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 identificerende persoonsgegevens voor intimiderende doeleinden (strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden)

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 identificerende persoonsgegevens boven water te krijgen. Die publieke toegankelijkheid van bronnen als het internet en de bereikbaarheid van anderen met social media bieden kwaadwillenden de mogelijkheid om deze identificerende persoonsgegevens te gebruiken om mensen vrees aan te jagen, te intimideren en te bedreigen. Dit kan resulteren in gedragingen die zodanig intimiderend zijn dat deze gedragingen naar de huidige in de maatschappij levende opvattingen als uiterst onwenselijk en strafwaardig worden gezien. Eén van deze onwenselijke en strafwaardige gedragingen is het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens voor intimiderende doeleinden, een gedraging die samenhangt met 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).

Het begrip 'doxing' is een term die wordt gebruikt door hackers en is afgeleid van het Engelse woord 'documents'. Hierbij worden identificerende persoonsgegevens geopenbaard met als doel een bepaald persoon vrees aan te jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn functie te belemmeren. Doxing kan grote impact hebben op de beoogde slachtoffers en hun naasten, op de groep waartoe zij behoren of van wie verondersteld wordt 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 doxing 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. Zeer onlangs is in de nationale media aandacht geschonken aan gevallen van doxing waarbij identificerende persoonsgegevens werden gebruikt voor intimiderende doeleinden, en 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. Bij anderen werd een vuurwerkbom in de tuin gegooid. 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 aan politieambtenaren naar voren.[1] Zo is een tijd lang getracht om de identiteit van undercoveragenten te onthullen.

Uitingsvormen die zich niet concreet openbaren in bijvoorbeeld bedreiging, belediging en dwang zijn veelal niet te kwalificeren als een strafbaar feit. Dit terwijl de consequenties ervan voor het leven van de betrokkenen groot kunnen zijn. Slachtoffers worden geïntimideerd en voelen zich niet meer veilig. Dit kan ertoe leiden dat zij zich anders gaan gedragen, zich in hun vrijheid belemmerd voelen, en niet meer naar buiten durven te treden, noch in de fysieke wereld, noch online. Deze ontwikkeling is zeer kwalijk. Eenieder moet zich veilig kunnen voelen. Het delen van andermans persoonsgegevens mag er niet toe leiden dat anderen zich daardoor in hun persoonlijke vrijheid of beroep beknot voelen. Daarom wordt voorgesteld het gebruik van identificerende 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 is onacceptabel

[1] https://www.politie.nl/binaries/content/assets/politie/onderwerpen/geweld-tegen-politieambtenaren/gtpa-cijfers-2017-tot-en-met-2020.pdf

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

Strafbaar wordt gesteld het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens van een ander of een derde met het oogmerk 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 - doxing – brengt immers teweeg dat slachtoffers zich niet meer vrij voelen in hun doen en laten vanwege het risico dat zij lopen dat hen iets zal worden aangedaan of vanwege het gevoel dat zij hebben dat hen iets zal kunnen worden aangedaan vanwege de dreiging die van de beschikbaarheid van identificerende 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 doxing, kan dit tot gevolg hebben dat zij zowel in de privésfeer als in de uitoefening van hun beroep consequenties ervaren. Gedragingen kunnen primair zijn gericht op het aanjagen van vrees of het veroorzaken van ernstige overlast voor de betrokkene en diens gezinsleden, maar ook tot gevolg hebben dat zij ernstig worden gehinderd in de uitoefening van hun 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, inmiddels is voorgesteld dit strafmaximum te verhogen tot drie jaar (Kamerstukken II 2019/20, 35564, nr. 2). Voor het gebruik van persoonsgegevens voor intimiderende doeleinden is evenwel niet vereist dat de gedraging een zodanige bedreiging met een ernstig misdrijf impliceert. Hoewel het voor belaging, strafbaar gesteld in artikel 285b Sr met een strafmaximum van drie jaar gevangenisstraf, vereiste oogmerk deels overeenkomt met dat voor het gebruik van persoonsgegevens voor intimiderende doeleinden, 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 het gebruik van persoonsgegevens voor intimiderende doeleinden ligt het zwaartepunt wat betreft de strafwaardigheid niet primair in de stelselmatige inbreuk op de persoonlijke levenssfeer maar veeleer bij het aanjagen van vrees, het veroorzaken van ernstige overlast of hinder in de uitoefening van ambt of beroep. Dit laat onverlet dat ook de inbreuk op de persoonlijke levenssfeer van de betrokkene in belangrijke mate bepalend is voor de laakbaarheid van het strafbaar te stellen gedrag.

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, strafbaar gesteld in artikel 284 Sr. Daarvoor 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 respectievelijk ten hoogste negen of vier jaren. Voor strafbaarheid wegens dwang, ambtsdwang, afdreiging of afpersing is vereist dat het slachtoffer ergens toe wordt gedwongen.[2] Ook in relatie tot deze

[2] 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 undercovers bekend in heel NL”. De rechtbank oordeelde dat de verdachten hiermee willens en

misdrijven onderscheidt de voorgestelde strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden zich 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 jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep te hinderen. In het geval het slachtoffer (nog) niet is gedwongen tot een bepaald handelen of nalaten, zal er wel sprake kunnen zijn van het strafbare gebruik van persoonsgegevens voor intimiderende doeleinden als aan de vorenbedoelde vereisten is voldaan.

Als in het openbaar identificerende persoonsgegevens worden gepubliceerd met een oproep om tegen de betrokkene een strafbaar feit te plegen, is dit eveneens strafbaar als opruiing (artikel 131 Sr). De dader van dit delict kan worden gestraft met gevangenisstraf van ten hoogste vijf jaren. Daarnaast kan een dergelijke gedraging, afhankelijk van de inhoud van het gepubliceerde bericht, het aanzetten tot haat of discriminatie (artikel 137d Sr) of belediging (artikel 261 Sr) opleveren. In dergelijke situaties zal steeds moeten worden bezien welk verwijt de dader wordt gemaakt. De beslissing of vervolging wordt ingesteld en welk strafrechtelijk verwijt de dader wordt gemaakt is aan het openbaar ministerie en zal afhankelijk zijn van de omstandigheden van het geval. Voor de volledigheid wordt opgemerkt dat het gebruik van persoonsgegevens voor intimiderende doeleinden niet moet worden gezien als een bijzondere vorm van opruiing. Voor opruiing is vereist dat anderen worden opgeroepen een strafbaar feit te plegen. Hoewel het oproepen een strafbaar feit tegen iemand te plegen 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. In voorkomende gevallen lijkt het, vanwege de ernst van de gedraging, dan ook aangewezen dat een verdachte wordt vervolgd vanwege opruiing.

Het gebruik van persoonsgegevens voor intimiderende doeleinden wordt strafbaar gesteld omdat in sommige gevallen geen overlap bestaat met bestaande strafbaarstellingen terwijl strafrechtelijk optreden wel wenselijk is. Deze strafbaarstelling voorziet daarmee in een aanvulling op de strafbepalingen waarmee andere vormen van intimidatie, zoals bedreiging en belaging, strafbaar zijn gesteld.

Het openbaar ministerie kan een strafrechtelijk onderzoek starten naar aanleiding van een verdenking van het gebruik van persoonsgegevens voor intimiderende doeleinden. 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. Het mogelijk intimiderende effect van de gedraging zal het slachtoffer kunnen weerhouden van het doen van aangifte vanwege de mogelijke consequenties die dit voor hem en zijn naasten kan hebben. Voorkomen moet worden dat het slachtoffer voor een dergelijke keuze wordt gesteld. Daarbij gaat het in het geval van het gebruik van persoonsgegevens voor intimiderende doeleinden om een gevaarzettingsdelict waarvoor geldt dat de samenleving er als geheel belang bij heeft dat hiertegen in ernstige gevallen wordt 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. Het algemeen belang kan bij het gebruik van persoonsgegevens voor intimiderende doeleinden in het bijzonder strekken tot strafvervolging in het geval identificerende persoonsgegevens van grote groepen gelijktijdig worden verspreid (bijvoorbeeld een ‘vijandelijke lijst’) of wanneer 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. Dit vraagt deels om een andere aanpak van de opsporing dan bij gedragingen in de fysieke wereld. Door het gebruik van persoonsgegevens voor intimiderende doeleinden aan te merken als een feit waarvoor voorlopige hechtenis is toegelaten, komen extra opsporingsbevoegdheden beschikbaar. De snelheid waarmee

---

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 internet en sociale media veranderen, maakt het voor het strafrechtelijk onderzoek noodzakelijk om relevante informatie zo snel mogelijk vast te leggen. Ook het identificeren van verdachten vraagt om een andere inzet van opsporing. Berichten op internet en sociale media worden vaak onder een accountnaam of «nickname» geplaatst. Voor het identificeren van de plaatser moeten bij een aanbieder verkeersgegevens kunnen worden gevorderd gericht op het achterhalen van het IP-adres van de plaatser en de bijbehorende metadata. In het kader van het opsporingsonderzoek is vastlegging van de volgende informatie van belang: de accountnaam waar het bericht mee is geplaatst, de openbaarheid van het bericht, 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, waarvoor dus voorlopige hechtenis kan worden opgelegd (artikel 126n/u Sv). Belangrijk is dat identificerende 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 betreffende persoonsgegevens nog niet zijn verwijderd 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 als het ontoegankelijk maken noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten, bevelen om gegevens ontoegankelijk te maken (artikel 125p Sv). In het geval van toepassing van artikel 9a van het Wetboek van Strafrecht (geen oplegging straf of maatregel), van oplegging van straf of maatregel, van vrijspraak of ontslag van alle rechtsvervolging kan de rechtbank 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 door een op de specifieke gedraging toegesneden strafbaarstelling mogelijk om strafwaardige gedragingen waarmee doxing gepaard kan gaan gerichter op te sporen, te vervolgen en te bewijzen. Het strafrechtelijk optreden is gericht op degene die door het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans gegevens bij de ander vrees wil teweegbrengen, hem ernstige overlast wil aandoen of wil hinderen in de uitoefening van zijn ambt of beroep. Het strafrecht is en blijft echter het ultimum remedium. In veel gevallen van doxing kan een andere, niet-strafrechtelijke procedure voldoende zijn om het laakbare gedrag te beëindigen, de dreiging weg te nemen en de dader op zijn gedrag aan te spreken. Bij de aanpak van het doxing is het dan ook noodzakelijk om eerst en vooral in te zetten op andere (preventieve) maatregelen. Daarbij is juist ook de inzet van partners buiten het domein van justitie en veiligheid noodzakelijk.

Het slachtoffer kan daarnaast zelf een civiele procedure starten vanwege tegen hem begane onrechtmatige gedragingen indien bekend is wie de gewraakte content online heeft geplaatst. Dan kan een schadevergoeding en het offline halen van de onrechtmatige content worden geëist. Mocht de dader niet bekend zijn, dan kan bij de tussenpersoon die de content host een melding worden gemaakt. Tussenpersonen als providers en online platformen hebben een rol om op te treden, indien zij ervan op de hoogte zijn dat op hun platformen of servers strafbare of onrechtmatige content staat.[3] Het deelnemen van tussenpersonen aan de Notice and Take Down gedragscode dient om in een dergelijk geval snel de geëigende maatregelen te kunnen nemen. Deze code bevat heldere afspraken over hoe te handelen bij meldingen van onrechtmatige en strafbare inhoud op internet. In de gevallen waarin de NTD-gedragscode 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 gedragscode niet heeft ondertekend, staat eveneens gang naar de civiele rechter open. Het normstellende karakter van de nieuwe strafbaarstelling kan het slachtoffer behulpzaam zijn in de hier genoemde procedures, in het bijzonder omdat de strafbaarstelling de onrechtmatigheid van de content weerspiegelt.

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

[3] Zie artikel 1 van de Gedragscode Notice-and-Take-Down 2018.

"vijandelijke lijsten" tegen te gaan. [4] 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.[5]

De strafbaarstellingen in deze andere landen hebben gemeen dat zij steeds betrekking hebben op het verspreiden en/of verzamelen van persoonsgegevens (zonder toestemming van de betrokkene). 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 aanjagen van vrees, het aandoen van ernstige overlast of het hinderen in 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 te bepalen is 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 'het ernstig belemmeren van ambt of beroep' op te nemen. Bijvoorbeeld in het geval dat persoonsgegevens van politieambtenaren worden verspreid zal de betrokkene hiermee kunnen beogen het uitoefenen van de functie te belemmeren, zodat hij strafbaar is.

4. Verhouding met fundamentele rechten

De strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden betreft een beperking van de vrijheid van meningsuiting. De vrijheid van meningsuiting wordt gewaarborgd in artikel 7 van de Grondwet en in artikel 10 van het Europees Verdrag van de Rechten van de Mens (EVRM). Op grond van de jurisprudentie van het Europese Hof tot bescherming van 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 strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden dient een in het tweede lid van artikel 10 EVRM opgenomen doel, te weten (in ieder geval) de bescherming van de rechten van anderen. Eenieder heeft immers ook recht op eerbiediging van zijn persoonlijke levenssfeer, zoals gewaarborgd in artikel 8 EVRM en artikel 10 van de Grondwet. Het verspreiden of ter beschikking stellen van identificerende persoonsgegevens van een ander met het oogmerk 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 raakt aan de persoonlijke levenssfeer van die ander. 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 grote ingrijpende en schadelijke effecten die het gebruik van persoonsgegevens voor intimiderende doeleinden kan hebben op het persoonlijke leven van slachtoffers. In de eerste plaats wordt hierdoor de onlinewereld verbonden met de fysieke wereld, in het bijzonder de fysieke persoonlijke levenssfeer. 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. In de tweede plaats leidt het gebruik van persoonsgegevens voor intimiderende doeleinden 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 en daarmee ook de partner en kinderen van het slachtoffer aangaan. 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 het gebruik van persoonsgegevens voor

[4] Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Verbesserung des strafrechtlichen Schutzes gegen sogenannte Feindeslisten (Drucksache 19/28678).
[5] Waaronder Alabama, Colorado, Oklahoma en Utah.

intimiderende doeleinden 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 – slachtoffer worden en waarvoor ze in een dergelijk geval dienen te vrezen. Dit wordt nog verstrekt als de identificerende persoonsgegevens zijn verspreid binnen een grote groep (bijvoorbeeld door het delen ervan in een app-groep of op social media), waardoor door slachtoffers noch door de politie ingeschat kan worden wie wanneer actie zou kunnen ondernemen. 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. Daarbij wordt mede overwogen, dat de vrijheid van meningsuiting niet alleen toepasselijk is op het individu, maar ook op de democratische samenleving als geheel. Het gebruik van de vrijheid van meningsuiting mag geen instrument zijn om de vrijheid van een ander te beperken.

Het samenbrengen en publiceren van persoonsgegevens kan in sommige gevallen wel degelijk een gerechtvaardigd belang opleveren. Bijvoorbeeld wanneer de intentie van de openbaarmaking is gelegen in het aan de kaak stellen van misstanden. In het tweede lid van het voorgestelde artikel 285d Sr is daarom expliciet 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 identificerende persoonsgegevens vereiste. Dit wetsvoorstel belet daarmee journalisten en klokkenluiders niet om nieuwsfeiten en misstanden openbaar te maken. 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 daarbij identificerende persoonsgegevens worden verspreid 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. Voor zover daarbij identificerende persoonsgegevens van een ander worden verspreid – bijvoorbeeld de naam van degene op wie wordt gereageerd – zal het vereiste oogmerk van de intimidatie immers ontbreken.

5. Adviezen

PM

6. Uitvoerings- en financiële consequenties

Doxing is een nieuw fenomeen, dat zich in korte tijd in verschillende vormen heeft gemanifesteerd. Het wetsvoorstel stelt de duidelijke norm dat het gebruik van persoonsgegevens voor intimiderende doeleinden onacceptabel is. Voorstelbaar is, dat de brede politieke verontwaardiging en de mede daaruit volgende strafbaarstelling bijdraagt aan de bewustwording van de ernstige gevolgen die doxing kan hebben. Naar verwachting zal dit een grote groep potentiële daders weerhouden om daadwerkelijk gebruik te maken van identificerende persoonsgegevens voor intimiderende doeleinden. Daarnaast vergroot de strafbaarstelling van het gebruik van persoonsgegevens voor intimiderende doeleinden de kansen van betrokkenen in niet-strafrechtelijke procedures, zoals een melding bij een internet tussenpersoon of een civiele procedure, omdat de strafbaarheid en onrechtmatigheid van dit soort gedragingen vaststaat. In deze procedures zal geen beroep worden gedaan op de capaciteit van politie en OM. Het wetsvoorstel zal daarom naar verwachting geen substantiële gevolgen hebben voor de werklast van de politie, het openbaar ministerie, de rechtspraak en de executie. De werkzaamheden voor de politie, het openbaar ministerie en de rechtspraak veranderen naar verwachting door deze wet niet in omvang en frequentie. Het wetsvoorstel verruimt in materieel opzicht uitsluitend het beoordelingskader. Daarbij wordt overwogen, dat het nieuwe wetsartikel vooral ten laste zal worden gelegd aanvullend op reeds bestaande aangiftes van bijvoorbeeld bedreiging en belaging. Deze paragraaf zal verder worden aangevuld na ommekomst van de consultatie.

II. ARTIKELSGEWIJZE TOELICHTING

Artikel I (Wijziging Wetboek van Strafrecht)

Eerste lid
In een nieuw artikel 285d Sr wordt strafbaar gesteld het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende 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. 'Zich verschaffen' betreft het zich doen toekomen van gegevens, hieronder kan met andere woorden worden verstaan het verzamelen van gegevens. Dit betreft bijvoorbeeld het via social media oproepen om het adres van een bepaalde persoon toe te zenden. 'Verspreiden of anderszins ter beschikking stellen' ziet op het distribueren of toezenden van gegevens. Dit hoeft niet in het openbaar te gebeuren.

De betekenis van 'identificerende persoonsgegevens' komt overeen met de betekenis die hieraan wordt gegeven in reeds bestaande strafbepalingen (onder andere de artikelen 231b en 435 Sr). Hiermee worden onder meer bedoeld de personalia van betrokkene, zoals zijn naam en geboortedatum. Deze gegevens zijn te karakteriseren als gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (Kamerstukken II 2011/12, 33352, nr. 3). Het kan gaan om alle gegevens waarmee een persoon kan worden geïdentificeerd, zoals (combinaties van) naam, adres, telefoonnummer, accounts, handles, nicknames (Kamerstukken II 2012/13, 33352, nr. 7). Soms zal de identiteit van een persoon niet uitsluitend aan de hand van een foto kunnen worden vastgesteld. Als dat het geval is kan de desbetreffende foto als zodanig geen identificerend persoonsgegeven zijn.[6] Dergelijke foto's kunnen uiteraard wel als identificerend persoonsgegeven worden aangemerkt in combinatie met andere gegevens waarmee de identiteit van de betrokkene kan worden vastgesteld.

Voor strafbaarheid is vereist dat degene die zich de identificerende persoonsgegevens verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt het oogmerk heeft om die ander vrees aan te jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen. Het oogmerk kan er ook op zijn gericht het teweegbrengen van vrees, ernstige overlast of hinder door een ander te laten bewerkstelligen. Bij het gebruik van persoonsgegevens voor intimiderende doeleinden kan het immers juist ook gaan om het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens van het beoogde slachtoffer, zoals zijn adres, zodat anderen hiermee in de richting van diegene kunnen handelen. Het gaat om het beoogde effect van de gedraging: het moet de bedoeling zijn dat het slachtoffer in zijn leven of beroepsuitoefening wordt belemmerd. Voor het slachtoffer kan het gegeven dat zijn adres bij anderen bekend is en mogelijk ook zal worden gebruikt zeer intimiderend zijn.

Met 'vrees' wordt, evenals in de delictsomschrijving van belaging (artikel 285b Sr), een emotie bedoeld, die ieder normaal mens onder vergelijkbare omstandigheden ook zou hebben. In de memorie van toelichting bij artikel 285b Sr (Kamerstukken II 1997/98, 25768, 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, 25768, nr. 7), de dader heeft daadwerkelijk het oogmerk om het slachtoffer bang te maken. Van 'ernstige overlast' en 'ernstige hinder van de uitoefening van ambt of beroep' kan sprake zijn in die gevallen waarin het 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 identificerende persoonsgegevens bekend is geworden.

Het oogmerk van degene die zich identificerende persoonsgegevens verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt zal in veel gevallen uit de context moeten worden afgeleid. Ook als de dader 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 dader erop gericht moet zijn geweest om de betrokkene vrees aan te jagen, ernstige overlast aan te doen of hem in te uitoefening van zijn functie te 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.

Niet hoeft te worden bewezen dat het slachtoffer ten gevolge van de gedraging vrees is aangejaagd, dat betrokkene ernstige overlast heeft ervaren of in de uitoefening van zijn functie is gehinderd. Het volstaat dat het *oogmerk* van de dader hierop is gericht. Of dit op het slachtoffer het beoogde effect heeft gehad is strafrechtelijk niet relevant, al maakt dat de bewijsvoering wel

[6] Zie ook de uitspraak van de rechtbank Rotterdam van 14 april 2017, ECLI:NL:RBNHO:2017:3643.

eenvoudiger. Strafrechtelijk voldoende is, evenals bij belaging, dat in het algemeen de gedraging geschikt en geëigend zou zijn om een bepaalde opstelling teweeg te brengen (Kamerstukken II 1997/1998, 25768, nr. 3, p. 16). Aldus worden deze gedragingen strafbaar gesteld ongeacht het resultaat ervan; het gebruik van persoonsgegevens voor intimiderende doeleinden is een formeel omschreven delict.

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 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 identificerende persoonsgegevens vereiste. In paragraaf 4 is toegelicht dat het samenbrengen en publiceren van persoonsgegevens een gerechtvaardigd belang kunnen dienen. Bijvoorbeeld wanneer het gaat om het aan de kaak stellen van misstanden. Voorop gesteld kan worden dat van strafbaarheid van journalisten en klokkenluiders geen sprake behoort te zijn wanneer bekendmaking van de gegevens in het algemeen belang noodzakelijk is. Het wetsvoorstel beoogt nadrukkelijk niet te voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders. Met het oog daarop is een zelfstandige uitzondering in de wet opgenomen voor degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens vereiste. 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 artikel 285d, tweede lid, Sr een waarborg op te nemen vergelijkbaar met de artikelen 139g, tweede lid, en 273, tweede lid, Sr.

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 identificerende persoonsgegevens met het oogmerk vrees aan te jagen, ernstige overlast aan te doen of de ander in de uitoefening van zijn ambt of beroep ernstig te 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.

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 inverzekeringstelling en de inzet van bijzondere opsporingsbevoegdheden als het vorderen van gegevens zullen noodzakelijk zijn bij de bestrijding van doxing. 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 identificerende 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 doxing. 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,

F.B.J. Grapperhaus