Ministerie van Justitie en Veiligheid

Aan de Minister van Justitie en Veiligheid

Directie Wetgeving en Juridische Zaken
Sector Straf- en Sanctierecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
16 mei 2023

Ons kenmerk
4664192

nota

Memorie van antwoord strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden (doxing)

1. Aanleiding

De Eerste Kamer heeft op 21 maart jl. voorlopig verslag uitgebracht over het wetsvoorstel strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden (ofwel: doxing). Bijgevoegd treft u aan de concept memorie van antwoord waarin de gestelde vragen zijn beantwoord.

2. Geadviseerd besluit

Instemmen met het aanbieden aan de Eerste Kamer van de memorie van antwoord over het wetsvoorstel strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden.

3. Kernpunten

Voor het voorlopig verslag is inbreng geleverd door de fracties van GroenLinks en de PvdA, D66 en SGP. De 50PLUS-fractie heeft zich aangesloten bij de vragen gesteld door GroenLinks en de PvdA, en de SGP. GroenLinks en de PvdA, en de SGP hebben met belangstelling kennisgenomen van het wetsvoorstel. De gestelde vragen hebben onder meer betrekking op het bij amendement verhoogde strafmaximum (GL en PvdA), de bijzondere strafverhogingsgrond voor doxing ten aanzien van bepaalde functionarissen (GL en PvdA), de reikwijdte van de strafbaarstelling (GL en PvdA, D66, SGP), het voor strafbaarheid vereiste oogmerk (GL en PvdA, SGP), de aansprakelijkheid van aanbieders en bij gebruik van algoritmes (D66) en het voorkomen en opsporen van doxing (GL en PvdA, SGP, D66).

4. Toelichting

Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden
De voorgestelde strafbaarstelling (artikel 285d Sr) betreft het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van een ander of een derde om die ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of hem in de uitoefening van zijn ambt of beroep ernstig te (laten) hinderen. Kortgezegd: het gebruik van persoonsgegevens voor intimiderende doeleinden of strafbare doxing. Het strafmaximum bedraagt twee jaar gevangenisstraf of geldboete van de vierde categorie (bij amendement verhoogd; voorheen een jaar gevangenisstraf of geldboete derde categorie). Als de gedraging wordt gepleegd tegen een persoon vanwege diens hoedanigheid van ambts- en gezagsdrager, of functionaris in het veiligheidsdomein, wordt het strafmaximum met een derde verhoogd (bij amendement ingevoegd; zie het voorgestelde artikel 285d, tweede lid, Sr).

Strafmaximum en strafverhogingsgrond
GroenLinks en PvdA hebben gevraagd naar de twee door de Tweede Kamer aangenomen amendementen die elkaar in strafmaximumverhogende werking versterken. In reactie op deze vragen is aangegeven dat het bij het bepalen van het strafmaximum in essentie gaat om de waardering van de ernst van een strafbaar feit. Daarbij is van belang hoe vanuit de samenleving hiernaar wordt gekeken. Het verhoogde strafmaximum biedt de strafrechter voldoende ruimte om de meest ernstige gevallen van strafbare doxing passend te kunnen bestraffen. De hoogte van het strafmaximum is in relatie tot de strafhoogtes voor soortgelijke delicten nog steeds verdedigbaar en geeft daarmee op passende wijze uiting geeft aan de meest ernstige verschijningsvormen van doxing.

Ten aanzien van de bijzondere strafverhogingsgrond voor doxing tegen bepaalde functionarissen hebben GroenLinks en PvdA gevraagd naar het met het amendement gecreëerde onderscheid tussen de groep functionarissen waarvoor de bijzondere strafverhogingsgrond geldt en andere functionarissen die niet tot de genoemde beroepsgroepen behoren. In reactie op deze vragen is aangegeven dat van de functionarissen genoemd in de strafverhogingsgrond veel wordt verwacht en dat zij een groot risico lopen slachtoffer te worden van intimidatie vanwege de functie die zij vervullen. Daartegen moet stevig kunnen worden opgetreden. Van de strafverhogingsgrond kan ook een afschrikwekkende werking uitgaan richting potentiële daders. Het strafmaximum biedt in elk geval ook voldoende ruimte om de ernstige gevallen van strafbare doxing, gepleegd tegen functionarissen die niet in de strafverzwaringsgrond zijn genoemd, proportioneel te kunnen bestraffen.

Reikwijdte van de strafbaarstelling
D66 heeft gevraagd of dreigen met doxing strafbaar is. In reactie daarop is toegelicht dat de dader om contact op te kunnen nemen met degene tegen wie het dreigen met doxing is gericht over persoonsgegevens van diegene zal moeten beschikken. Als de dader deze persoonsgegevens heeft verschaft met het oogmerk de ander vrees aan te jagen, ernstige overlast aan te doen of ernstig te hinderen in de uitoefening van zijn ambt of beroep, waarvan in deze gevallen doorgaans sprake zal zijn, is sprake van strafbare doxing.

Over de noodzaak van strafbaarheid van het ‘zich verschaffen’ van persoonsgegevens voor intimiderende doeleinden zijn vragen gesteld door GroenLinks en PvdA, en SGP. SGP heeft gevraagd wanneer het zich verschaffen van persoonsgegevens strafbaar wordt. Door GroenLinks en PvdA is gevraagd is of het ‘zich verschaffen’ van persoonsgegevens niet al strafbaar zou zijn als poging tot doxing als het niet als gedraging in de delictsomschrijving zou zijn opgenomen en of niet al sprake is van een ander strafbaar feit. Zij hebben ook gevraagd waarom in plaats van het ‘zich verschaffen’ van persoonsgegevens niet het doen van een oproep om persoonsgegevens te delen strafbaar is gesteld.

Het 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 al het oogmerk had diegene te intimideren. Als het ‘zich verschaffen’ van persoonsgegevens niet zou zijn opgenomen in de delictsomschrijving zou degene die zich persoonsgegevens verschaft van een ander om die ander daarmee in de fysieke wereld te intimideren, niet strafbaar zijn voor een poging tot verspreiding van persoonsgegevens. Ook dergelijk handelen is op zichzelf strafwaardig. Door deze strafbaarstelling wordt strafrechtelijk optreden al mogelijk in de fase van het zich verschaffen van persoonsgegevens voor intimiderende doeleinden. Daarmee wordt de aanmerkelijke kans verkleind dat meer schade wordt toegebracht.

Bij het zich verschaffen van persoonsgegevens is geen sprake van een ander strafbaar feit, zoals computervredebreuk (artikel 138ab Sr) of het overnemen van niet-openbare computergegevens (artikel 138c Sr), omdat het bij die misdrijven gaat om niet-openbare gegevens. 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. Er is ook geen sprake van afpersing of bedreiging omdat de strafbaarstelling van het zich verschaffen van persoonsgegevens voor intimiderende doeleinden op andere gedragingen ziet dan de strafbaarstellingen van bedreiging en afpersing.

Oogmerkvereiste
GroenLinks en PvdA hebben gevraagd voorbeelden te geven van gedragingen die worden gezien als aanjagen van vrees, aandoen van ernstige overlast en ernstig hinderen in de uitoefening van ambt of beroep en gedragingen die daar net niet onder vallen. Zij hebben ook gevraagd naar het bewijs van het voor strafbaarheid vereiste oogmerk. D66 heeft twijfels over de handhaafbaarheid van de strafbaarstelling van het zich verschaffen van persoonsgegevens voor intimiderende doeleinden omdat het oogmerk in die gevallen niet bekend zal worden en heeft gevraagd de handhaving toe te lichten.

De bedoeling van een persoon bij het verzamelen van gegevens zal niet altijd duidelijk zijn. Maar er kunnen zich ook situaties voordoen waarin wel kan worden bewezen dat de verdachte zich persoonsgegevens heeft verschaft met het oogmerk van intimidatie. 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. 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 gebruik van persoonsgegevens. Het oogmerk zal in sommige gevallen ook uit de context kunnen worden afgeleid. Veel hangt derhalve af van hetgeen uit objectieve feiten en omstandigheden blijkt over het oogmerk van de dader. In reactie op de gestelde vragen zijn verschillende voorbeelden genoemd.

D66 heeft gevraagd waarom in de delictsomschrijving de afbakening is gemaakt bij 'ernstige' overlast en 'ernstige' hinder. In reactie daarop is toegelicht dat in de omschrijving van het voor strafbaarheid vereiste oogmerk een grens is 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 en te beschadigen in hun persoonlijk leven. Daarvan hoeft nog geen sprake te zijn in gevallen van 'gewone' hinder en overlast. Daarbij speelt ook mee dat deze strafbaarstelling een beperking van de vrijheid van meningsuiting betreft. Een beperking kan alleen noodzakelijk zijn voor zover deze proportioneel is. Daarom gaat de voorgestelde strafbaarstelling niet verder dan strikt noodzakelijk.

Aansprakelijkheid van aanbieders en bij gebruik van algoritmes
D66 heeft gevraagd naar het melden van strafbare doxing bij tussenhandeldiensten en of er medeplichtigheid ontstaat als de betreffende content niet wordt verwijderd. In reactie daarop wordt aangegeven dat slachtoffers door de strafbaarstelling de mogelijkheid hebben om aangifte te doen bij de politie en de mogelijkheid hebben om doxing te melden bij tussenhandeldiensten met een verzoek tot verwijdering van gegevens. Tussenhandeldiensten zijn niet aansprakelijk indien ze niet weten van de activiteit of informatie met een onrechtmatig karakter op hun dienst danwel zodra ze dat wel weten prompt handelen om de illegale inhoud te verwijderen of de toegang daartoe onmogelijk te maken.

Wanneer een platform dat bij het verkrijgen van de kennis over strafbare doxing de gegevens waarmee dit delict is gepleegd prompt verwijdert, is het platform dus niet aansprakelijk.

Daarnaast heeft D66 gevraagd wie er aansprakelijk zou kunnen zijn bij gebruik van algoritmes voor het plegen van doxing. In reactie daarop is aangegeven dat dit een technisch complex scenario is. Het is zeer onwaarschijnlijk dat dit zonder menselijke aansturing zal kunnen gebeuren. Indien menselijke aansturing mogelijk zou zijn, is diegene die aanstuurt ook verantwoordelijk en kan diegene daarvoor eventueel ook strafrechtelijk aansprakelijk zijn.

Voorkomen en opsporen van doxing
SGP heeft gevraagd naar de capaciteit van politie en het openbaar ministerie om serieus werk te kunnen maken van de opsporing van strafbare doxing. Hoeveel doxing zaken daadwerkelijk zullen instromen is uiteraard nog niet bekend. De prognoses van het aantal zaken lopen uiteen: het openbaar ministerie verwacht een aanzienlijk aantal zaken, 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. Daarom zal kort na de inwerkingtreding van de wet worden gestart met een invoeringstoets om te monitoren hoeveel zaken er instromen.

4.1 Politieke context
Het wetsvoorstel is op 7 februari jl. met algemene stemmen aangenomen door de Tweede Kamer. Over de amendementen bij dit wetsvoorstel is als volgt gestemd:

- Amendement-Michon-Derkzen (nr. 7) over het verlagen van de grens voor strafbaarheid van doxing door het schrappen van 'ernstig' voor overlast en hinder (ontraden): voor waren BIJ1, Fractie Den Haan, Lid Gündoğan, de VVD, de SGP, BBB, JA21, de PVV en Groep Van Haga. Overige fracties waren tegen. Conclusie: ***verworpen.***
- Amendement-Michon-Derkzen (nr. 8) over verhoging van het strafmaximum naar twee jaar gevangenisstraf en geldboete van de vierde categorie (oordeel Kamer): voor waren DENK, Fractie Den Haan, Lid Gündoğan, D66, de VVD, de SGP, het CDA, BBB, JA21, de PVV en Groep Van Haga. Overige fracties waren tegen. Conclusie: ***aangenomen***.
- Amendement-Van der Staaij/Kuik (nr. 10) over een strafverhogingsgrond voor doxing ten aanzien van ambts- en gezagsdragers en functionarissen in het veiligheidsdomein (ontraden): voor waren SP, GroenLinks, Volt, DENK, Fractie Den Haan, de PvdA, de PvdD, Lid Gündoğan, de ChristenUnie, de VVD, de SGP, het CDA, BBB, JA21, de PVV en Groep Van Haga. Overige fracties waren tegen. Conclusie: ***aangenomen***.

4.2 Ontwikkelingen hiervoor
U heeft eerder ingestemd met indiening van het wetsvoorstel, het nader rapport en de nota naar aanleiding van het verslag bij de Tweede Kamer. De beslisnota waarin u om instemming werd gevraagd is openbaar gemaakt.

4.3 Krachtenveld
De memorie van antwoord is afgestemd met DRC en DGPenV.

5. Informatie die niet openbaar gemaakt kan worden
Niet van toepassing, alles uit deze nota wordt openbaar.