moeten worden beoordeeld op basis van de omstandigheden die zich in dat geval voordoen. In mijn antwoord op de voorgaande vraag van de leden van de fracties van **GroenLinks** en de **PvdA** noemde ik al enkele voorbeelden van gedragingen die naar mijn mening niet onder het bereik van de voorgestelde strafbaarstelling zouden moeten vallen. Daarbij speelt ook mee dat deze strafbaarstelling een beperking van de vrijheid van meningsuiting betreft. Voor de beoordeling of een beperking van de vrijheid van meningsuiting gerechtvaardigd is, is onder meer van belang of daartoe een dringende maatschappelijke noodzaak bestaat. In dit geval is de maatschappelijke noodzaak gelegen in de ingrijpende en schadelijke effecten die strafbare doxing kan hebben op het persoonlijke leven van slachtoffers (artikel 10 EVRM). Bij het gebruik van persoonsgegevens voor intimiderende doeleinden wordt een grens overschreden vanwege de ernstige inbreuk op het persoonlijk leven van slachtoffers. Een beperking kan alleen noodzakelijk zijn voor zover deze ook proportioneel is. Daarom gaat de voorgestelde strafbaarstelling niet verder dan strikt noodzakelijk en is deze gericht op gevallen waarin persoonsgegevens van anderen worden verzameld en verspreid met het oogmerk 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. Of de drempel hiermee inderdaad juist is gelegd of dat deze toch te hoog is zal ik, zoals ik ook heb toegezegd bij de behandeling van dit wetsvoorstel in de Tweede Kamer, betrekken bij de invoeringstoets over dit wetsvoorstel.

De leden van de **D66**-fractie hebben gevraagd naar het zich verschaffen van persoonsgegevens voor intimiderende doeleinden. Zij hebben twijfels bij de handhaafbaarheid hiervan omdat het oogmerk in die gevallen niet bekend zal worden en vragen de regering of zij de handhaving van de strafbaarstelling van het zich verschaffen nader kan toelichten.

Bij het zich verschaffen van persoonsgegevens kan aan verschillende situaties worden gedacht: iemand vraagt anderen persoonsgegevens te verstrekken of iemand gaat daar geheel zelfstandig naar op zoek. Dit zich verschaffen van persoonsgegevens zal moeten plaatsvinden voordat gegevens daadwerkelijk kunnen worden gebruikt om een ander te intimideren. Op grond van de voorgestelde bepaling is dit strafbaar als de betrokkene op het moment van het zich verschaffen van persoonsgegevens van een ander het oogmerk had diegene te intimideren.

De bedoeling van een persoon bij het verzamelen van gegevens zal niet altijd duidelijk kunnen zijn. Maar er zullen zich situaties kunnen voordoen waarin wel kan worden bewezen dat de verdachte zich persoonsgegevens heeft verschaft met het oogmerk van intimidatie. Bijvoorbeeld als een lijst van persoonsgegevens wordt aangetroffen bij een doorzoeking en de verdachte of een getuige verklaart dat deze zijn verzameld om de betrokkenen thuis 'een aangekleed bezoekje' te kunnen brengen. De mogelijke bewijsproblematiek met betrekking tot subjectieve bestanddelen in een delictsomschrijving doet niet af aan de strafwaardigheid van de gedraging. Dat in deze fase strafrechtelijk optreden al mogelijk wordt en daarmee de aanmerkelijke kans wordt verkleind dat meer schade wordt toegebracht, is daarbij eveneens van betekenis. Politie en justitie mogen niet met lege handen staan als bijvoorbeeld tijdens een doorzoeking een omvangrijke selectie persoonsgegevens wordt aangetroffen waarvan duidelijk is dat deze met kwaadwillende bedoelingen zijn verzameld. De handhaving van de strafbaarstelling zal naar verwachting beperkt zijn tot dit soort gevallen, waarin het oogmerk van de betrokkene bij het zich verschaffen van persoonsgegevens bekend wordt.

Ook de leden van de **SGP**-fractie hebben gevraagd naar de strafbaarstelling van het zich verschaffen van persoonsgegevens van een ander voor intimiderende doeleinden. Deze leden hebben gevraagd wanneer het zich verschaffen van persoonsgegevens strafbaar wordt. Daarbij veronderstellen zij dat intimiderende doeleinden zich pas openbaren na het verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde. Zij hebben gevraagd of de verdachte met terugwerkende kracht strafbaar wordt als hij later het oogmerk krijgt om reeds verschafte gegevens te gebruiken met het oogmerk een ander vrees aan te jagen.

Voor strafbaarheid op grond van het voorgestelde artikel 285d Sr is het oogmerk van de dader op het moment van het zich verschaffen, verspreiden of anderszins ter beschikking stellen van gegevens bepalend. Als dit oogmerk op dat moment was gericht op het vrees aan (laten) jagen, ernstige overlast aan (laten) doen of ernstig (laten) hinderen in de uitoefening van ambt of beroep is de dader strafbaar. Als de betrokkene over persoonsgegevens beschikt en op enig moment het idee krijgt om deze gegevens te gebruiken om een ander te intimideren wordt hij niet met terugwerkende kracht strafbaar vanwege het zich verschaffen van die gegevens. Dan is de betrokkene wel strafbaar als hij de persoonsgegevens verspreid met voormeld oogmerk. Overigens kan het oogmerk van een dader reeds bekend worden ten tijde van het zich verschaffen van persoonsgegevens, bijvoorbeeld als de betrokkene in een appgroep vraagt persoonsgegevens van een bepaalde groep personen te delen omdat hij diegenen wil intimideren.

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

In het door de leden van de SGP-fractie genoemde voorbeeld waarbij de verstrekker geen weet heeft van de intimiderende doeleinden van de ontvanger, zal geen sprake zijn van strafbaar handelen van de kant van de verstrekker. De verstrekker heeft namelijk niet het voor de strafbare intimidatie vereiste oogmerk. Om tot een bewezen feit te komen is inderdaad een vorm van opzet vereist, te weten het oogmerk van intimidatie. Het oogmerk van de verdachte bij de strafbaar gestelde gedragingen met de persoonsgegevens van een ander of een derde moet zijn gericht op het (laten) aanjagen van vrees, het (laten) aandoen van ernstige overlast of ernstig (laten)

hinderen in de uitoefening van ambt of beroep. Dit moet worden vastgesteld om tot een bewezen feit te komen.

4. Delictsomschrijving

De leden van de **D66**-fractie hebben gevraagd of het wel klopt dat dreigen met doxing binnen de delictsomschrijving van de strafbaarstelling valt. Daarbij hebben zij specifiek gevraagd naar het geval dat iemand dreigt om persoonsgegevens van een ander te zullen delen, zonder dat deze zich reeds de persoonsgegevens heeft verschaft, verspreid of anderszins ter beschikking gesteld. Bijvoorbeeld de situatie dat iemand op internet een bericht van een anoniem account krijgt met het dreigement waarin staat dat zijn of haar persoonsgegevens openbaar zullen worden gemaakt, zonder dat degene die hiermee dreigt zich de persoonsgegevens reeds heeft verschaft, deze heeft verspreid of anderszins ter beschikking heeft gesteld. Volgens deze leden kan dit dreigement dezelfde schadelijke gevolgen hebben voor het slachtoffer als bij 'echte doxing'.

In de meeste gevallen waarin iemand dreigt met doxing zal diegene het oogmerk hebben de ander vrees aan te jagen, ernstige overlast aan te doen of ernstig te hinderen in de uitoefening van zijn ambt of beroep. Om te bepalen of diegene strafbaar is, zal moeten worden vastgesteld of diegene zich ook met dit oogmerk persoonsgegevens van de ander heeft verschaft, deze heeft verspreid of anderszins ter beschikking heeft gesteld. Dat zal al snel het geval zijn. Om contact op te kunnen nemen met degene tegen wie het dreigen met doxing is gericht zal de dader immers over persoonsgegevens van diegene moeten beschikken. In het door de leden van de **D66**-fractie genoemde voorbeeld zal het kunnen gaan om de gegevens die nodig zijn om diegene een bericht te sturen zoals een username of emailadres. In dergelijke gevallen valt dreigen met doxing onder de delictsomschrijving van de strafbaarstelling. Situaties waarbij de betrokkene dreigt met doxing maar daarvoor geen persoonsgegevens heeft verzameld of verspreid laten zich moeilijk voorstellen. Wanneer een slachtoffer door het dreigen met doxing zou worden gedwongen iets te doen, niet te doen of te dulden, bijvoorbeeld doordat daaraan een bepaalde voorwaarde wordt verbonden, zou overigens ook sprake kunnen zijn van strafbare dwang (artikel 284 Sr; artikel 297 Sr BES).

Vervolgens hebben de leden van de **D66**-fractie gevraagd of het verspreiden dan wel in bezit hebben van persoonsgegevens onder de reikwijdte van de strafbaarstelling valt als degene van wie die persoonsgegevens zijn, van niets weet en geen deel uitmaakt van de besloten app-groep. Zij vragen of het element van intimidatie uit de strafbaarstelling dan aanwezig is.

Het is voor strafbaarheid op grond van de voorgestelde strafbaarstelling niet bepalend dat degene van wie de persoonsgegevens zijn weet heeft van het feit dat diens persoonsgegevens zijn gevraagd of verspreid. Van belang is dat het oogmerk bij het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens erop is gericht om die ander vrees aan te jagen dan wel aan te laten jagen, ernstige overlast aan te doen dan wel aan te laten doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel ernstig te laten hinderen. Het verzamelen of verspreiden van persoonsgegevens hoeft op zichzelf niet het intimiderend effect te sorteren; het gaat om de bedoeling waarmee de betrokkene deze handelingen verricht. Er kan bijvoorbeeld worden gevraagd naar een adres dat kan worden gebruikt om het slachtoffer een huisbezoek te brengen. Ook kan een adres worden verspreid zodat anderen het slachtoffer thuis kunnen bezoeken. Het feit dat het slachtoffer hiermee, als dit in een besloten app-groep gebeurt waarvan het slachtoffer geen lid is, niet bekend is betekent niet dat dit toelaatbaar is. In het genoemde voorbeeld delen de leden van de appgroep gezamenlijk het oogmerk om de verspreide persoonsgegevens te gebruiken om het slachtoffer te intimideren. Strafbaarstelling is nodig om daartegen op te kunnen treden.

5. BES

De leden van de fracties van **GroenLinks** en de **PvdA** hebben gevraagd op welke wijze met de bestuurscolleges en/of de eilandsraden van de BES overleg is geweest over de vraag of deze strafbaarstelling op gelijke wijze wenselijk is in Caribisch Nederland en of er wellicht lokale aanpassingen nodig waren.

De voorgestelde strafbaarstelling is ter consultatie voorgelegd aan de openbare lichamen in Caribisch Nederland. Het Openbaar Lichaam Bonaire heeft in reactie op dit wetsvoorstel aangegeven 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. Ook het College bescherming persoonsgegevens BES heeft advies uitgebracht over het wetsvoorstel. Daarin wordt de noodzaak van de strafbaarstelling van doxing onderschreven omdat misbruik van persoonsgegevens voor intimiderende doeleinden ernstige schade kan toebrengen. De ontvangen

adviezen hebben geen aanleiding gegeven om in een aangepaste strafbaarstelling voor Caribisch Nederland te voorzien.

Naar aanleiding van het advies van de Raad van State waarin werd geadviseerd in de toelichting nader in te gaan op de strafbaarstelling van doxing in Caribisch Nederland is nogmaals informeel ambtelijk contact opgenomen met het Korps Politie Caribisch Nederland en het openbaar ministerie BES. Ook uit dat contact is niet gebleken dat lokale aanpassingen in de strafbaarstelling nodig zijn. Daarom is – conform het uitgangspunt van het kabinetsbeleid dat alle Nederlanders gelijkwaardig behandeld worden waaruit volgt dat de burgers in Caribisch Nederland hetzelfde niveau van strafrechtelijke bescherming wordt geboden - aangesloten bij de formulering van de strafbepaling zoals deze in Nederland is voorgesteld. Zo kan worden voorkomen dat degenen die zich in Caribisch Nederland schuldig maken aan doxing straffeloos blijven.

6. Verhouding andere wetgeving

De leden van de fracties van **GroenLinks** en de **PvdA** hebben gevraagd in hoeverre de nieuwe wetgeving en wetgevingsvoorstellen vanuit de Europese Unie met betrekking tot sociale media en het internet, zoals de Digital Markets Act en de Digital Services Act, een bijdrage leveren aan het voorkomen van strafbare doxing en het snel offline halen van content die strafbare doxing inhoudt.

De Digital Services Act biedt geharmoniseerde regels voor tussenhandeldiensten, inclusief regels over wat zij moeten doen met illegale content. Door het gebruik van persoonsgegevens voor intimiderende doeleinden strafbaar te stellen wordt duidelijk gemaakt dat berichten waarmee deze strafbare gedraging wordt gepleegd, gezien kunnen worden als illegale content. Dat betekent onder andere dat na inwerkingtreding van de Digital Services Act meldingen over strafbare doxing door slachtoffers rechtstreeks bij hostingservices moeten kunnen worden gedaan en dat er bij kennis van het bestaan van strafbare doxing bij de dienst prompt wordt gehandeld om deze illegale informatie te verwijderen.

De leden van de fracties van **GroenLinks** en de **PvdA** hebben daarnaast gevraagd of het zich verschaffen van persoonsgegevens niet strafbaar zou zijn als poging tot doxing op grond van artikel 45 Sr als het als het 'zich verschaffen' van persoonsgegevens niet als gedraging in de delictsomschrijving zou zijn opgenomen. Zij hebben gevraagd of het wenselijk is om tevens de 'poging tot verschaffen' van persoonsgegevens met het oogmerk om – kort gezegd – strafbare doxing te plegen, ook al strafbaar te stellen en hoe dit zich verhoudt tot het wettelijke systeem waarin alleen voor ernstige delicten met een strafbedreiging van 8 jaar of meer ook de voorbereiding strafbaar gesteld is via artikel 46 Sr.

Inderdaad zou het zich verschaffen van persoonsgegevens in sommige gevallen een strafbare poging tot het gebruik van persoonsgegevens voor intimiderende doeleinden kunnen opleveren, ook als het 'zich verschaffen' van persoonsgegevens voor intimiderende doeleinden niet zou zijn opgenomen in de delictsomschrijving en daarmee niet strafbaar zou zijn op grond van de voorgestelde strafbepaling. Een strafbare poging tot doxing kan bijvoorbeeld aan de orde zijn als het verspreiden van de persoonsgegevens niet zou zijn gelukt vanwege een technisch probleem bij de verspreiding. Een essentiële voorwaarde voor een strafbare poging is namelijk dat het delict (de strafbare doxing) niet wordt voltooid vanwege een van de wil van de dader onafhankelijke omstandigheid. Iemand kan zich echter ook persoonsgegevens verschaffen van een ander om die ander daarmee in de fysieke wereld vrees aan te jagen, ernstige overlast te veroorzaken of ernstig te hinderen in de uitoefening van ambt of beroep. Als het handelen van de betrokkene zich hiertoe heeft beperkt, is er nog geen sprake van een strafbare poging tot verspreiding van persoonsgegevens. Zoals ik heb toegelicht in mijn antwoord op een vraag van de leden van de **D66**-fractie is ook dergelijk handelen op zichzelf strafwaardig en is strafbaarstelling wenselijk (zie ook paragraaf 3).

Een strafbare poging tot doxing is echter niet ondenkbaar. Een voorbeeld is de situatie waarin in een appgroep persoonsgegevens worden gevraagd maar deze gegevens niet beschikbaar bleken. Net als voor alle andere misdrijven geldt dat een poging tot het plegen van een misdrijf strafbaar is als het voornemen van de dader zich door een begin van uitvoering heeft geopenbaard (artikel 45, eerste lid, Sr). De verhouding tot de zelfstandige strafbaarstelling van voorbereidingshandelingen voor zeer ernstige misdrijven – waarnaar deze leden ook vroegen – bestaat daarin, dat dergelijke strafbaarstellingen het niet laten aankomen op een begin van uitvoering, hetgeen dus onder de voorgestelde strafbaarstelling wel wordt vereist.

Vervolgens hebben de leden van de fracties van **GroenLinks** en de **PvdA** gevraagd waarom er niet voor is gekozen het doen van een oproep om persoonsgegevens te delen met het oogmerk om daar vervolgens strafbare doxing mee te plegen strafbaar te stellen, in plaats van het 'zich verschaffen' van de persoonsgegevens. Deze leden hebben tevens gevraagd in welke

omstandigheden (een poging tot) het verschaffen van persoonsgegevens voor intimiderende doeleinden dermate laakbaar is dat deze strafbaar gesteld moet worden, maar niet al valt onder een ander strafbaar feit, met name de misdrijven met betrekking tot (persoons)gegevens zoals computervredebreuk (artikel 138ab Sr) of het overnemen van niet-openbare computergegevens (artikel 138c Sr).

Graag beantwoord ik de vraag van deze leden waarom 'zich verschaffen' in de strafbaarstelling niet is vervangen door het doen van een oproep om persoonsgegevens te delen, als volgt. Het 'zich verschaffen van persoonsgegevens' voor intimiderende doeleinden kan in samenwerking met diverse betrokkenen plaatsvinden. Onder die omstandigheden zal strafbaarheid kunnen worden aangenomen wegens medeplegen van doxing. Maar het 'zich verschaffen van persoonsgegevens' kan ook geheel zelfstandig gebeuren en ook die delictsvorm dient – zoals hiervoor toegelicht – strafbaar te zijn. Reeds hierom is niet overwogen de delictsgedraging 'zich verschaffen' te vervangen door 'het doen van een oproep om persoonsgegevens te delen' te plegen. Voor zover het gaat om de strafbaarheid van het aanzetten van anderen tot doxing kan worden volstaan met strafbaarheid op grond van artikel 46a Sr (poging om een ander te bewegen een misdrijf te begaan) en de deelnemingsvorm uitlokking, op grond waarvan degenen strafbaar zijn die iemand door giften, beloften, misbruik van gezag, geweld, bedreiging, of misleiding of door het verschaffen van gelegenheid, middelen of inlichtingen pogen te bewegen tot strafbare doxing of daarmee strafbare doxing opzettelijk uitlokken.

In reactie op de vraag van deze leden waarom bij het zich verschaffen van persoonsgegevens geen sprake is van een ander strafbaar feit, zoals computervredebreuk (artikel 138ab Sr) of het overnemen van niet-openbare computergegevens (artikel 138c Sr) merk ik op dat het bij die misdrijven gaat om niet-openbare gegevens. Van computervredebreuk is sprake als opzettelijk en wederrechtelijk wordt binnengedrongen in een geautomatiseerd werk. Dat kan uiteraard worden gedaan om daarmee niet-openbare gegevens te verkrijgen. Bij het eerdergenoemde overnemen van computergegevens gaat het om het opzettelijk en wederrechtelijk overnemen of doorgeven van niet-openbare gegevens. Voor doxing wordt vaak informatie gebruikt die openbaar is, zonder dat opzettelijk en wederrechtelijk een computer wordt binnengedrongen («hacken») of opzettelijk en wederrechtelijk gegevens worden overgenomen. Het gaat bijvoorbeeld om een combinatie van gegevens over een persoon uit verschillende bronnen. Denk daarvoor aan de gegevens die in een zeer beperkte kring van personen bekend zijn, zoals een huisadres of gegevens over de deelname aan een bepaald sportevenement die online zijn geplaatst. Voor strafbaarheid wegens doxing is de wijze van verkrijging van deze gegevens niet relevant. Strafrechtelijke aansprakelijkheid ontstaat zonder dat sprake hoeft te zijn van het hacken van een computer om deze gegevens te verkrijgen of van het overnemen van niet-openbare gegevens uit een computer, van een ander misdrijf hoeft dan nog geen sprake te zijn.

De leden van de fracties van **GroenLinks** en de **PvdA** hebben ook gevraagd hoe het oogmerk tot vrees, ernstige overlast of ernstige hinder kan worden bewezen bij alleen het verschaffen van persoonsgegevens. Zij hebben gevraagd hiervan een voorbeeld te geven. Daarnaast hebben zij gevraagd naar het onderscheid tussen deze specifieke strafbaarstelling van het zich verschaffen van persoonsgegevens voor intimiderende doeleinden en strafrechtelijke afpersing of bedreiging.

Voor een antwoord op de eerste vraag van deze leden verwijs ik graag naar paragraaf 3 van deze memorie waarin ik met behulp van voorbeelden heb verduidelijkt hoe het voor strafbaarheid vereiste oogmerk kan worden bewezen.

De strafbaarstelling van doxing ziet op andere gedragingen dan de strafbaarstellingen van bedreiging en afpersing. Voor strafbare bedreiging (artikel 285 Sr; artikel 298 Sr BES) is vereist dat iemand wordt bedreigd met bepaalde ernstige misdrijven. Een voorbeeld van strafbare doxing betreft het in een appgroep vragen naar het adres van een bepaald persoon zodat diegene 'de waarheid kan worden verteld'. Dergelijk handelen levert geen strafbare bedreiging op, omdat niet wordt bedreigd met een bepaald ernstig misdrijf, zoals omschreven in het eerste lid van het voorgestelde artikel 285 Sr. Van afpersing (artikel 317 Sr) is in dit geval ook geen sprake omdat daarvoor is vereist dat iemand, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, een ander door geweld of bedreiging met geweld dwingt tot de afgifte van een goed, tot het aangaan van een schuld of het ter beschikking stellen van gegevens. Voor de vervulling van de delictsomschrijving van het voorgestelde artikel 285d Sr is niet vereist dat iemand ergens toe wordt gedwongen, maar dat de dader zich persoonsgegevens verschaft, deze verspreidt of anderszins ter beschikking stelt met de bedoeling angst, ernstige hinder of overlast te veroorzaken. Ook wat oogmerk betreft verschilt het voorgestelde artikel 285d Sr dus met artikel 317 Sr waar het in laatstgenoemd artikel is gericht op wederrechtelijke bevoordeling.

De leden van de **D66**-fractie hebben gevraagd wie strafrechtelijk verantwoordelijk is als zelflerende algoritmes de persoonsgegevens van iemand verspreiden teneinde te intimideren en wat de rol van sociale media-platforms is in deze.

Het scenario dat leden van de **D66**-fractie hebben beschreven is technisch erg complex. Een dergelijk algoritme of systeem zou in eerste instantie zelfstandig informatie van webpagina's moeten zoeken, vinden en bewaren, om vervolgens een plek te creëren om de informatie te publiceren. Het algoritme of systeem zou dan bijvoorbeeld zelf een account moeten maken op social media (waar die platformen dan ook op kunnen ingrijpen) of een website moeten bouwen om de informatie op te plaatsen. Dat is een erg complexe serie 'handelingen' en vraagt dermate veel rekenkracht dat het zeer onwaarschijnlijk is dat dit zonder menselijke aansturing zal kunnen gebeuren. Indien menselijke aansturing wel mogelijk zou zijn, is diegene die aanstuurt ook verantwoordelijk en kan diegene daarvoor eventueel ook strafrechtelijk aansprakelijk zijn.

Ook hebben de leden van de D66-fractie gevraagd of, en zo ja, hoe algoritmes gaan worden ingezet bij de opsporing van doxing.

In algemene zin kan gesteld worden dat het zoeken naar persoonsgegevens op internet nagenoeg alleen kan met gebruikmaking van algoritmes. Dat geldt bijvoorbeeld al voor een eenvoudige zoekslag met google search in voor het brede publiek toegankelijke bronnen, waarvoor Google algoritmes gebruikt. Hiervan kan de politie, binnen haar bestaande bevoegdheden, ook gebruik maken wanneer gezocht wordt op persoonsgegevens van een slachtoffer van doxing. Of het, na inwerkingtreding van het wetsvoorstel, noodzakelijk zal zijn om aanvullende middelen in te zetten, hangt af van onder meer het aantal en het type zaken. Daar kan op dit moment nog weinig over worden gezegd, anders dan dat dit binnen de bestaande opsporingsbevoegdheden zal moeten passen.

7. Aangifte

De leden van de **D66**-fractie hebben gevraagd wie naast het slachtoffer aangifte kunnen doen van strafbare doxing. Zij hebben gevraagd of maatschappelijke organisaties of het in 2024 operationeel wordende meldpunt doxing dit ook kunnen.

Er dient een onderscheid te worden gemaakt tussen het doen van een aangifte van strafbare doxing bij de politie en het melden van doxing bij tussenhandeldiensten. Door de strafbaarstelling worden slachtoffers in staat gesteld om aangifte te doen van het gebruik van persoonsgegevens voor intimiderende doeleinden. Ook anderen die daarvan kennis dragen kunnen aangifte doen (artikel 161 Sv). De politie heeft overigens geen aangifte nodig om een opsporingsonderzoek te kunnen starten.

Slachtoffers kunnen daarnaast een melding van strafbare doxing doen bij tussenhandeldiensten met een verzoek tot verwijdering van gegevens waarmee dit feit is gepleegd of een melding hiervan doen via een meldpunt. Meldpunten hebben specifieke expertise op het gebied van illegale inhoud en kunnen verzoeken doen bij tussenhandeldiensten om deze inhoud te verwijderen. Meldpunten kunnen de informatie die zij ontvangen doorgeven aan de politie ten behoeve van een opsporingsonderzoek, maar hebben niet tot taak aangifte te doen van strafbare feiten. Voorbeelden van bestaande meldpunten zijn het Expertisebureau Online Kindermisbruik (EOKM) en het Meldpunt internet discriminatie (MiND). Voor doxing en andere onrechtmatige online content wordt in de loop van 2024 een laagdrempelige meldvoorziening opgezet die content kan classificeren en illegale content met een verwijderverzoek kan doorgeleiden naar internet tussenpersonen. Dat is een maatregel die de druk op de strafrechtketen en op de civiele rechter moet verminderen.

Deze leden hebben ook gevraagd of een platform medeplichtig is aan doxing als het persoonsgegevens van het slachtoffer niet op verzoek van het slachtoffer worden verwijderd. Daarnaast hebben zij gevraagd of het slachtoffer het platform (mede-) aansprakelijk kan stellen voor (inmiddels) geleden schade als het platform uitvoering geeft aan het bevel van officier van justitie om persoonsgegevens ontoegankelijk te maken.

Artikel 6:196c BW regelt de vrijstellingen voor aansprakelijkheid van internettussenpersonen, overeenkomstig de Richtlijn Elektronische Handel. Deze richtlijn zal begin 2024 worden vervangen door de Digital Services Act. Tussenhandeldiensten zijn niet aansprakelijk indien ze niet weten van de activiteit of informatie met een onrechtmatig karakter op hun dienst dan wel zodra ze dat wel weten prompt handelen om de illegale inhoud te verwijderen of de toegang daartoe onmogelijk te maken. Een platform dat bij het verkrijgen van de kennis over strafbare doxing de gegevens

waarmee dit delict is gepleegd prompt verwijdert, is dus niet aansprakelijk. Of (mede-) aansprakelijkheid bestaat hangt dus af van het al dan niet voldoen aan deze voorwaarden en van de omstandigheden van het concrete geval.

De officier van justitie kan, met een machtiging van de rechter-commissaris, die enkel wordt afgegeven ingeval van verdenking van strafbare doxing of een ander strafbaar feit als bedoeld in artikel 67, eerste lid, Sv, een bevel geven om terstond alle maatregelen te nemen die redelijkerwijs van de aanbieder kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten (artikel 125p Sv). Indien de aanbieder daaraan voldoet, zal hij niet worden vervolgd (artikel 54a Sr) vanwege betrokkenheid bij een strafbaar feit dat door een ander is gepleegd met gebruikmaking van de dienst van de aanbieder.

De leden van de **SGP**-fractie hebben gevraagd of de opsporingsinstanties zoals de politie en het openbaar ministerie voldoende capaciteit hebben om van iedere aangifte van strafbare doxing serieus werk te maken. Daarbij hebben zij gewezen op het risico van secundaire victimisatie dat kan ontstaan wanneer slachtoffers zich melden, maar hun zaak op de plank blijft liggen. Deze leden hebben gevraagd of verhoogde inzet op dit onderwerp is berekend.

De politie is voorbereid op de inwerkingtreding van dit wetsvoorstel door de betreffende medewerkers op te leiden over de strafbaarstelling, en door aanpassing van de informatievoorziening zodat aangiftes van doxing kunnen worden geregistreerd. Hoeveel doxing zaken straks zullen instromen is thans nog niet bekend. Daarbij speelt mee dat deze gedraging nu niet strafbaar is, en dus ook niet wordt bijgehouden hoe vaak het nu voorkomt. De prognoses van het aantal zaken lopen om die reden ook uiteen: het openbaar ministerie verwacht een aanzienlijk aantal zaken te krijgen op het gebied van strafbare doxing, de rechtspraak verwacht geen significante stijging van het aantal zaken en de politie schat in dat het aantal aangiften niet zodanig groot gaat zijn dat er niet voldoende capaciteit voor zal zijn. Om een beter overzicht te krijgen van het daadwerkelijk aantal zaken en de werklast voor de politie, het openbaar ministerie en de rechtspraak wordt direct na inwerkingtreding een invoeringstoets gestart waarin (onder andere) wordt gemonitord hoeveel zaken er instromen en of die in de plaats komen van zaken in verband met gedragingen die nu al strafbaar zijn zoals bedreiging.

8. Geconsolideerde wettekst

De leden van de **D66**-fractie hebben gevraagd waarom geen geconsolideerde versie van dit wetsvoorstel ter beschikking is gesteld.

Dit wetsvoorstel stelt een gedraging strafbaar die nu nog niet strafbaar is, te weten het gebruik van persoonsgegevens voor intimiderende doeleinden. Omdat het hier slechts gaat om enkel een toevoeging van een nieuwe strafbaarstelling aan het Wetboek van Strafrecht en het Wetboek van Strafrecht BES, zou een geconsolideerde doelwet in dit geval weinig toegevoegde waarde hebben voor de beoordeling van het wetsvoorstel. Daarom wordt geen aanleiding gezien een geconsolideerde versie van het Wetboek van Strafrecht en het Wetboek van Strafrecht BES, die dus slechts op een enkel onderdeel worden gewijzigd, ter beschikking te stellen.

De Minister van Justitie en Veiligheid,