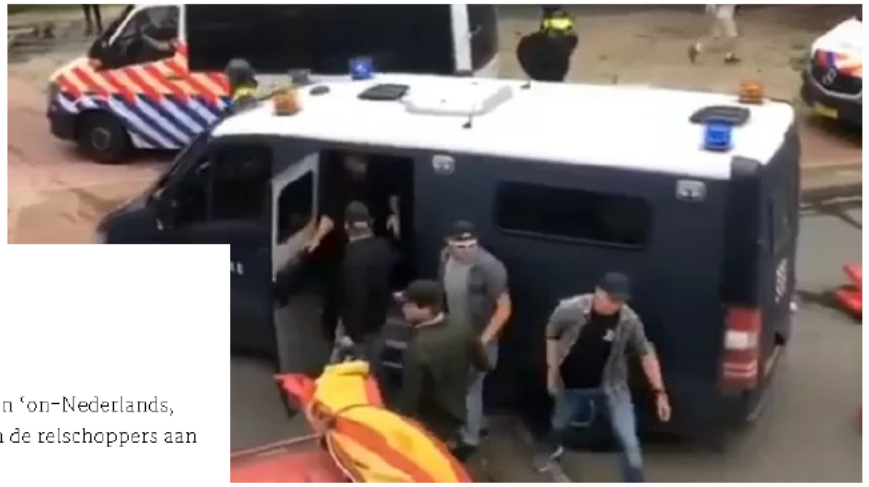
Aanslag was gericht tegen huis van politieman, vrouw en kinderen waren alleen thuis

13 december 2020 om 13:50 • Aangepast 14 december 2020 om 13:36

Bij daglicht is de schade goed te zien (foto: Noël van Hooft)



ien Haag © Twitter

Korpschef Van Essen: bedreigers undercoveragenten aanpakken

De korpschef van de Nationale Politie Henk van Essen noemt het bedreigen van agenten 'on-Nederlands, ongekend en ontoelaatbaar". De korpschef zegt in De Telegraaf vastbesloten te zijn om de relschoppers aan te pakken.

Amateurspeurder dreigt adressen undercovers te publiceren na boerenprotest, politie alert

Katwijkse agenten maken zich zorgen: 'Wij hebben ook een gezin thuis'

Foto: Politie

Agent wil vervolging afdwingen van man die hem bedreigde met fysiek geweld


Buiten reikwijdte

Buiten reikwijdte


Buiten reikwijdte

Aandacht in en vanuit korps

Buiten reikwijdte

4. Handelingskader Doxing (2020)
5. Wetsvoorstel strafbaarstelling doxing (2022)

Buiten reikwijdte


Buiten reikwijdte

Buiten reikwijdte

Het huidige palet aan strafbaarstellingen

1. **Artikel 184 Sr** De politie mag niet belemmerd worden bij de rechtmatige uitvoering van een wettelijke taak (artikel 184 Sr).
2. **Artikel 426bis Sr** Op de openbare weg beperken van de vrije beweging van een ander of een ander samen met een of meer anderen blijven opdringen of hinderlijk blijven volgen
3. **Artikel 2:47 APV** hinderlijk gedrag op openbare plaatsen
4. **Artikel 2:50 APV** hinderlijk gedrag in voor het publiek toegankelijke ruimten).
5. **Bestuurlijke of strafrechtelijke maatregel** zich niet mogen bevinden op een bepaalde locatie, zoals gebiedsontzegging of locatieverbod, samenscholingsverbod, noodbevel of -verordening burgemeester (artikel 172 lid 3 Gemeentewet) of wederrechtelijk aanwezig zijn in een woning of besloten lokaal (138 Sr).
6. **Artikel 139f en 137g Sr** Onrechtmatig vastgelegde beelden, bijvoorbeeld beelden die heimelijk zijn vastgelegd, mogen uiteraard niet worden verspreid. Hiertegen kan worden opgetreden op grond van de artikelen 139f en 139g Sr.
7. **Artikel 261/2** Smaad - Een foto-afbeelding kan voorts op verschillende wijzen beledigend voor een politieambtenaar zijn; ofwel als smaad of laster door de begeleidende teksten
8. **Artikel 266 Sr** Belediging - Wanneer bijvoorbeeld een bewerking van een afbeelding van een politieambtenaar de waardigheid van diens persoon aantast.
9. **Artikel 285 Sr** Bedreiging (zoals beelden op een strafbare wijze gepubliceerd, zodanig worden gepresenteerd dat sprake is van bedreiging of smaad. Door het toevoegen van commentaren of manipulatie van fotobeelden kan een politieambtenaar worden bedreigd met een misdrijf tegen het leven.
10. En verder de strafbaarstellingen **Artikel 179 Sr** Ambtsdwang, **Artikel 285b Sr** belaging, **Artikel 132 Sr** opruiing

Betekenis voor de politie

1. Doxing strafbaarstelling, identificeren
2. Buiten reikwijdte
3.
4.

Doxing strafbaarstelling

ARTIKEL I

Artikel 285d Wetboek van Strafrecht (nieuw)

1. Hij die zich identificerende persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk om die ander vrees aan te jagen dan wel aan te laten jagen, ernstige overlast aan te doen dan wel aan te laten doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel te laten hinderen, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

2. Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het zich verschaffen, verspreiden of anderszins ter beschikking stellen van de gegevens, bedoeld in het eerste lid, vereiste.

ARTIKEL III

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


Buiten reikwijdte

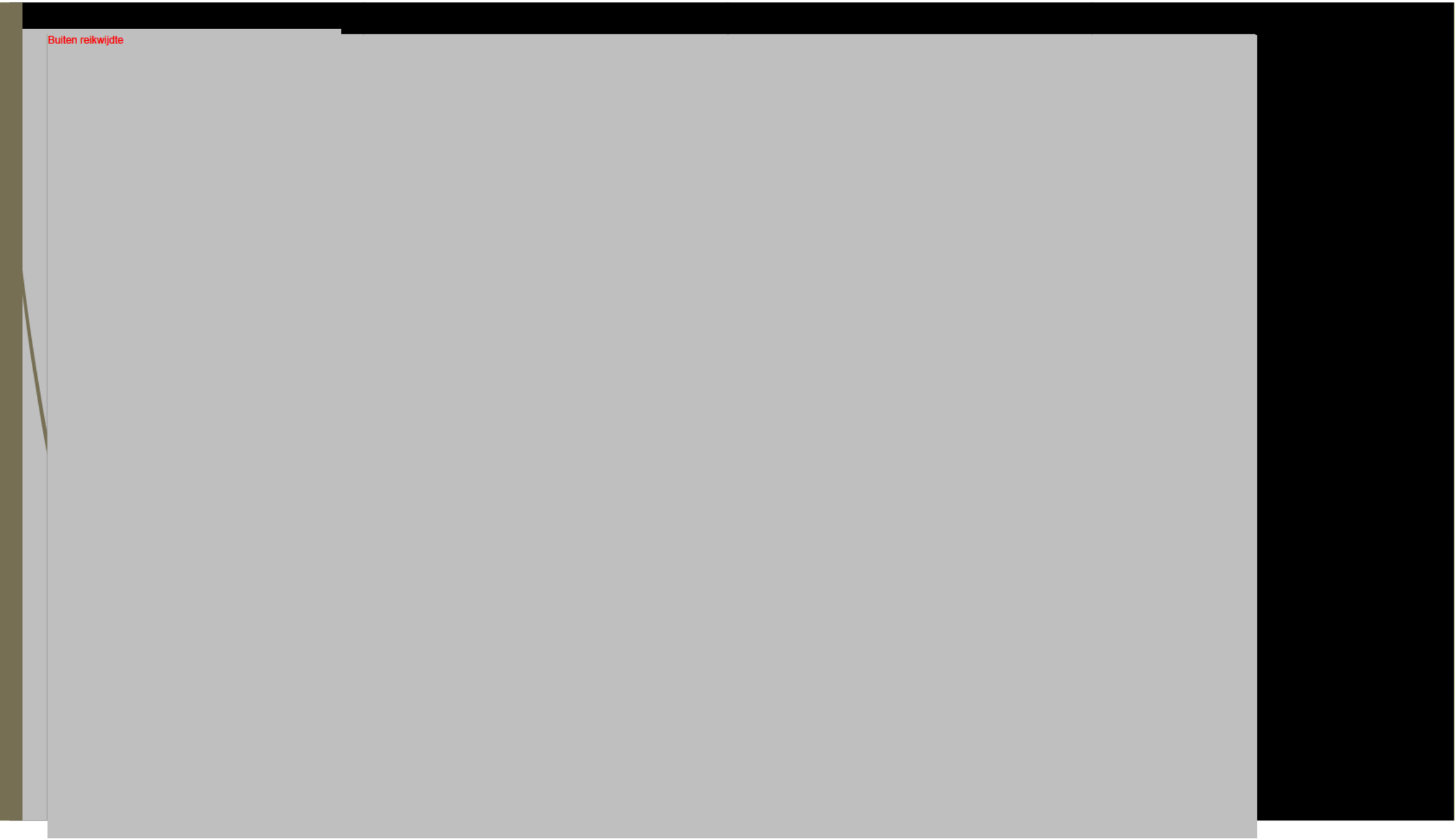
Voorbeelden uitspraken kortgeding

1. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZUT:2010:BM6266
2. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:569
3. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBLIM:2018:8762
4. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2019:4954
5. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2019:110

Buiten reikwijdte

Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte

Buiten reikwijdte

Centraal Georganiseerd Overleg Politie (CGOP)
Werkgroep Rechtspositie Bescherming Dienders (WGRPBD)

CAOP
Postbus 556, 2501 CN Den Haag
Lange Voorhout 13, 2514 EA Den Haag
KVK-nummer 41158878

Inlichtingen: 5.1.2.e
Telefoon: +31 5.1.2.e
E-mail: 5.1.2.e @caop.nl
Datum: 6 oktober 2022
Bijlage(n): 1
Ons kenmerk: WGRPBD/22.02438.3

Aan De voorzitter en leden van de Werkgroep
Rechtspositie Bescherming Dienders

Verslag van de vergadering van de werkgroep rechtspositie bescherming dienders van 15 september 2022 **van 16.00 tot 17.30 uur** per MS Teams.

Aanwezig:
Van de zijde van J&V:
5.1.2.e (voorzitter) en 5.1.2.e
Van de zijde van de Nationale Politie:
5.1.2.e
Van de zijde van de centrales:
5.1.2.e
Van de zijde van het secretariaat (CAOP):
5.1.2.e (verslag)

Gast:
5.1.2.e (NP)

Afwezig:
5.1.2.e, 5.1.2.e en 5.1.2.e (JenV)
5.1.2.e, 5.1.2.e en 5.1.2.e (NP)
5.1.2.e (ANPV)
5.1.2.e (Equipe)

Agenda

1. Opening.
2. Presentatie Doxing door politie (WGRPDB/22.02410)

Buiten reikwijdte

b. Handelingskader doxing.

Buiten reikwijdte

4. Stand van zaken thema's stellingname rechtspositie – bescherming diender.

Buiten reikwijdte

b. Wetsvoorstel Doxing/strafbaarstelling van het 'kale feit' doxing als bloot rechtsfeit.
c. Onderzoek maatregelen om doxing tegen te gaan.

Buiten reikwijdte

politiebureaus.

Buiten reikwijdte

Verslag

1. Opening en mededelingen

De voorzitter start de vergadering om 16.02 uur en heet de aanwezigen welkom. Zij stelt de agenda ongewijzigd vast. De heer 5.1.2.e is uitgenodigd om een presentatie te geven over doxing. Een korte voorstelronde volgt.

2. Presentatie Doxing door politie (WGRPDB/22.02410)

De heer 5.1.2.e geeft de presentatie, deze is aan het verslag gehecht. De inhoud van de sheets wordt als hier herhaald en ingelast beschouwd. Hetgeen in aanvulling daarop is opgemerkt en/of gevraagd, is hieronder weergegeven.

Sheet 1 – context (I)

De voorzitter vraagt de heer 5.1.2.e voorbeelden te geven van doxing. De heer 5.1.2.e noemt het schietincident tijdens de boerenprotesten in Friesland. Men ging op zoek naar de collega die geschoten heeft. Degene die zij vonden was de verkeerde, terwijl van diegene wel de persoonsgegevens online zijn gezet. Dit heeft tot een onbeheersbare situatie heeft geleid. Daarnaast noemt hij een voorbeeld uit Amsterdam, waarbij een digitale wijkagent was betrokken, die heel adequaat heeft gereageerd. De doxing bleek door een vijftienjarige vanaf een zolderkamer te gebeuren. Doxing kent veel verschijningsvormen, aldus spreker.

Sheet 2 – context (II)

De heer 5.1.2.e meldt dat aan een handelingskader 2.0 wordt gewerkt. Hij zal hierover later meer vertellen.

Sheet 3 – doel

De voorzitter vraagt of de heer 5.1.2.e zal aangeven waar zaken in de staande organisatie worden ingeregeld. De heer 5.1.2.e bevestigt dit, dat komt bij zie sheet 4 aan de orde.

Sheet 4 – dimensies en maatregelen

- Preventie: De heer 5.1.2.e licht toe dat er in de organisatie onvoldoende kennis over doxing is. Ook wijst hij op de rol die sociale media kunnen spelen in het vormen van verbinding met de samenleving. Dit kent echter ook gevaren, waar de collega's zich bewust van moeten zijn. Zij moeten ook niet naïef in zijn ten aanzien van het gebruik van sociale media. Het bevorderen van kennis en bewustwording over doxing wil men onderdeel laten zijn van de training van de IV-organisatie. Daarnaast gaat men op intranet periodiek aandacht besteden aan doxing, worden er materialen ontwikkeld en wil bewerkstelligen dat het onderwerp in het curriculum van de PA wordt opgenomen.
- Monitoring en quick response: spreker benoemt dat in de praktijk de medewerkers zelf constateren dat sprake is van doxing. Hij vindt echter dat de politie dit via de OCID (Organized Crime Intelligence Division) voor de rekening moet nemen, ondanks dat doxing grotendeels plaatsvindt buiten het gezichtsveld, in afgeschermde groepen. Daarnaast zou men met name rond demonstraties en andere incidenten moeten

monitoren, omdat dat de momenten zijn waarop doxing plaatsvindt. Daarom is men bezig om doxing in de crisisstructuur in te bedden.
De voorzitter vraagt of dit gericht is op de eigen mensen en niet zozeer op de pleger. De heer 5.1.2.e bevestigt dit. Plegen en verspreiden hoort voor hem onder het kopje 'verstoren'. Deze aanpak gaat ook niet over doxing van andere personen die werkzaam zijn in de publieke sfeer, zoals politici, aldus spreker.

- Opvang en ondersteuning collega's: zoals spreker al aangaf is er weinig kennis in de organisatie, ook bij leidinggevenden, die een grote rol spelen in de opvang van collega's. Dit terwijl de opvang en ondersteuning wel echt iets vergt van de organisatie. Daarom wordt er veel onderzoek gedaan naar (de impact van) doxing. Omdat de leidinggevende een centrale rol heeft in de opvang en ondersteuning, wil men graag een moment creëren waarop medewerker en leidinggevende samen zitten om te kijken waar kwetsbaarheden zitten, bijvoorbeeld op sociale media en de veiligheidsinstellingen op de telefoon. Hiervoor wil men hen graag ondersteunen met goede digitale kennis.
- Partnerstrategie: spreker meldt dat er een goede procedure met de tech bedrijven is ingeregeld. De afdeling 'interceptie en sensing' van de landelijke eenheid is 'single point of contact' en 'trusted flagger' voor alle sociale media bedrijven. Zij hebben goede en snelle toegang tot deze bedrijven, zodat dingen direct kunnen worden verwijderd als dat moet. Het punt is echter dat dit binnen de organisatie nog niet echt bekend is, aldus spreker. Dit zal dus beter moeten worden gecommuniceerd en ingeregeld. In geval van doxing kan de 'interceptiedesk' van de eenheid naar de Landelijke Eenheid om de bevriezing of verwijdering te realiseren. Desgevraagd legt spreker uit dat een 'Notice en take down-procedure' een gestandaardiseerde manier is van aangeven wat er aan de hand is, waarmee richting het sociale media bedrijf of de provider kan worden aangegeven dat en waarom iets uit de lucht moet worden gehaald. Ook hiervoor geldt dat veel mensen deze procedure nog niet kennen en dat ook hierover dus beter moet worden gecommuniceerd, zegt hij.
- Communicatie en kennisontwikkeling: spreker is van mening dat het belangrijk is om de collega's te vertellen dat ze worden gesteund als hen iets overkomt en hen te informeren over hun eigen verantwoordelijkheid. Daarnaast komen er nieuwe fenomenen aan, zoals 'deep fake'. Het is van belang ook hier alvast over na te denken en dingen te ontwikkelen. In dit kader vindt ook communicatie plaats over het nieuwe handelingskader, over de formulieren en procedures et cetera die op intranet of agora worden gezet, zodat informatie snel vindbaar is.
- Verstoren: de heer 5.1.2.e legt uit dat dit een redelijk nieuw gebied is, dat technisch en juridisch zal moeten worden uitgezocht. Los daarvan moet er, als er sprake is van doxing, iets van worden gezegd. Dat geldt zowel voor degenen die doxen als voor degenen die het verspreiden. Overigens is het zaak om ook niet te proactief te zijn en zaken niet onnodig groot te maken. Technisch gezien kan om verstoring te bewerkstelligen via de algoritmen samenwerking worden gezocht met sociale media bedrijven. Dit is echter moeilijk te concretiseren. Spreker is van mening dat hiervoor met name in de crisisstructuur scenario's moeten worden ontwikkeld en mensen hierop te trainen. 5.2.1 . De voorzitter vraagt of agenten in dergelijke gevallen enkel worden gefilmd of dat zij ook daadwerkelijk worden belaagd. De heer 5.1.2.e bevestigt dat het gaat over filmen of het maken van foto's, zonder dat men weet wat er mee gedaan wordt. De heer 5.1.2.e wijst er in dit kader op dat het maken van foto's an sich nog geen doxing hoeft te zijn.
- Opsporing en vervolging: hiermee wordt bedoeld, dat wanneer er in geval van doxing opsporing en vervolging plaatsvinden, de collega van de resultaten daarvan op de hoogte wordt gesteld. De casemanagers GTPA kunnen een belangrijke rol spelen in de inbedding hiervan.

Sheet 5 en 6 – communicatie
Spreker geeft aan dat de wens bestaat voor een landelijke doxing website met alle beschikbare content.

De voorzitter vraagt of alle genoemde dimensies in plan van aanpak terugkomen. De heer 5.1.2.e bevestigt dat. Hierbij zal men zich vooral zal richten op dingen die kunnen en niet op dingen die niet kunnen. Desgevraagd geeft hij aan dat het plan van aanpak wordt gedeeld voordat de wetgeving er is. Hij

Centraal Georganiseerd Overleg Politie (CGOP)
Werkgroep Rechtspositie Bescherming Dienders (WGRPBD)

CAOP
Postbus 556, 2501 CN Den Haag
Lange Voorhout 13, 2514 EA Den Haag
KVK-nummer 41158878

Inlichtingen: 5.1.2.e
Telefoon: +31 5.1.2.e
E-mail: 5.1.2.e @caop.nl
Datum: 6 oktober 2022
Bijlage(n): 1
Ons kenmerk: WGRPBD/22.02438.3

Aan De voorzitter en leden van de Werkgroep
Rechtspositie Bescherming Dienders

Verslag van de vergadering van de werkgroep rechtspositie bescherming dienders van 15 september 2022 **van 16.00 tot 17.30 uur** per MS Teams.

Aanwezig:
Van de zijde van J&V:
5.1.2.e (voorzitter) en 5.1.2.e
Van de zijde van de Nationale Politie:
5.1.2.e
Van de zijde van de centrales:
5.1.2.e
Van de zijde van het secretariaat (CAOP):
5.1.2.e (verslag)

Gast:
5.1.2.e (NP)

Afwezig:
5.1.2.e, 5.1.2.e en 5.1.2.e (JenV)
5.1.2.e, 5.1.2.e en 5.1.2.e (NP)
5.1.2.e (ANPV)
5.1.2.e (Equipe)

Agenda

1. Opening.
2. Presentatie Doxing door politie (WGRPDB/22.02410)

Buiten reikwijdte

b. Handelingskader doxing.

Buiten reikwijdte

4. Stand van zaken thema's stellingname rechtspositie – bescherming diender.

Buiten reikwijdte

b. Wetsvoorstel Doxing/strafbaarstelling van het 'kale feit' doxing als bloot rechtsfeit.
c. Onderzoek maatregelen om doxing tegen te gaan.

Buiten reikwijdte

politiebureaus.

Buiten reikwijdte

Verslag

1. Opening en mededelingen

De voorzitter start de vergadering om 16.02 uur en heet de aanwezigen welkom. Zij stelt de agenda ongewijzigd vast. De heer 5.1.2.e is uitgenodigd om een presentatie te geven over doxing. Een korte voorstelronde volgt.

2. Presentatie Doxing door politie (WGRPDB/22.02410)

De heer 5.1.2.e geeft de presentatie, deze is aan het verslag gehecht. De inhoud van de sheets wordt als hier herhaald en ingelast beschouwd. Hetgeen in aanvulling daarop is opgemerkt en/of gevraagd, is hieronder weergegeven.

Sheet 1 – context (I)

De voorzitter vraagt de heer 5.1.2.e voorbeelden te geven van doxing. De heer 5.1.2.e noemt het schietincident tijdens de boerenprotesten in Friesland. Men ging op zoek naar de collega die geschoten heeft. Degene die zij vonden was de verkeerde, terwijl van diegene wel de persoonsgegevens online zijn gezet. Dit heeft tot een onbeheersbare situatie heeft geleid. Daarnaast noemt hij een voorbeeld uit Amsterdam, waarbij een digitale wijkagent was betrokken, die heel adequaat heeft gereageerd. De doxing bleek door een vijftienjarige vanaf een zolderkamer te gebeuren. Doxing kent veel verschijningsvormen, aldus spreker.

Sheet 2 – context (II)

De heer 5.1.2.e meldt dat aan een handelingskader 2.0 wordt gewerkt. Hij zal hierover later meer vertellen.

Sheet 3 – doel

De voorzitter vraagt of de heer 5.1.2.e zal aangeven waar zaken in de staande organisatie worden ingeregeld. De heer 5.1.2.e bevestigt dit, dat komt bij zie sheet 4 aan de orde.

Sheet 4 – dimensies en maatregelen

- Preventie: De heer 5.1.2.e licht toe dat er in de organisatie onvoldoende kennis over doxing is. Ook wijst hij op de rol die sociale media kunnen spelen in het vormen van verbinding met de samenleving. Dit kent echter ook gevaren, waar de collega's zich bewust van moeten zijn. Zij moeten ook niet naïef in zijn ten aanzien van het gebruik van sociale media. Het bevorderen van kennis en bewustwording over doxing wil men onderdeel laten zijn van de training van de IV-organisatie. Daarnaast gaat men op intranet periodiek aandacht besteden aan doxing, worden er materialen ontwikkeld en wil bewerkstelligen dat het onderwerp in het curriculum van de PA wordt opgenomen.
- Monitoring en quick response: spreker benoemt dat in de praktijk de medewerkers zelf constateren dat sprake is van doxing. Hij vindt echter dat de politie dit via de OCID (Organized Crime Intelligence Division) voor de rekening moet nemen, ondanks dat doxing grotendeels plaatsvindt buiten het gezichtsveld, in afgeschermde groepen. Daarnaast zou men met name rond demonstraties en andere incidenten moeten

monitoren, omdat dat de momenten zijn waarop doxing plaatsvindt. Daarom is men bezig om doxing in de crisisstructuur in te bedden.
De voorzitter vraagt of dit gericht is op de eigen mensen en niet zozeer op de pleger. De heer 5.1.2.e bevestigt dit. Plegen en verspreiden hoort voor hem onder het kopje 'verstoren'. Deze aanpak gaat ook niet over doxing van andere personen die werkzaam zijn in de publieke sfeer, zoals politici, aldus spreker.

- Opvang en ondersteuning collega's: zoals spreker al aangaf is er weinig kennis in de organisatie, ook bij leidinggevenden, die een grote rol spelen in de opvang van collega's. Dit terwijl de opvang en ondersteuning wel echt iets vergt van de organisatie. Daarom wordt er veel onderzoek gedaan naar (de impact van) doxing. Omdat de leidinggevende een centrale rol heeft in de opvang en ondersteuning, wil men graag een moment creëren waarop medewerker en leidinggevende samen zitten om te kijken waar kwetsbaarheden zitten, bijvoorbeeld op sociale media en de veiligheidsinstellingen op de telefoon. Hiervoor wil men hen graag ondersteunen met goede digitale kennis.
- Partnerstrategie: spreker meldt dat er een goede procedure met de tech bedrijven is ingeregeld. De afdeling 'interceptie en sensing' van de landelijke eenheid is 'single point of contact' en 'trusted flagger' voor alle sociale media bedrijven. Zij hebben goede en snelle toegang tot deze bedrijven, zodat dingen direct kunnen worden verwijderd als dat moet. Het punt is echter dat dit binnen de organisatie nog niet echt bekend is, aldus spreker. Dit zal dus beter moeten worden gecommuniceerd en ingeregeld. In geval van doxing kan de 'interceptiedesk' van de eenheid naar de Landelijke Eenheid om de bevriezing of verwijdering te realiseren. Desgevraagd legt spreker uit dat een 'Notice en take down-procedure' een gestandaardiseerde manier is van aangeven wat er aan de hand is, waarmee richting het sociale media bedrijf of de provider kan worden aangegeven dat en waarom iets uit de lucht moet worden gehaald. Ook hiervoor geldt dat veel mensen deze procedure nog niet kennen en dat ook hierover dus beter moet worden gecommuniceerd, zegt hij.
- Communicatie en kennisontwikkeling: spreker is van mening dat het belangrijk is om de collega's te vertellen dat ze worden gesteund als hen iets overkomt en hen te informeren over hun eigen verantwoordelijkheid. Daarnaast komen er nieuwe fenomenen aan, zoals 'deep fake'. Het is van belang ook hier alvast over na te denken en dingen te ontwikkelen. In dit kader vindt ook communicatie plaats over het nieuwe handelingskader, over de formulieren en procedures et cetera die op intranet of agora worden gezet, zodat informatie snel vindbaar is.
- Verstoren: de heer 5.1.2.e legt uit dat dit een redelijk nieuw gebied is, dat technisch en juridisch zal moeten worden uitgezocht. Los daarvan moet er, als er sprake is van doxing, iets van worden gezegd. Dat geldt zowel voor degenen die doxen als voor degenen die het verspreiden. Overigens is het zaak om ook niet te proactief te zijn en zaken niet onnodig groot te maken. Technisch gezien kan om verstoring te bewerkstelligen via de algoritmen samenwerking worden gezocht met sociale media bedrijven. Dit is echter moeilijk te concretiseren. Spreker is van mening dat hiervoor met name in de crisisstructuur scenario's moeten worden ontwikkeld en mensen hierop te trainen. 5.2.1 . De voorzitter vraagt of agenten in dergelijke gevallen enkel worden gefilmd of dat zij ook daadwerkelijk worden belaagd. De heer 5.1.2.e bevestigt dat het gaat over filmen of het maken van foto's, zonder dat men weet wat er mee gedaan wordt. De heer 5.1.2.e wijst er in dit kader op dat het maken van foto's an sich nog geen doxing hoeft te zijn.
- Opsporing en vervolging: hiermee wordt bedoeld, dat wanneer er in geval van doxing opsporing en vervolging plaatsvinden, de collega van de resultaten daarvan op de hoogte wordt gesteld. De casemanagers GTPA kunnen een belangrijke rol spelen in de inbedding hiervan.

Sheet 5 en 6 – communicatie
Spreker geeft aan dat de wens bestaat voor een landelijke doxing website met alle beschikbare content.

De voorzitter vraagt of alle genoemde dimensies in plan van aanpak terugkomen. De heer 5.1.2.e bevestigt dat. Hierbij zal men zich vooral zal richten op dingen die kunnen en niet op dingen die niet kunnen. Desgevraagd geeft hij aan dat het plan van aanpak wordt gedeeld voordat de wetgeving er is. Hij

bespreekt het plan van aanpak, dat grotendeels is geschreven, volgende week met 5.1.2.e en 5.1.2.e .

Niet onder reikwijdte

De voorzitter dankt de heer 5.1.2.e voor de presentatie.

3. Buiten reikwijdte

Niet onder reikwijdte

- Niet onder reikwijdte

Buiten reikwijdte

c. Buiten reikwijdte
Niet onder reikwijdte

d. Buiten reikwijdte
Niet onder reikwijdte

Niet onder reikwijdte

[redacted]

4. Buiten reikwijdte

Niet onder reikwijdte

[redacted]

b. Wetsvoorstel Doxing/strafbaarstelling van het 'kale feit' doxing als bloot rechtsfeit.

De voorzitter geeft aan dat de Tweede Kamer vragen heeft gesteld die momenteel worden beantwoord. Als de beantwoording naar tevredenheid is dan gaat het voorstel naar de Eerste Kamer. De streefdatum van 1 januari 2023 is nog steeds reëel.

c. Onderzoek maatregelen om doxing tegen te gaan.

De voorzitter geeft aan dat dit zowel gaat over de maatregelen die in de wet zitten als over maatregelen om providers te verzoeken of dwingen om bepaalde dingen te doen om doxing tegen te gaan of te zorgen dat het stopt. Voor het traject 'online content modernisatie' is men vanuit het Rijk bezig met een plan van aanpak. De werkgever doet hier zelf niet zo veel mee. Het is echter goed om te weten dat dit loopt.

Buiten reikwijdte

[redacted]

e. Tegengaan van hinderlijk volgen politiecollega's (inclusief filmen/foto's) en observeren van politiebureaus.

Ook in dit kader verwijst de voorzitter naar de presentatie van de heer 5.1.2.e. Daarnaast was hier een actiepunt om te leren van de ervaringen in andere landen. Op de uitvraag naar onderzoeken zijn heel veel linkjes gekomen, die nog verder moeten worden verkend. Spreker brengt in herinnering dat de bonden ook nog zouden kijken. Desgevraagd geeft mevrouw 5.1.2.e aan dat zij hierover niets van de heer 5.1.2.e heeft gehoord. De voorzitter vraagt mevrouw 5.1.2.e haar collega's te vragen dit bespreekbaar te maken, met name bij de Scandinavische landen. Mevrouw 5.1.2.e reageert bevestigend. Onduidelijk is of er – zoals eerder gemeld – in het najaar van 2022 een congres zal plaatsvinden. Mevrouw 5.1.2.e suggereert dat de strafbaarstelling van doxing mooi is om te delen. Wellicht dat dit nog relevante informatie oplevert. Zij zal dit aan haar collega's meegeven.

Over de onderzoeken merkt mevrouw 5.1 2 e op dat een goede eerste stap zou zijn om met elkaar vast te stellen of de onderzoeken specifiek genoeg zijn. Zij vraagt of voor de werkgroep nog steeds het uitgangspunt is om hiervan te leren en wellicht zaken te kunnen toepassen? De voorzitter reageert bevestigend.

f Buiten reikwijdte

Niet onder reikwijdte

g. Buiten reikwijdte

Niet onder reikwijdte

5. Buiten reikwijdte

Niet onder reikwijdte

Buiten reikwijdte

Centraal Georganiseerd Overleg Politie (CGOP)
Werkgroep Rechtspositie Bescherming Dienders (WGRPBD)

Actiepuntenlijst van de WG RPBD van 15 september 2022 – organisatorisch

Datum vergadering	Actie-punt	Onderwerp	Actie	Actiehouder	Gereed
Niet onder reikwijdte					

Bespreekpuntenlijst van de WG RPBD van 15 september 2022 – inhoudelijk

Doxing – Aanwezigheid en vindbaarheid online – Filmen, hinderlijk volgen en observeren

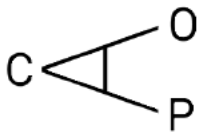
(sub) onderwerp	*Nog nader uit te werken*	*Stand van zaken*	*Actie*
Filmpjes offline halen		Afdeling 5.1.2.e van de LE is 'single point of contact' en 'trusted flagger' voor alle sociale media bedrijven.	NP – communicatie hierover in de organisatie
		'Notice en take down-procedure' is in gebruik.	NP – communicatie hierover in de organisatie
Wetsvoorstel doxing		Momenteel worden de vragen van de Tweede Kamer beantwoord.	Afwachten en stand van zaken delen in de werkgroep
Voorstelbare dreiging	Welke maatregelen kunnen worden getroffen zodra sprake is van voorstelbare dreiging.	Bij 'nationale veiligheid' is dit onderzocht. Kijken wat in de beleidsvorming kan worden meegenomen.	NP – afwachten
	Welke andersoortige voorzieningen zijn er?	Kijken hoe leidinggevenden ondersteund kunnen worden in de hulp die zij aan medewerkers geven.	NP – Vergroten van bekendheid van de voorzieningen
Buiten reikwijdte			
	Buiten reikwijdte		
Jur. analyse huidige wetgeving	Loopt, analyse nog niet gereed. Bep. vormen van filmen zullen strafbare doxing opleveren.	Onbekend	JenV – afwachten
Niet onder reikwijdte			

Gesprek met providers en tech-bedrijven

(sub) onderwerp	*Nog nader uit te werken*	*Stand van zaken*	*Actie*
Niet onder reikwijdte			

Algemeen – Geweld Tegen Politie Ambtenaren

(sub) onderwerp	*Nog nader uit te werken*	*Stand van zaken*	*Actie*
Niet onder reikwijdte	Niet onder reikwijdte		
	Niet onder reikwijdte		



	Niet onder reikwijdte						

Doxing als strafbaar feit

Implementatieplan Politie

Door	5.1 2 e
Afdeling	Staf Korpsleiding | Directie Operatiën | 5.1.2.e
Versienummer	0.9
Datum	28 september 2023
Kenmerk	Projectplan
Status	Definitief
Rubricering	Politie INTERN - Bedrijfsvoering

Inhoudsopgave

Overzicht stakeholders

DOELSTELLING PROJECT			
1. De organisatiebrede implementatie van doxing als strafbaar feit, in samenwerking met de betrokken organisatieonderdelen en disciplines, 2. Het werkend maken van het handelingskader doxing voor de teamchef en zorgen voor de monitoring en doorontwikkeling van dit werkproces.			
STAKEHOLDERS			
Rol	**Naam**	**Eenheid**	**Toelichting - Omschrijving**
Opdrachtgever	5.1.2.e		
Projectleider	5.1.2.e		
INTERN			
OPSPORING			5.1.2.e
DIENST VERLENING	5.1.2.e		
GGP	5.1.2.e		
COMMUNICATIE	5.1.2.e		

			5.1.2.e
GTPA	5.1.2.e		
VIK	5.1.2.e		
IV-BEVEILIGING	5.1.2.e		
CCB-PARAATHEID	5.1.2.e		
JURIDISCH	5.1.2.e		
DIGITALE EXPERTISE	5.1.2.e		
KENNIS MANAGEMENT	5.1.2.e		

KENNISEIGENAAR	5.1.2.e		
INFORMATIE MANAGEMENT **Advies en meelezen op afstand.**	5.1.2.e		
VKK STAF-DO	5.1.2.e		
IBT-OBT	5.1.2.e		
EXTERN			
OPENBAAR MINISTERIE	5.1.2.e		
DEPARTEMENT V&J	5.1.2.e		
MINISTERIE VAN BINNENLANDSE ZAKEN	5.1.2.e		

1 Inleiding

1.1 (Politie)doxing in context

Wetgeving

Onder doxing wordt in de volksmond doorgaans verstaan: 'het delen van persoonsgegevens met intimiderende intenties'. In het beoogde artikel 285d h Sr definieert de wetgever het strafbaar feit (samengevat) als volgt: 'het delen van persoonsgegevens met het oogmerk om de ander vrees aan te jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen'. In het kader van dit projectplan benoemen wij dit strafbare feit als doxing.

Alhoewel doxing als fenomeen vijf jaar geleden in Nederland nog vrij onbekend was nam het sinds 2019 een hoge vlucht, in tijden van sociale spanningen en maatschappelijke onrust. Gedurende de Coronapandemie en tijdens bijvoorbeeld de omvangrijke Boerenprotesten werd doxing doelbewust als instrumenteel intimidatiemiddel tegen overwegend frontlijnmedewerkers als politieagenten ingezet. Het op grote schaal – en hoofdzakelijk online - delen van persoonsgegevens van politieagenten of daartoe al dan niet indirect oproepen werd in deze periode eerder regel dan uitzondering. Doxing lijkt inmiddels een ingrijpend en effectief intimidatiemiddel verworden dat naast politieagenten ook politici, wetenschappers en medici treft.

De beschikbare (wetenschappelijke) kennis en inzichten rond politiedoxing is nog zeer beperkt. Het fenomeen is vrij nieuw en speelt – voor zover vast te stellen – nog slechts in een klein aantal landen. De oorzaak kan onder meer worden gezocht in het afnemend vertrouwen in overheid, politiek en het politieapparaat; Institutionele erosie genoemd. [1]

Het delen van persoonsgegevens met het door de wetgever omschreven oogmerk gebeurt echter al langer en is gerelateerd aan maatschappelijke bewegingen als bijvoorbeeld de zogeheten cancelculture en volgt vaak op naming and shaming van personen via het internet. Sociale media fungeren als gelegenheidsstructuur en bieden kwaadwillende personen mede door de snelle verspreiding in grote groepen een groot podium via uiteenlopende platformen.

Dit document bevat het projectplan voor de politie in relatie tot doxing als nieuw strafbaar feit in Nederland. De strafbaarstelling van dit delict, per 1 januari 2024, heeft invloed op diverse organisatieonderdelen, portefeuilles en taakvelden. Dit project biedt overzicht ten aanzien van de verschillende actoren, stakeholders en geeft een overzicht van wat dit voor de politie als uitvoeringsorganisatie betekent.

Ten aanzien van doxing heeft de Politie een bijzondere dubbelrol; enerzijds op samenlevingsniveau als dienstverlener maar óók als werkgever, in het geval van politiedoxing. Nederlandse politieagenten worden als beroepsgroep óók door doxing getroffen en daarom bestaat er vanuit het perspectief van de werkgeversverantwoordelijkheid een interne opgave. De opbrengst van recent, intensief praktijkonderzoek naar politiedoxing heeft het belang van het tijdig onderkennen en acteren in geval van politiedoxing aangetoond. Voor het korps is er inmiddels voor de direct leidinggevenden een handelingskader politiedoxing ontwikkeld.

Aan zowel de teamchef als lijnverantwoordelijke en de binnen dit kader opgenomen disciplines zijn verschillende rollen en taken toegekend. Het werkend maken van dit kader en ook de doorontwikkeling ervan vraagt om organisatiebrede kennisdeling- en borging, training en scholing. Het implementatietraject wordt vanuit de portefeuille Geweld Tegen Politieambtenaren (GTPA) uitgevoerd.

Dit plan van aanpak biedt overzicht binnen de verschillende fasen van het implementatietraject en de gehanteerde prioritering. Daarnaast bevat het een omschrijving van de vastgestelde rollen en verantwoordelijkheden van de procesdeelnemers en stakeholders en een overzicht van concrete actiepunten per portefeuille.

---

[1] 5.1.2.e , *Thesis Politiedoxing,* 5.1.2.e , *2023.*

1.2 Ontwikkelingen

In de loop van 2020 intensiveerde binnen het korps de aandacht voor het fenomeen doxing, dat zich destijds overwegend richtte op de collegiale opvang en ondersteuning van gedoxte politiemedewerkers en hun thuisfront. Vanuit het perspectief van goed werkgeverschap en de raakvlakken met het programma VPT-GTPA heeft de politie inmiddels de eerste stappen gezet: vanuit praktijkonderzoek naar doxingcasuïstiek is een goed werkbaar Handelingskader Politiedoxing voor teamchefs opgeleverd.

Generiek strafbaar feit

Omdat de strafbaarstelling van doxing in Nederland echter niet enkel geldt voor politieagenten, maar voor eenieder, dient de politie zich als uitvoeringsorganisatie breed op de komst van dit strafbaar feit te prepareren. Hiervoor zal per organisatieonderdeel de uitvoeringsconsequentie moeten worden bepaald, tezamen met de vervolgstappen en de concrete acties die dit oplevert. Binnen het projectplan en de implementatiefase wordt een onderscheid gehanteerd tussen de 'reguliere' vormen van doxing en het werkproces rond politiedoxing. Een toelichting op dit onderscheid en wat dit concreet betekent leest u in paragraaf 2.3. Daarnaast wordt noodgedwongen, gezien de druk op het implementatieproces wegens de naderende strafbaarstelling, een prioritering aangebracht in zaken die in het nu en voor later relevant zijn.

Opdracht en mandaat

Dit onderhavige plan wordt uitgevoerd in opdracht en met mandaat van portefeuillehouder GTPA Peije de Meij en Programmaleider Veilige Publieke taak & GTPA 5.1.2 e. Dit implementatietraject is niet dermate omvangrijk dat een portfolioproces wordt gevolg; de impact op de eenheden en haar capaciteit is beperkt.

De realisatie van dit projectplan doxing wordt uitgevoerd door 5.1.2 e in de rol van landelijk projectleider en in samenwerking met de verschillende kwartiermakers per eenheid.

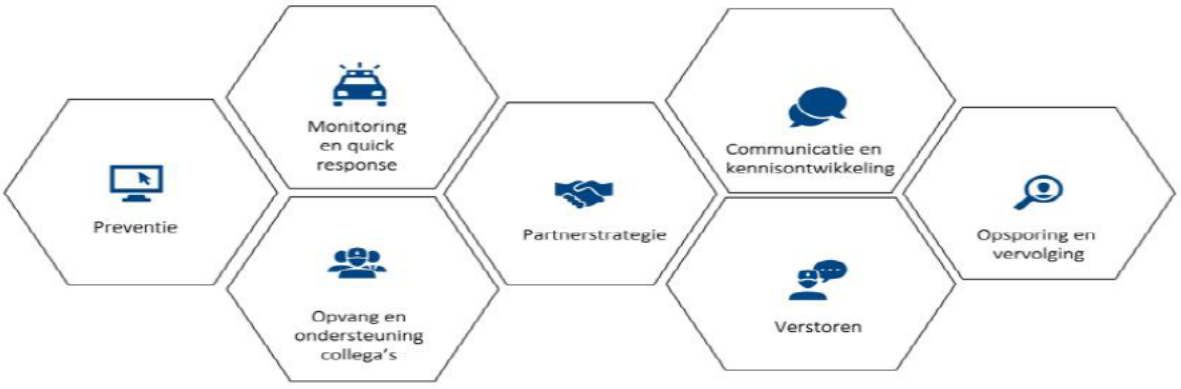
1.3 Voorgeschiedenis

Politiedoxing

In de loop van 2020 intensiveerde de ontwikkeling en strategievorming ten aanzien van de integrale organisatiereactie op politiedoxing. Dit leidde in 2021 mede tot een oproep van de korpschef aan de Minister om doxing strafbaar te stellen. De ontwikkeling van een interne aanpak alleen al voor politiedoxing vroeg om een brede benadering en leidt tot betrokkenheid en capaciteit van verschillende organisatieonderdelen en disciplines. Een eerder vanuit de portefeuille GTPA opgesteld (voorlopig) plan van aanpak dat in mei 2022 in het BOO (Breed Operationeel Overleg) werd omarmd, bevatte de onderstaande doelstelling:

De medewerkers van de politiezijn zich bewust van de gevaren en impact van doxing en nemen de nodige preventieve maatregelen. Daarnaast worden de medewerkers die toch slachtoffer zijn geworden van doxing op praktisch en sociaal-emotioneel gebied ondersteund door de organisatie.

In dit voorlopige plan worden de onderstaande zeven dimensies genoemd als belangrijke pijlers voor de integrale aanpak van politiedoxing:



Bron: Plan van aanpak doxing, 5.1.2.e, september 2022.

Het huidige projectplan wordt mede vormgegeven aan de hand van de inzichten die binnen het bovenstaande ontwikkelproces zijn opgedaan.

Handelingskader politiedoxing

Vanuit het werkgeversperspectief is inmiddels – gekoppeld aan de dimensie 'collegiale opvang en ondersteuning' – een eerste handelingskader voor leidinggevenden opgeleverd. Dit kader richt zich op een eerste processtructurering ingeval van politiedoxing, waarbij aan diverse specialismen en disciplines specifieke rollen en taken zijn toegekend. Het welzijn en de fysieke veiligheid van de gedoxte politiemedewerker en hun thuisfront staan binnen deze werkwijze centraal. De teamchef heeft in dit proces een regisserende rol en bedient zich van kennis en deskundigheid die wordt opgehaald vanuit diverse disciplines.

De ervaren gevolgen van de instrumentele toepassing van politiedoxing houdt – zo blijkt uit een eerste onderzoek naar dit fenomeen – sterk verband met de aanpak door de politieorganisatie en kent op hoofdlijnen een sociaal-emotionele en praktisch-inhoudelijke kant. De combinatie van maatregelen en objectieve inschattingen dienen bedreigde medewerkers het gevoel te geven dat hun emoties voldoende worden onderkend en begrepen, én dat hun veiligheid (en die van hun omgeving) op een aanvaardbaar niveau wordt gebracht.

Het ontwikkelde handelingskader voor leidinggevenden geldt als een eenduidig, landelijk werkprocesdocument. Vanwege de (steevast aanwezige) complexiteit qua verloop van politiedoxing en de hieraan verbonden noodzakelijke handelingssnelheid, is het zaak om de binnen het kader betrokken disciplines van valide informatie en concrete handvatten te voorzien. Binnen het algehele implementatieproces en vanuit het perspectief van werkgeversverantwoordelijkheid zal het werkend maken van dit kader de eerste prioriteit zijn, waarna via ervaringsleren de verbeter-en ontwikkelpunten vastgesteld dienen te worden.

1.4 Projectdoelstelling

Omdat de strafbaarstelling van doxing echter geldt voor eenieder dient de Politie zich qua implementatie op zowel het generieke deel – de invoering van doxing als nieuw strafbaar feit – als de interne (door)ontwikkeling en procesvoering rond politiedoxing te richten. In bovenstaand verband bezien kent het huidige projectplan de onderstaande hoofddoelen:

1. Realiseren dat het generieke strafbaar feit doxing in het korps geïmplementeerd wordt, in samenwerking met de betrokken organisatieonderdelen en de portefeuille VPT-GTPA.
2. Zorgdragen dat ten aanzien van GTPA het handelingskader doxing voor leidinggevenden en zijn bedoelde werking gaat linden in het korps en via ervaringsleren wordt doorontwikkeld.

In paragraaf 2.3 zijn de subdoelen per organisatieonderdeel beschreven en uitgewerkt tot concrete, geprioriteerde actiepunten.

2 Implementatieopgave wetsvoorstel

2.1 De opdracht

De komst van het strafbaar feit doxing heeft invloed op bestaande processen, systemen en applicaties, maakt aanpassingen noodzakelijk binnen verschillende portefeuilles en vraagt om het aanbieden van eenduidige en gevalideerde informatie aan zowel burgers als politiemedewerkers.

Vanaf het moment van de inwerkingtreding van doxing als strafbaar feit zal de politieorganisatie samen met het Openbaar Ministerie optrekken binnen het proces van opsporing en vervolging. Hierbij zijn de bestaande afspraken uit de ELA (Eenduidige Landelijke Afspraken) - omtrent agressie en geweld tegen functionarissen met een publieke taak – het vertrekpunt.

Een eerdere impactanalyse rond de komst van doxing als nieuw feit levert het beeld op dat de impact – qua verwachte aantallen delicten – voor de politieorganisatie beperkt is. Omdat doxing echter sterk verband houdt met sociale spanning en maatschappelijk ongenoegen is een adequate inschatting van capaciteit en werklast eenvoudigweg nu niet te maken. De implementatieopgave is onderverdeeld in het generieke werkproces rond doxing en het werkproces rond het fenomeen politiedoxing.

Voor het generieke werkproces rond doxing is van belang dat;

- De systemen van de betrokken organisatieonderdelen zijn ingericht en toegerust op de verwerking van doxing als nieuw strafbaar feit,
- De aan de burger verstrekte algemene informatie overal in en vanuit het korps hetzelfde is, ongeacht het type medium of applicatie dat gebruikt wordt,
- De binnen de betrokken portefeuilles werkzame medewerkers over voldoende gevalideerde informatie en kennis beschikken om hun taken goed uit te kunnen voeren,
- Gevalideerde informatie en kennis op de juiste platformen beschikbaar wordt gesteld en er sprake is van onderhoud in het kader van kennismanagement, m.a.w. de borging en beheer van politiekundige informatie,
- De projectleider op hoofdlijnen de sturing van de implementatieopgave kan blijven uitoefenen,
- Er hiervoor per eenheid een centraal contactpersoon/ aanspreekpunt wordt ingeregeld;
    - Als schakel tussen de rol van de projectleider op hoofdlijnen en de ontwikkelingen en ervaringen binnen het operationele werkveld,
    - Als contactpersonen op zowel inhoudsniveau als ten aanzien van de geldende werkprocessen,
- De projectleider periodiek ruggespraak heeft met deze contactpersonen rond de implementatieopgave en kan bijsturen waar nodig.

Voor het interne werkproces rond politiedoxing is het van belang dat:

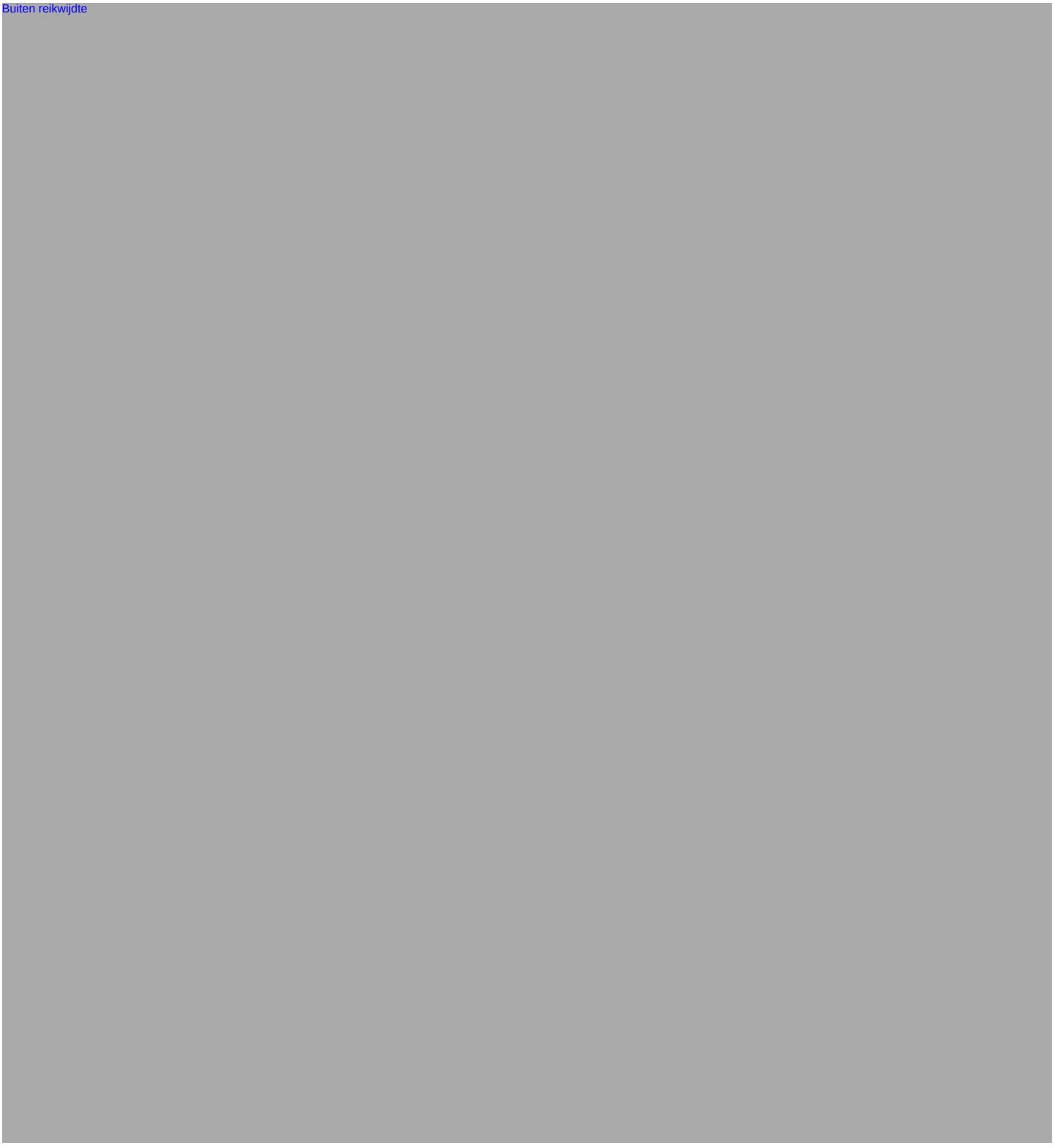
- De leidinggevenden en de betrokken specialismen voldoende zijn uit- en toegerust om hun rol en verantwoordelijkheid per 1 januari 2024 goed uit te kunnen voeren,
- Het ontwikkelde handelingskader politiedoxing als werkinstructie via de bestaande kanalen met het operationele en tactisch leidinggevende kader wordt verspreid,
- Er sprake is van landelijke monitoring van de met het handelingskader opgedane ervaringen,
- Elke politie-eenheid beschikt over een centraal aanspreekpunt, dat vanuit materiedeskundigheid aan de hulpvragen of informatiebehoefte vanuit casuïstiek kan voldoen,
- De projectleider periodiek overleg voert met deze materiedeskundigen per eenheid om het proces van ervaringsleren te monitoren.

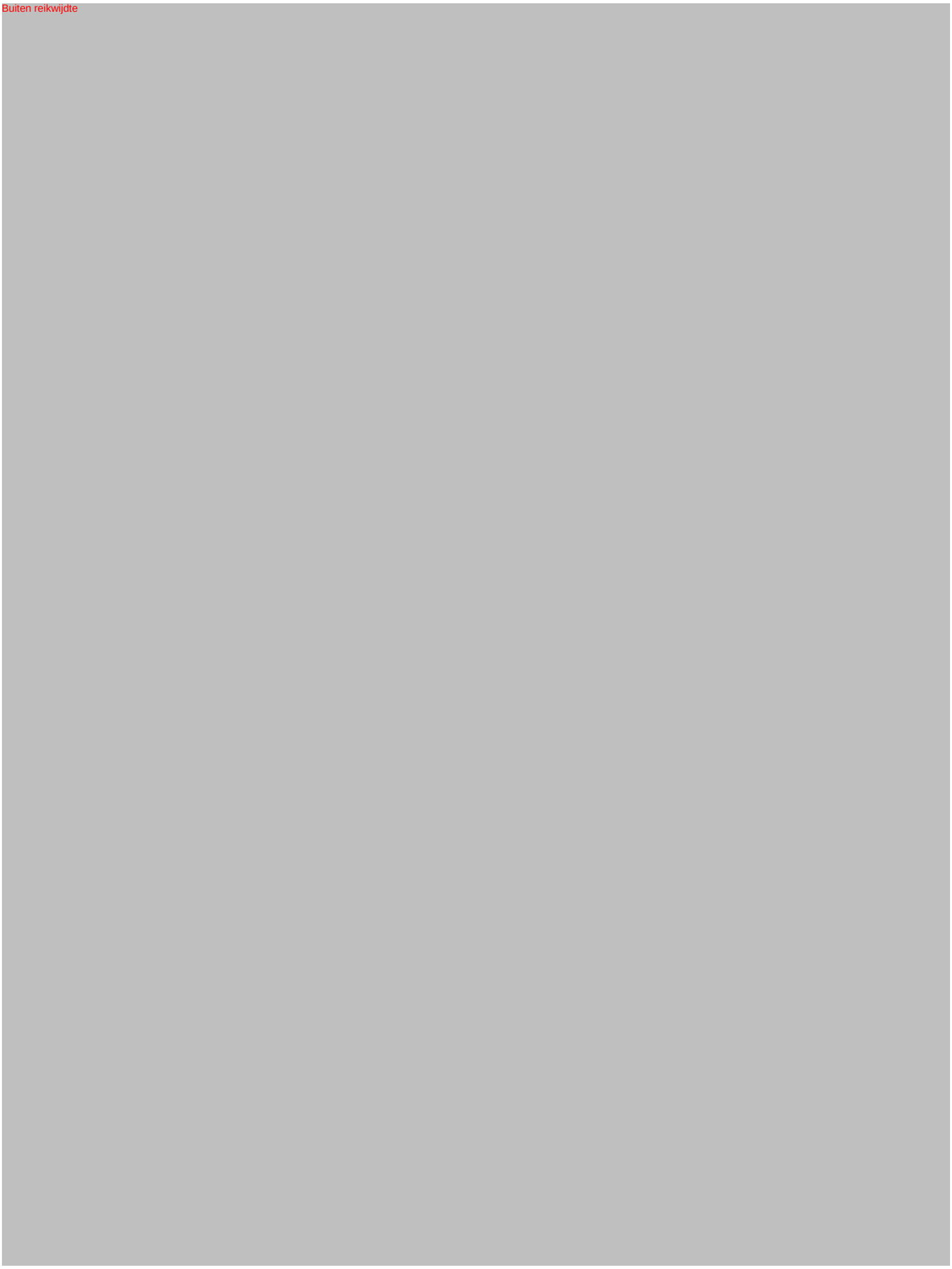
Aan de hand van dit projectplan is om besluitvorming ten aanzien van:

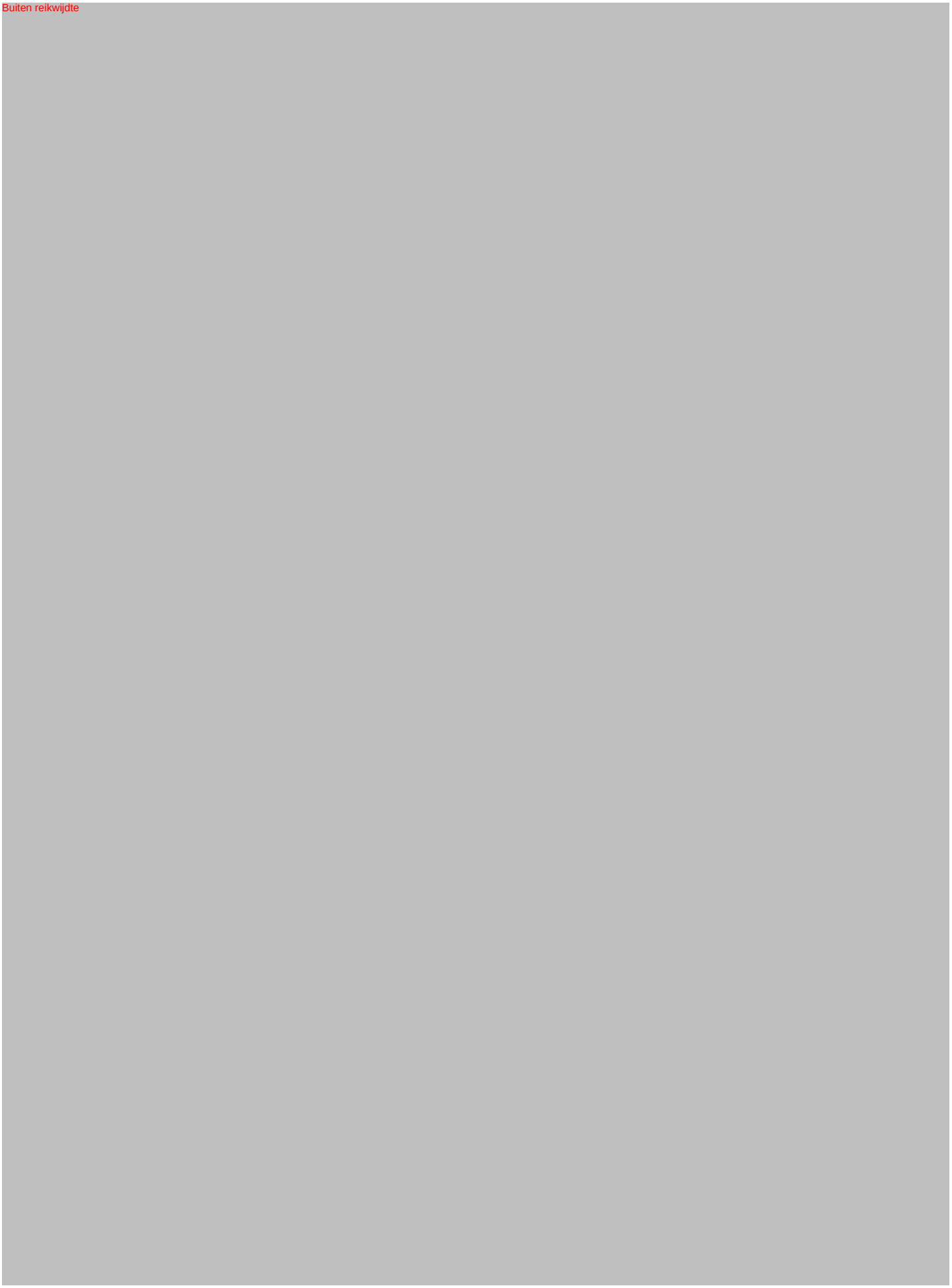
- **Paragraaf 2:** De implementatieopgave ten aanzien van het wetsvoorstel en de zowel in-als externe actie-en ontwikkelpunten die hieraan zijn verbonden,
- **Paragraaf 3:** Het vanuit de perspectieven van risicoreductie en borgingsaspecten benoemen van een kwartiermaker per politie-eenheid die verantwoordelijk is voor;
    - Het starten van het borgingsproces, via het aanstellen van een centrale contactpersoon voor de vragen en/of informatiebehoefte vanuit het werkveld,
    - Het creëren van een centraal en materiedeskundig intern aanspreekpunt rond doxing in zowel generieke zin als voor het werkproces rond politiedoxing.

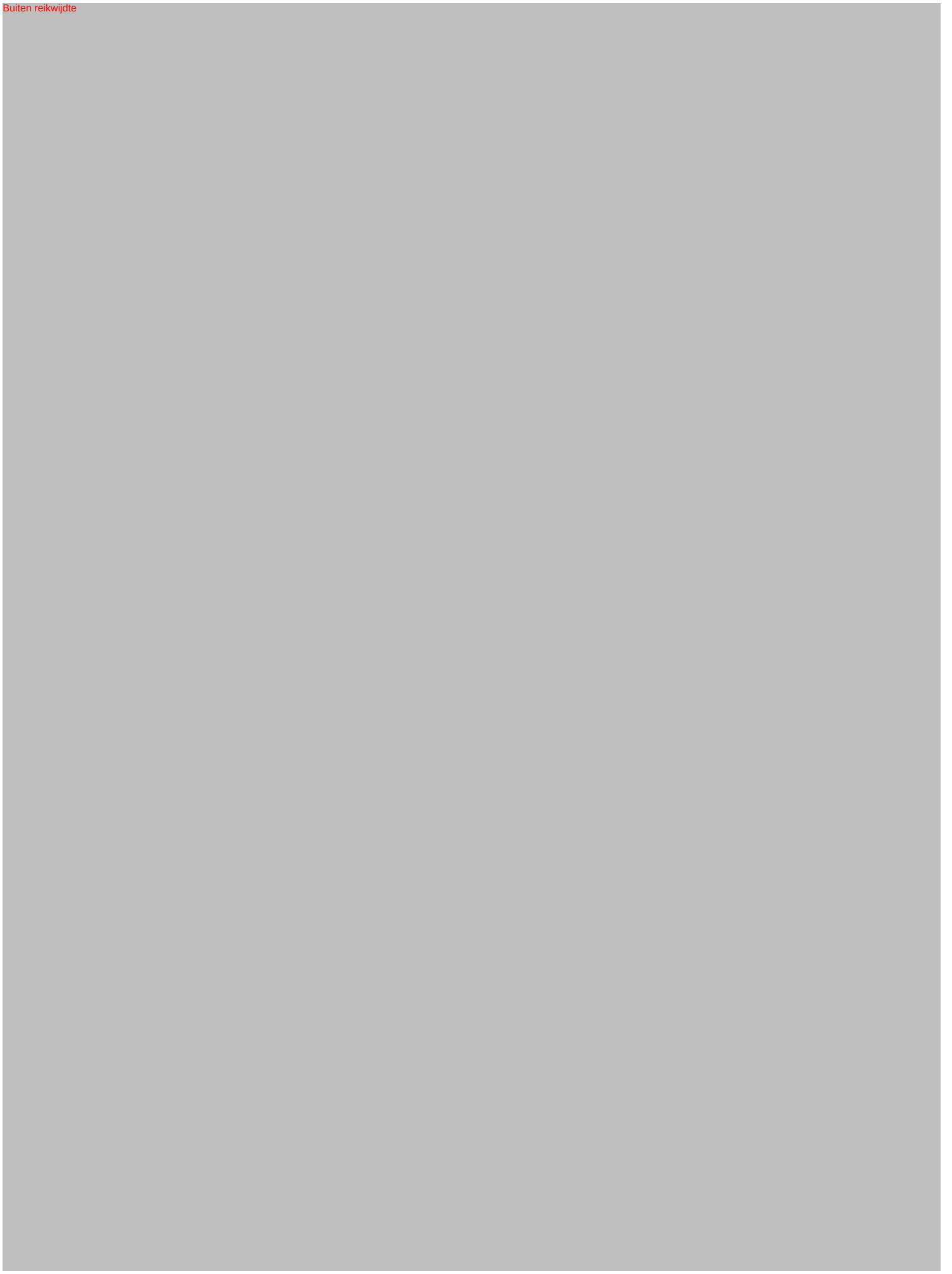
2.2 Operationele uitvraag diverse portefeuilles

2.3 Actiepunten per organisatieonderdeel




Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte

3 Risicoreductie en borging: korte termijn

Binnen dit projectplan is sprake van een voorzienbaar risico dat het implementatie-en borgingsproces kwetsbaar maakt. De deskundigheid ten aanzien van (politie)doxing ligt op dit moment namelijk besloten bij slechts enkele personen in het korps. Daarnaast is momenteel nog geen sprake van interne aanspreekpunten per eenheid om aan de (informatie)behoeften, vragen en noodzakelijke expertise vanuit het werkveld te voldoen. In redelijkheid mag worden verwacht dat de komst van het strafbaar feit doxing zorgt voor een dergelijke kennis-en informatiebehoefte op zowel het proces-als themaniveau. Het werkproces rond politiedoxing zal – naar verwachting – leiden tot eenzelfde soort vragen of behoeften.

De projectleider richt zich vanuit een regierol met een tactisch-strategische blik volledig op de hoofdlijnen van dit organisatiebrede implementatie-en borgingsproces. Het contact en de afstemming met de betrokken stakeholders vraagt in de fase van implementatie nadrukkelijk tijd en aandacht vanuit deze rol en positie. Het ontbreken van centraal georganiseerde toegang tot voldoende deskundige contactpersonen in de eenheden kan daarnaast leiden tot het overvragen van de projectleider, op casusniveau.

Vanuit de perspectieven van risicoreductie en het doel van uiteindelijke organisatieborging bezien zijn de volgende zaken relevant;

1. Kennis delen is vermenigvuldigen; een groot deel van de kennis en materiedeskundigheid ligt nu hoofdzakelijk bij enkele personen besloten, terwijl het onderwerp vraagt om organisatiebrede overdracht, toegang en borging. Naast het proces van kennismanagement – dat zich richt op de organisatiebrede ontsluiting van eenduidige, gevalideerde informatie – is elke eenheid gebaat bij (enkele) materiedeskundige medewerkers, op zowel het proces-als inhoudsniveau.
2. In het kader van de invoeringstoets doxing – gericht op de vaststelling of sprake is van knelpunten bij de uitvoeringsorganisaties – is voor tussentijdse bijsturing een spoedige terugkoppeling naar de beleidstafels noodzakelijk. De projectleider is belast met deze afstemmingslijnen richting het Openbaar Ministerie en Departement V&J en dient hiervoor te beschikken over de ervaringen vanuit het werkveld, zoals
    a. Is de wet moeilijk toe te passen of te interpreteren?
    b. Zijn er knelpunten ten aanzien van de juridische elementen van dit artikel, w.o. de bewijslast en het element ‘oogmerk’,
    c. Werkt het snel verwijderen van gegevens bij doxing in de praktijk op een vergelijkbare manier als bij andere delicten?
    d. Bestaan er knelpunten ten aanzien van het uitleggen of toepassen van deze wet?
3. In het kader van het ervaringsleren en de te maken ontwikkelslag binnen het werkproces politiedoxing is organisatiebrede monitoring op de werking in de praktijk noodzakelijk. De projectleider belegt hiervoor periodiek een moment van afstemming en overleg met de aangestelde contactpersonen per eenheid.

3.1.1 Aanwijzen kwartiermakers

Buiten reikwijdte

3.1.2 Kennismanagement

Buiten reikwijdte

Typ Naam Dienst of Naam Eenheid
Typ Postadres Dienst of Postadres Eenheid

Werkgroep doxing politie en dgpenv

1. Kennismaken
2. Bespreken wat we wel en wat we niet willen oppakken in de werkgroep doxing en hoe we dat willen aanpakken (Zijn er onderwerpen die ten onrechte wel of niet in onderstaand schema zitten (zie ook relevante afgesproken actiepunten in bijlage 1)

Actiepunten vanuit de WGRPBD relevant voor aanpak doxing en bezien of nadere actie vanuit werkgroep doxing nodig is of anderszins			
Buiten reikwijdte			
Verkenning politieambtenaren die gevolgd en gefilmd worden.	Gedachte: 1. aard/omvang: voorbeelden ophalen binnen politie en bij vakbond 2. inventarisatie mogelijke maatregelen -rond politiebureau -rond huis -elders 3. analyse wetgeving		
Buiten reikwijdte			

Buiten reikwijdte

Overig		
Buiten reikwijdte		
...		

Werkgroep doxing politie en dgpenv

1. Kennismaken
2. Bepreken doel van deze werkgroep
3. Bespreken wat we willen oppakken in de werkgroep en hoe we dat willen aanpakken
   a. Actiepunten vanuit de WGRPBD relevant voor aanpak doxing en voorstel nadere actie

Preventie		WGRPBD	Werkgroep doxing
Buiten reikwijdte			
	aard en omvang probleem politieambtenaren die gevolgd en gefilmd etc worden en mogelijke maatregelen die al worden genomen door politie of zouden kunnen worden genomen.	verkenning politie en jenv	verkenning werkgroep doxing? - aard/omvang: voorbeelden ophalen binnen politie en bij vakbond? -inventarisatie mogelijke maatregelen -rond politiebureau -rond huis -elders

Buiten reikwijdte

Buiten reikwijdte

Repressie	Buiten reikwijdte		
	wetgevend kader filmen etc	Verkenning	werkgroep doxing? aanzet juridische analyse (5.1.2.e)?

Buiten reikwijdte

b. Voorstel: de werkgroep doxing ook laten kijken naar de volgende onderwerpen: wat gebeurt daar al dan niet op/ is het voldoende; en aparte vraag: kunnen we een en ander ook meenemen naar WGRPBD of juist niet:
   - politie intern beeld probleem van doxing (aard en omvang) samen met uitvraag filmen etc?

Met opmerkingen (5.1.2.e) niet eens, keep it smart!

Buiten reikwijdte

- ...

Mogelijk relevante actiepunten WGRPBD 25 oktober 2021

Primair relevant
Secundair relevant (vooralsnog)

Datum vergadering	Actie-punt	Onderwerp	Actie	Actie-houder	Gereed
Niet onder reikwijdte					
Niet onder reikwijdte					
Niet onder reikwijdte					

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte					
25-10-2021	#19 en #20	Filmen, hinderlijk volgen en observeren collega's	Nadere verkenning over de strafbaarheid van filmen, hinderlijk volgen en observeren van collega's. Bekijken welke maatregelen men in de verschillende situaties kan nemen.	Politie en JenV	
Niet onder reikwijdte					

Niet onder reikwijdte

Met opmerkingen 5.1.2.e **:** Een overzicht van de rechtspraak al beschikbaar?

Niet onder reikwijdte

Afspraken stellingname:			
1.	***Beschermen van de medewerker tegen fysieke vormen van agressie en geweld:***	-	
a.	[redacted]	[redacted]	Niet onder reikwijdte [redacted]
2.	***Beschermen van de medewerker tegen online agressie:***	-	
a.	Srafbaarstelling van het 'kale feit' doxing.	Consultatie afgerond.	Consultatie afgerond ; consultatieadviezen verwerken en dan naar RvS
b.	Onderzoek overige maatregelen om doxing en privacyinbreuken politieagenten tegen te gaan, waaronder gesprek met providers en tech-bedrijven.	Ideeen voor maatregelen bespreken met de bonden. Subwerkgroep cao doxing J&V en politie. Daarin wordt gekeken naar handelingskader en voorstellen bonden in de bijlage van de stellingname.	Vraag: Wie moet welk gesprek voeren providers en tech-bedrijven en waarover?

c.	Interne voorlichtingscampagne over veiligheidsrisico s aanwezig- en vindbaarheid op internet.	Stavaza politie?	Politie: loopt toch?
d.	Hinderlijk volgen politiecollega s (inclusief filmen/foto s) en observeren van politiebureaus tegengaan.	Wat willen de bonden hiermee?	Vraag : Van wie wordt actie gevraagd en welke actie?
3.	Buiten reikwijdte	-	
a.	Niet onder reikwijdte		
4.	Buiten reikwijdte	-	
a.	Niet onder reikwijdte		

Voorstellen bijlage stellingname; te toetsen/verkennen op proportionaliteit /wenselijkheid/ haalbaarheid/ uitvoerbaarheid:	-	-	
1.	***Maatregelen om diender te beschermen tegen 'kale doxing' (iedereen die zonder redelijk doel foto's/filmpjes plaatst):***	-	

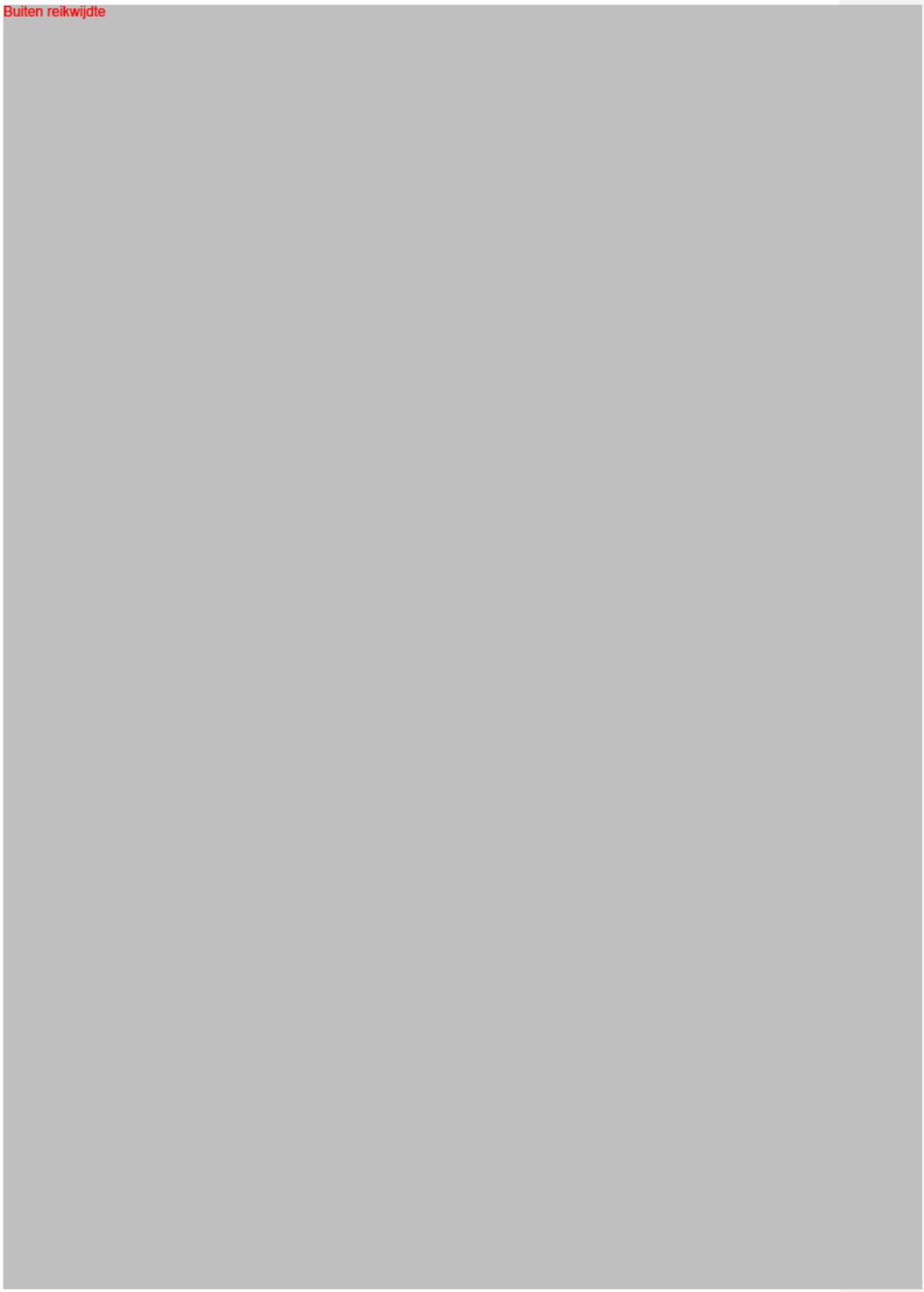
a.	Strafbaarstelling doxing		Zie onder punt 1 hierboven.
b.	Verplichting tot blurren van gezichten politiemensen op foto's en filmpjes sociale media.	WG Doxing?	Heroverweging standpunt wetgeving tov blurbrief 2017.Zie voorstel werkgroep onder punt 2 hierboven.
c.	Verwijderen van filmpjes en foto's speciale media door providers.	WG Doxing?	Op verzoek van politie als werkgever? Zie punt e hieronder. Mogelijk eerst te bespreken in voorgestelde subwerkgroep, zie punt 2 hierboven.
d.	Plaatsen van een waarschuwing dat informatie cq wat te zien is in filmpjes/foto's met duiding voorzien worden van: niet geverifieerde feiten.	Door politie of provider?	Door politie (commuicatie?)?
e.	Onderzoek naar inzetten wetgeving schenden privacy.	Wat bedoelen bonden hiermee? Wordt hiermee bedoeld inzet civiele recht door werkgever.	Wordt hier bedoeld inzetten door politie als werkgever? Mogelijk eerst bespreken in voorgestelde subwerkgroep, zie onder punt 2 hierboven.
f.	Collega's worden soms hinderlijk gevolgd waarbij ook opnamen worden gemaakt en geplaatst op sociale media. maatregelen om dit tegen te gaan.	Wat willen bonden hiermee?	Zie afspraak 2d. stellingname.
g.	Plaatsing foto's/filmpjes etc. alleen mogelijk als individu bekend is bij provider cq alleen op naam.	WG Doxing	Bespreken in voorgestelde subwerkgroep (relatie met petititie Gordon?)
2.	Buiten reikwijdte		
a.	Niet onder reikwijdte		

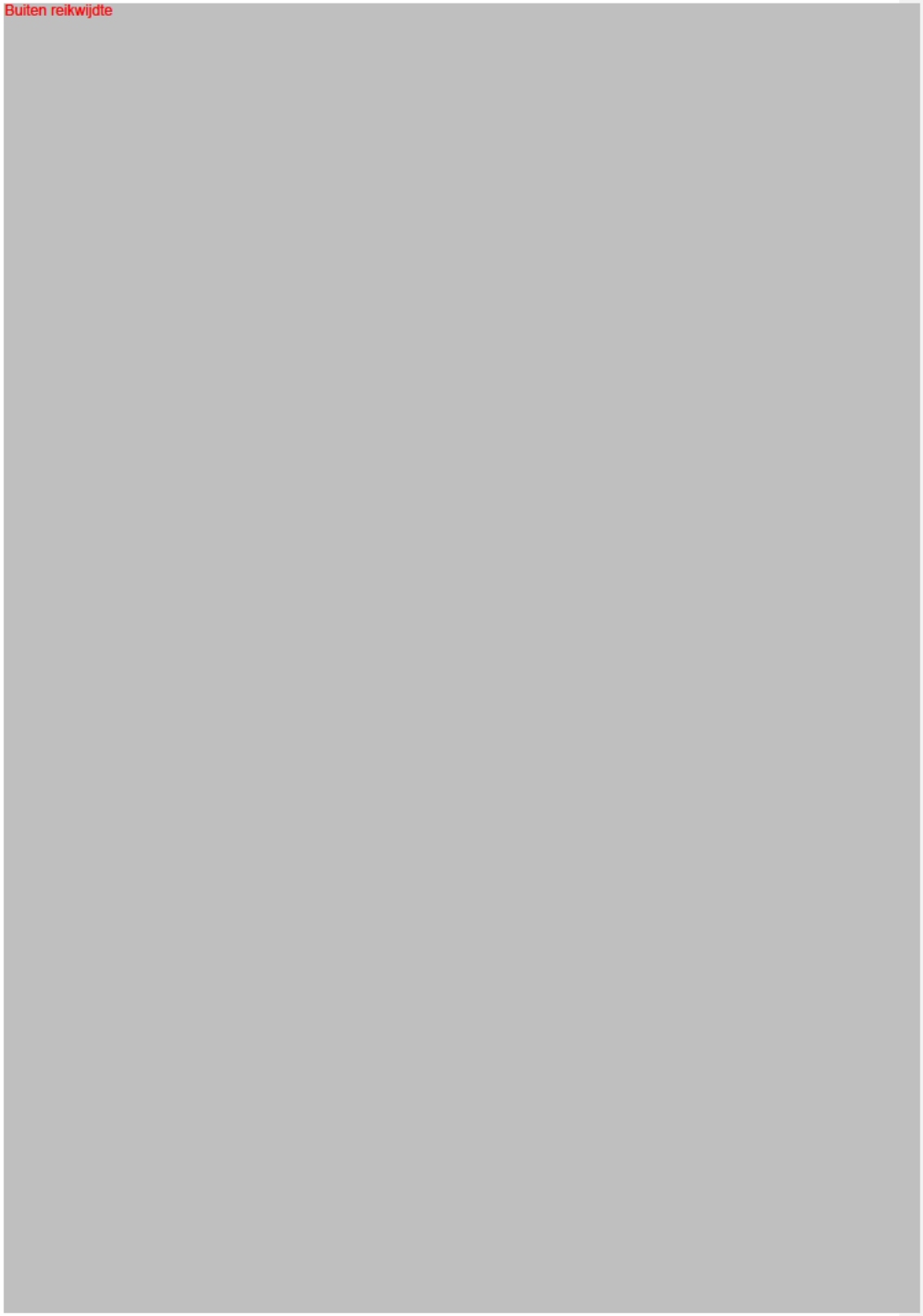
c.			Niet onder reikwijdte

h.	Niet onder reikwijdte		
3.	Buiten reikwijdte	-	
a.	Niet onder reikwijdte		
-	-	-	
-	-	-	
c.	Aanpak ontwikkelen om tegen te gaan dat politiebureaus in aantal steden worden geobserveerd om opnamen te kunnen maken van collega's en te achterhalen wie ze zijn etc.	Kan politie preventieve maatregelen nemen? Wat willen we precies?	Zie afspraak 2d stellingname. Is dit preventieve actie of de vraag naar een strafbaarstelling?
-	-	-	

d.			Niet onder reikwijdte
-	-	-	
-	-	-	
4.	Buiten reikwijdte	-	

a.	Niet onder reikwijdte		
-	-	-	
-	-	-	
c.	Na rechterlijke uitspraak verwijderen beeld en tekstmateriaal van internet en sociale media. Verdere verspreiding strafbaar stellen.	WG Doxing	Bespreken in voorgestelde werkgroep onder 2.


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte

Mogelijk relevante actiepunten WGRPBD 25 oktober 2021

Primair relevant
Secundair relevant (vooralsnog)

Datum vergadering	Actie-punt	Onderwerp	Actie	Actie-houder	Gereed
Buiten reikwijdte					
Buiten reikwijdte					
25-10-2021	#9	Gesprek met providers en tech-bedrijven	Terugkoppelen wat er in de organisatie gebeurt op het punt van het offline halen van gemonteerde filmpjes zonder of met onjuiste context	5.1.2.e	
Buiten reikwijdte					
25-10-2021	#13	Strafbaarstelling doxing	De brief van de korpschef inzake de internet consultatie met de werkgroep delen	5.1.2.e	
Buiten reikwijdte					

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

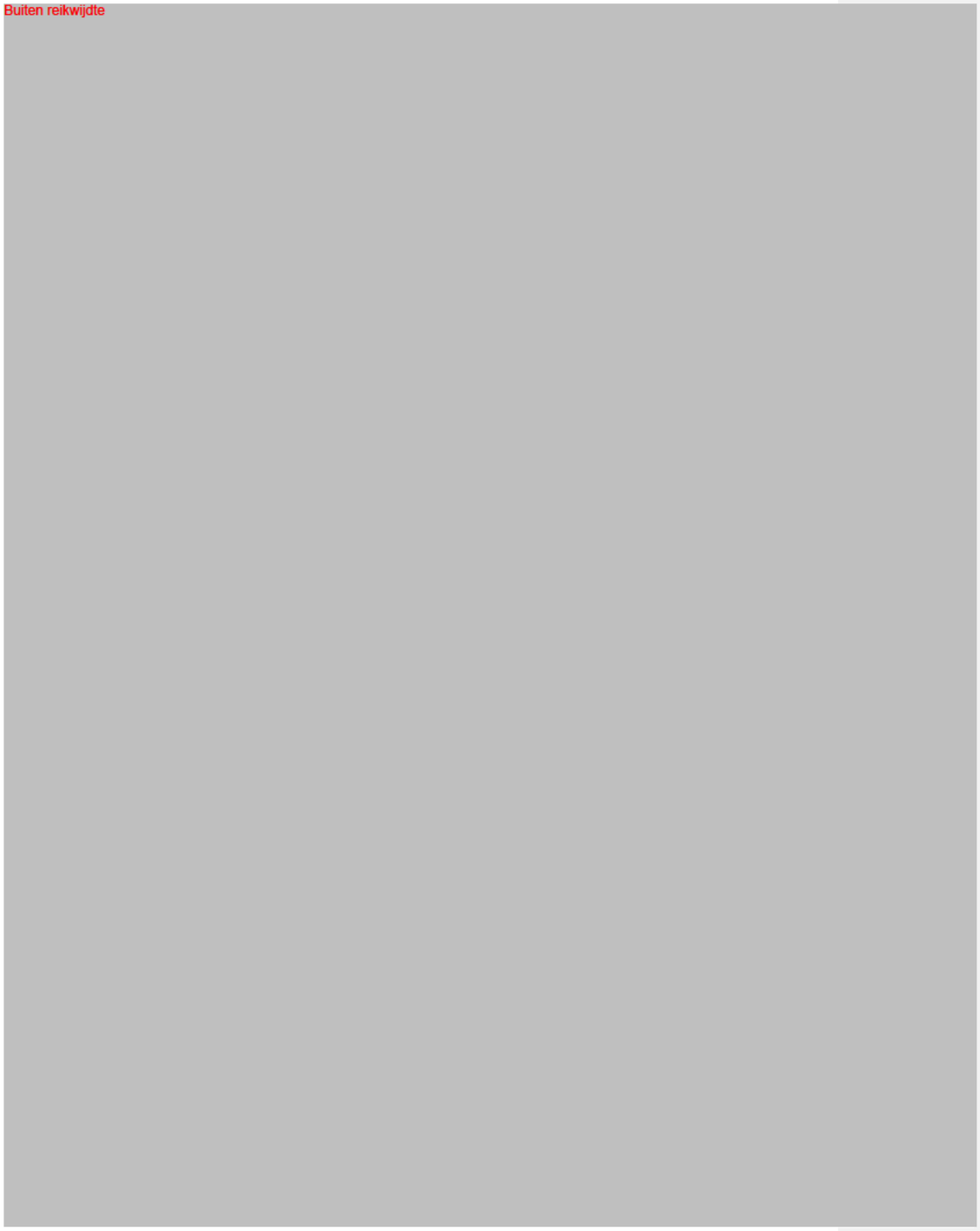
[redacted]

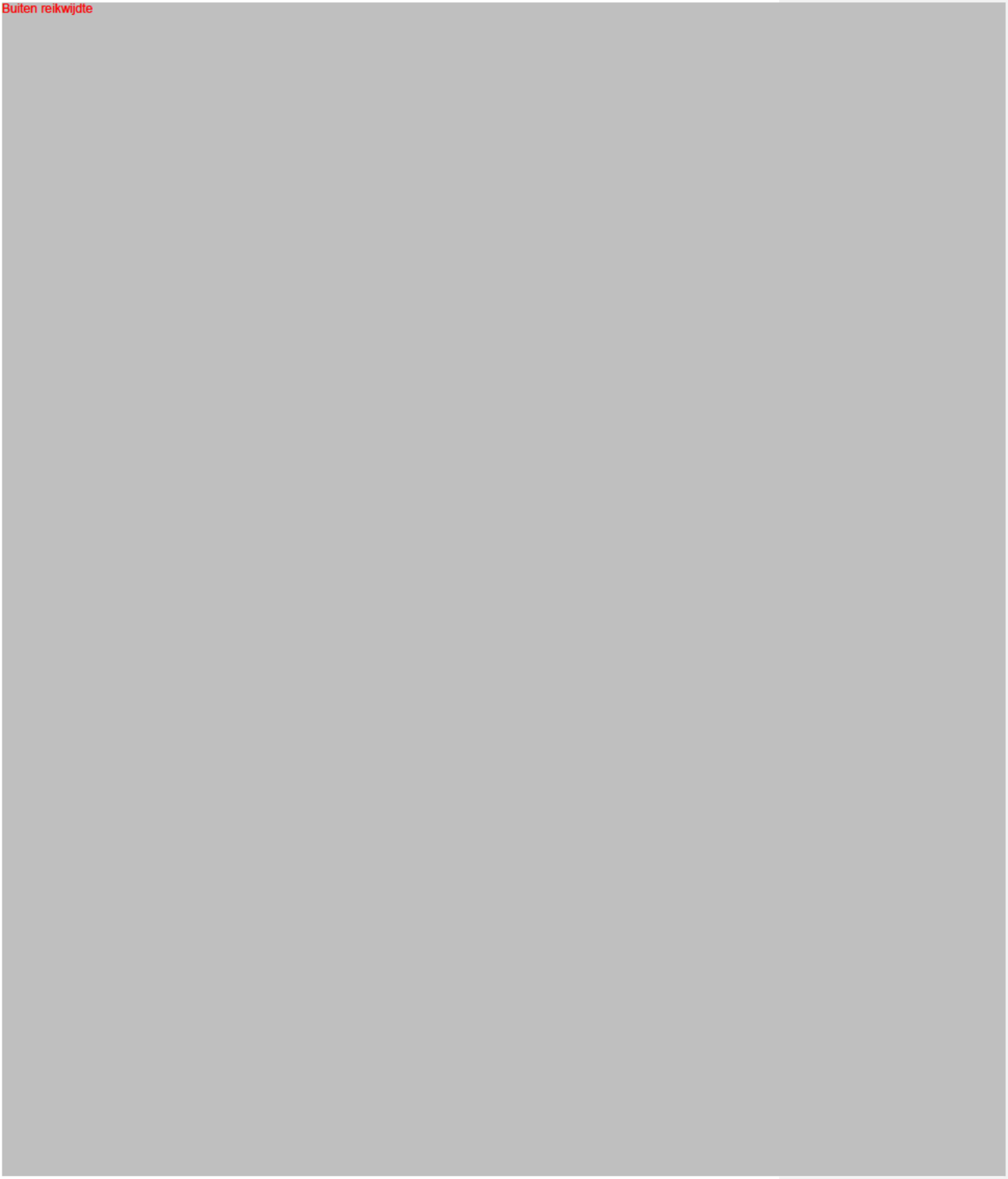
25-10-2021	#19 en #20	Filmen, hinderlijk volgen en observeren collega's	Nadere verkenning over de strafbaarheid van filmen, hinderlijk volgen en observeren van collega's. Bekijken welke maatregelen men in de verschillende situaties kan nemen.	Politie en JenV	

Met opmerkingen 5 1 2 e: Een overzicht van de rechtspraak al beschikbaar?

Buiten reikwijdte

[redacted]


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte

Werkgroep doxing politie en dgpenv

1. Kennismaken
2. Bepreken doel van deze werkgroep
3. Bespreken wat we willen oppakken in de werkgroep en hoe we dat willen aanpakken
   a. Actiepunten vanuit de WGRPBD relevant voor aanpak doxing en voorstel nadere actie

Preventie		WGRPBD	Werkgroep doxing
Buiten reikwijdte			
	aard en omvang probleem politieambtenaren die gevolgd en gefilmd etc worden en mogelijke maatregelen die al worden genomen door politie of zouden kunnen worden genomen.	verkenning politie en jenv	verkenning werkgroep doxing? - aard/omvang: voorbeelden ophalen binnen politie en bij vakbond? -inventarisatie mogelijke maatregelen -rond politiebureau -rond huis -elders

Buiten reikwijdte

Buiten reikwijdte

Repressie	Buiten reikwijdte		
	wetgevend kader filmen etc	Verkenning	werkgroep doxing? aanzet juridische analyse (5.1.2.e)?

Buiten reikwijdte

b. Voorstel: de werkgroep doxing ook laten kijken naar de volgende onderwerpen: wat gebeurt daar al dan niet op/ is het voldoende; en aparte vraag: kunnen we een en ander ook meenemen naar WGRPBD of juist niet:
   - politie intern beeld probleem van doxing (aard en omvang) samen met uitvraag filmen etc?

Met opmerkingen (5.1.2.e) niet eens, keep it smart!

Buiten reikwijdte

- ...

Mogelijk relevante actiepunten WGRPBD 25 oktober 2021

Primair relevant
Secundair relevant (vooralsnog)

Datum vergadering	Actie-punt	Onderwerp	Actie	Actie-houder	Gereed
Niet onder reikwijdte					
Niet onder reikwijdte					
Niet onder reikwijdte					

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte					
25-10-2021	#19 en #20	Filmen, hinderlijk volgen en observeren collega's	Nadere verkenning over de strafbaarheid van filmen, hinderlijk volgen en observeren van collega's. Bekijken welke maatregelen men in de verschillende situaties kan nemen.	Politie en JenV	
Niet onder reikwijdte					

Niet onder reikwijdte

Met opmerkingen 5.1.2.e **:** Een overzicht van de rechtspraak al beschikbaar?

Niet onder reikwijdte

Afspraken stellingname:			
1.	***Beschermen van de medewerker tegen fysieke vormen van agressie en geweld:***	-	
a.	[redacted]	[redacted]	Niet onder reikwijdte [redacted]
2.	***Beschermen van de medewerker tegen online agressie:***	-	
a.	Srafbaarstelling van het 'kale feit' doxing.	Consultatie afgerond.	Consultatie afgerond ; consultatieadviezen verwerken en dan naar RvS
b.	Onderzoek overige maatregelen om doxing en privacyinbreuken politieagenten tegen te gaan, waaronder gesprek met providers en tech-bedrijven.	Ideeen voor maatregelen bespreken met de bonden. Subwerkgroep cao doxing J&V en politie. Daarin wordt gekeken naar handelingskader en voorstellen bonden in de bijlage van de stellingname.	Vraag: Wie moet welk gesprek voeren providers en tech-bedrijven en waarover?

c.	Interne voorlichtingscampagne over veiligheidsrisico s aanwezig- en vindbaarheid op internet.	Stavaza politie?	Politie: loopt toch?
d.	Hinderlijk volgen politiecollega s (inclusief filmen/foto s) en observeren van politiebureaus tegengaan.	Wat willen de bonden hiermee?	Vraag : Van wie wordt actie gevraagd en welke actie?
3.	Buiten reikwijdte	-	
a.	Niet onder reikwijdte		
4.	Buiten reikwijdte	-	
a.	Niet onder reikwijdte		

Voorstellen bijlage stellingname; te toetsen/verkennen op proportionaliteit /wenselijkheid/ haalbaarheid/ uitvoerbaarheid:	-	-	
1.	***Maatregelen om diender te beschermen tegen 'kale doxing' (iedereen die zonder redelijk doel foto's/filmpjes plaatst):***	-	

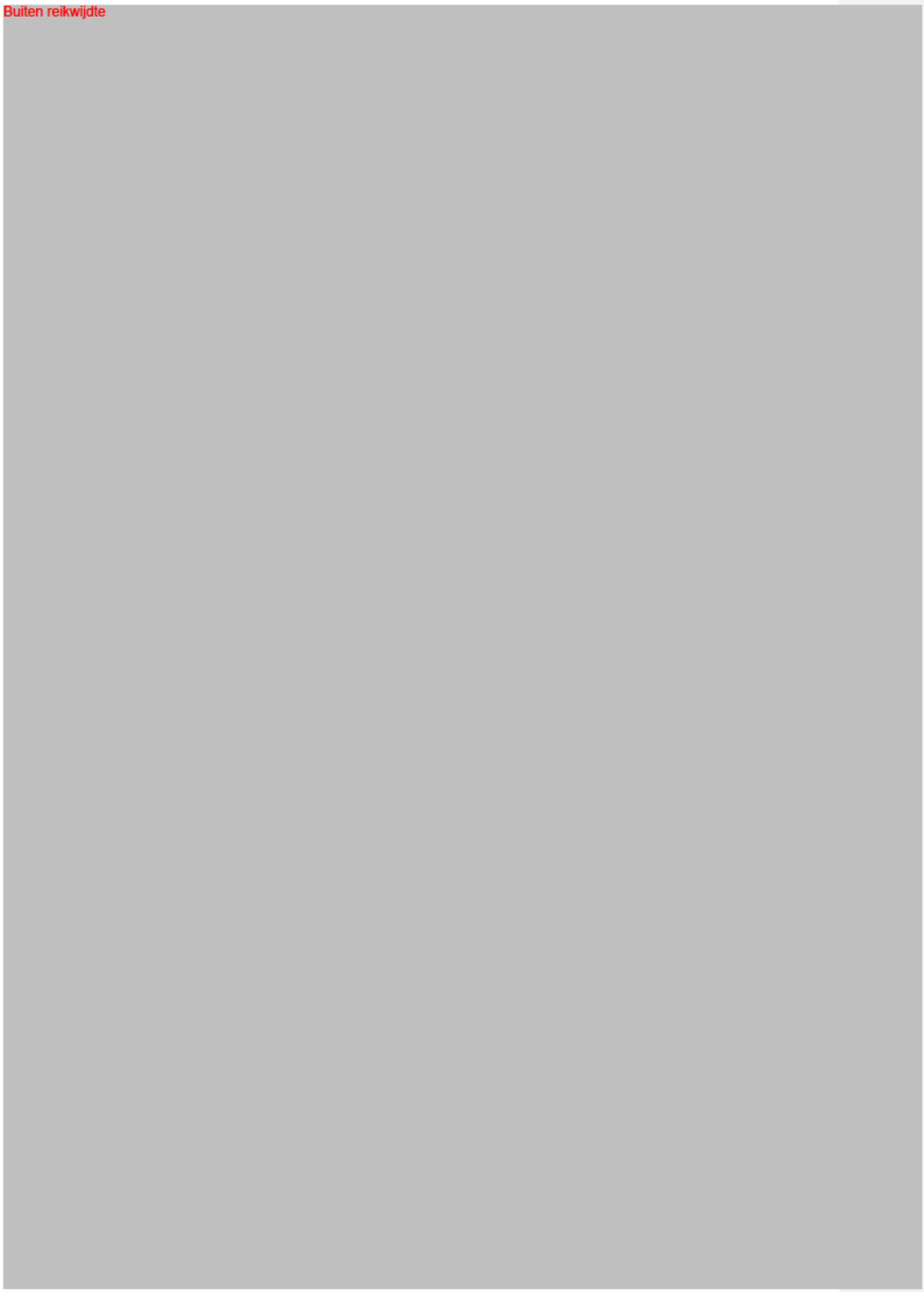
a.	Strafbaarstelling doxing		Zie onder punt 1 hierboven.
b.	Verplichting tot blurren van gezichten politiemensen op foto's en filmpjes sociale media.	WG Doxing?	Heroverweging standpunt wetgeving tov blurbrief 2017.Zie voorstel werkgroep onder punt 2 hierboven.
c.	Verwijderen van filmpjes en foto's speciale media door providers.	WG Doxing?	Op verzoek van politie als werkgever? Zie punt e hieronder. Mogelijk eerst te bespreken in voorgestelde subwerkgroep, zie punt 2 hierboven.
d.	Plaatsen van een waarschuwing dat informatie cq wat te zien is in filmpjes/foto's met duiding voorzien worden van: niet geverifieerde feiten.	Door politie of provider?	Door politie (commuicatie?)?
e.	Onderzoek naar inzetten wetgeving schenden privacy.	Wat bedoelen bonden hiermee? Wordt hiermee bedoeld inzet civiele recht door werkgever.	Wordt hier bedoeld inzetten door politie als werkgever? Mogelijk eerst bespreken in voorgestelde subwerkgroep, zie onder punt 2 hierboven.
f.	Collega's worden soms hinderlijk gevolgd waarbij ook opnamen worden gemaakt en geplaatst op sociale media. maatregelen om dit tegen te gaan.	Wat willen bonden hiermee?	Zie afspraak 2d. stellingname.
g.	Plaatsing foto's/filmpjes etc. alleen mogelijk als individu bekend is bij provider cq alleen op naam.	WG Doxing	Bespreken in voorgestelde subwerkgroep (relatie met petititie Gordon?)
2.	Buiten reikwijdte		
a.	Niet onder reikwijdte		

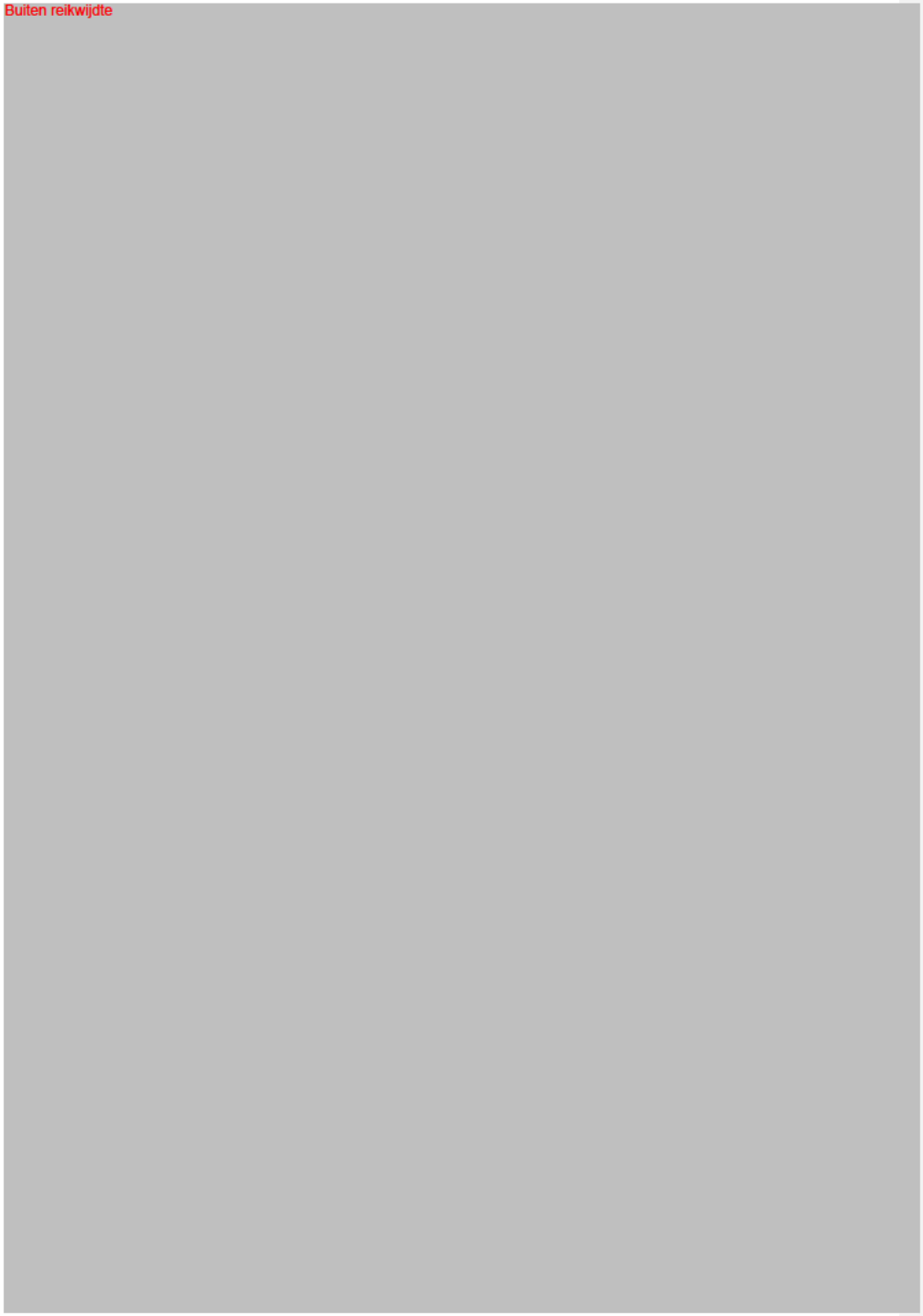
c.			Niet onder reikwijdte

h.	Niet onder reikwijdte		
3.	Buiten reikwijdte	-	
a.	Niet onder reikwijdte		
-	-	-	
-	-	-	
c.	Aanpak ontwikkelen om tegen te gaan dat politiebureaus in aantal steden worden geobserveerd om opnamen te kunnen maken van collega's en te achterhalen wie ze zijn etc.	Kan politie preventieve maatregelen nemen? Wat willen we precies?	Zie afspraak 2d stellingname. Is dit preventieve actie of de vraag naar een strafbaarstelling?
-	-	-	

d.			Niet onder reikwijdte
-	-	-	
-	-	-	
4.	Buiten reikwijdte	-	

a.	Niet onder reikwijdte		
-	-	-	
-	-	-	
c.	Na rechterlijke uitspraak verwijderen beeld en tekstmateriaal van internet en sociale media. Verdere verspreiding strafbaar stellen.	WG Doxing	Bespreken in voorgestelde werkgroep onder 2.


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte

DOXINGCASUISTIEK

Arnhem, april 2021:

Op last van de burgemeester wordt op Koningsdag een overvol stadspark ontruimd wegens het overtreden van de coronaregels. Onder de honderden aanwezigen zijn verschillende coronademonstranten die bewust de confrontatie met de politie zoeken en uit zijn op escalatie. Een politieagent gebruikt fysiek geweld tegen één van de demonstranten, terwijl een andere demonstrant alles filmt. 5.1.2.e [redacted] Er ontstaat een omvangrijke mediastorm die weken aanhoudt. De beelden worden meer dan een miljoen keer bekeken.

Er wordt – 5.1.2.e [redacted]

Doxing in deze casus is vanuit het demonstratiemilieu doelgericht ingezet als instrumenteel intimidatiemiddel. 5.1.2.e [redacted]

Doxing en intimidatie van de romeos, juli 2022:

Tijdens de omvangrijke Boerenprotesten van begin juli publiceert een bekende coronascepticus via twitter enkele foto's en een video van een lid van een aanhoudingseenheid, in de volksmond gekend als de ROMEOS. 5.1.2.e [redacted].

5.1.2.e [redacted]

5.1.2.e [redacted]. De opmars van doxing leeft onder deze eenheid en hindert hen sterk in de uitoefening van hun beroep en taakstelling. Er is geen sprake van een incident; doxing van de ROMEOS heeft zich tot een frequent toegepast intimidatiemiddel ontwikkeld in tijden van maatschappelijke onrust en rond demonstraties.

Schietincident Boerenprotest, juli 2022:

5.1.2.e [redacted]

5.1.2.e 5.1.2.e [redacted]

5.1.2.e [redacted]

De hevigheid van deze vorm van doxing, als vorm van collectieve actie tegen een individuele agent, zorgt voor handelingsverlegenheid en mijdgedrag onder politieagenten. De extreme gevolgen van doxing stralen hiermee verder uit dan 'slechts' geïsoleerde incidenten; het raakt directe collega's, naburige politiebureaus en de politie als institutie. Doxing zet daarnaast de kernwaarden van de politie als onder hoogspanning, want, in hoeverre willen agenten nog moedig zijn, of verbindend, als dit de gevolgen kunnen zijn?

5.2.1 [redacted]

Voorbeelden en casuïstiek

Blog april 2021
Zo ook in het Sonsbeekpark in Arnhem waar mijn collega's optraden. De filmpjes die nadien op social media verschenen lieten best heftige beelden zien. Maar zoals zo vaak, laten deze filmpjes niet altijd het hele verhaal zien. Er gaat altijd iets aan vooraf. Helaas wordt die context niet meegegeven.
Wat ik ronduit verafschuw en sterk veroordeel zijn foto's die op facebook en andere platforms verschenen waarop een van mijn collega's is te zien met woorden als 'fascist', 'nazi', 'NSB'er' en 'ramt graag kinderen in elkaar'. Daarbij wordt ook een oproep gedaan om zijn naam te achterhalen. Dit heeft niet alleen een enorme impact op hem en zijn familie, maar op alle collega's en hun gezinnen. Want zo raakt het werk opeens en ongewild hun persoonlijke levenssfeer. En besef daarbij dat mijn collega's in touw zijn voor ieders veiligheid.
In 2020 was er een toename van 86% van het aantal keren dat politiemensen op sociale media werden belaagd en bedreigd. Dit kan je niet los zien van het opzettelijk willen achterhalen van privégegevens met als doel intimidatie en bedreiging, ook wel doxing genoemd. Een ontwikkeling die niet alleen zorgelijk, maar ook volstrekt onacceptabel is.

Blauw (Personeelsblad politie) juni 2021, artikel Een prijs op je hoofd

Casus (nog bewerken)

(Tijdens doorzoeking bedrijf is foto net gezicht medewerker gemaakt. Deze foto is door een derde op internet geplaatst met vermelding van de tekst 'Undercover agent werkt bij eenheid xxxx' . Foto circuleert vervolgens onder criminele netwerken op het internet en diverse sociale media.)

Buiten reikwijdte

Buiten reikwijdte

Plaatsen filmpje en oproep namen en adressen, opruiing en belediging.
Na een aanhouding tijdens een demonstratie zijn privé-opnames van de aanhouding op internet geplaatst.
Op social media werden de persoonsgegevens van collega's opgevraagd. Het filmpje is zeer vaak gedeeld en kwam telkens terug in de (social) media, waarna opruiingen, beledigingen en bevragen naar adressen van de collegae bleven door gaan. Een medewerker werd privé in de winkel en tijdens haar werkzaamheden vaak aangesproken omdat zij herkend werd van het filmpje.
➔ Na strafrechtelijk onderzoek zijn 4 mensen veroordeeld en loopt nog een onderzoek naar andere personen.

Plaatsen privéadressen politieambtenaren op internet
Enkele politieagenten zijn de afgelopen tijd thuis bezocht nadat hun adressen door relschoppers online zijn gezet , 5 februari 2021
https://www.nu.nl/coronavirus/6114712/agenten-thuis-opgewacht-nadat-relschoppers-adressen-online-plaatsen.html

Er is 500 euro op mijn hoofd gezet'
Demonstranten maken er sinds de corona-uitbraak een sport van om leden van een Aanhoudingseenheid (AE), Romeo's in de volksmond, te herkennen en ontmaskeren. 'Een zorgwekkende ontwikkeling. Ik heb gehoord dat er een foto van mij en mijn collega's rondgaat in bepaalde groepen op Telegram. Mensen bieden 500 euro om mijn gegevens te achterhalen', commandant bij de AE in Amsterdam.

Doxing
Afgelopen week hoort Dennis dat een foto van zijn eenheid rondgaat op Telegram en er wordt gevraagd om privégegevens. Er wordt 500 euro uitgeloofd voor de informatie. ‘Dan schrik je toch wel even. De video van de op het eerste oog onschuldige vrouw is blijkbaar veelvuldig op Facebook gedeeld en zo ook opgepakt door een extreme groepering. Ik heb in het verleden al vaker op het internet gestaan. Toen was het meer ‘’let op dit is een stille’’ en werd geen geld uitgeloofd voor mijn gegevens. Dit is anders.’

5.1.2.i

"Vanmiddag werd in het Opsporings Afstemmingsoverleg (OAO) gevraagd om indien bekend casussente mailen waarbij alleen sprake is van Doxing, zonder een gronddelict.

In Leiden heeft onlangs de volgende casus gespeeld die wij als DR hebben overgenomen van basisteam Leiden Midden.
In de stad Leiden hingen een aantal posters met daarop een foto van een collega, 5.1.2.e

Op zich geen strafbaar feit, maar wel erg vervelend en toch enigszins bedreigend (niet in strafrechtelijke zin) voor de collega. Ook betrof het feitelijk geen smaad.
Door de forensische opsporing zijn de posters onderzocht en hier kwam uit vingerafdrukken een verdachte naar voren die eerder door collega 5.1.2.e was aangehouden en die proces-verbaal tegen hem had opgemaakt.

Met de officier van justitie is toen 5.2.1 buiten heterdaad aan te houden als verdacht van ambtsdwang, artikel 179SR.

“Hij die door geweld of enige andere feitelijkheid of bedreiging met geweld of enige andere feitelijkheid een ambtenaar dwingt tot het volvoeren van een ambtsverrichting of het nalaten van een rechtmatige ambtsverrichting,
wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.”

5.1.2.e . 5.2.1

De verdachte werd aangehouden, er werd een stevig woordje met hem gesproken (5.1.2.e) en daarna werd de verdachte heengezonden.
De zaak werd geseponeerd, omdat Doxing geen strafbaar feit op zich betreft en er verder geen sprake was van een verdenking voor een ander strafbaar feit.

We hebben dus eigenlijk geen middelen om Doxing alleen aan te pakken. 5.2.1

Zo meldde de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in het Dreigingsbeeld Terrorime Nederland, dat ieder kwartaal gepubliceerd wordt, dat boosheid en ongenoegen over de coronamaatregelen onder meer leiden tot doxing door activisten die persoonsgegevens van mensen die werken bij de politie en politici online zetten, als intimidatietactiek (Von Piekartz, 2020) In januari 2021 zijn de gegevens van tientallen undercoveragenten (zogenoemde ‘romeo’s’) gedoxed, en na de avondklokrellen is de online jacht op hen opgevoerd via Telegram- en Facebookgroepen, meldde de Volkskrant (Von Piekartz & Bahara, 2021). De Facebookgroep Steungroep Boeren en Burgers, die 165.000 leden telt, zette doxing in als intimidatiemiddel door te dreigen met de publicatie van gegevens van tientallen romeo’s (Von Piekartz & Bahara, 2021). In radicaal-rechtse Telegramgroepen, zoals De Bataafse Republiek (5.000 leden), gaat ook al een tijd een lijst rond met huisadressen van ‘linkse’ journalisten en ministers, soms met de oproep om een ‘burgerwacht’ te vormen die de genoemde personen ‘geweldloos op non-actief kan stellen’ (Von Piekartz & Bahara, 2021). En in maart 2020

kregen Twitteraars bij hun voordeur stikkers geplakt van Vizier op Links, een anoniem account met circa 16.000 volgers, dat linkse opiniemakers, activisten en politici het leven probeert onmogelijk te maken.
In de pers komen ook voorbeelden uit de VS langs, zoals het Twitteraccount @YesYoureRacist ('ja, je bent racist'), dat de identiteit van racisten probeert te achterhalen. Toen in augustus 2017 via dit account werd opgeroepen tot hulp bij het opsporen van de betogers in Charlottesville, groeide het aantal volgers binnen een paar dagen van 65.000 naar bijna 400.000 (van Houwelingen, 2017). Dit geeft een indicatie van hoe snel het fenomeen kan groeien.

https://www.binnenlandsbestuur.nl/digitaal/honderden-adressen-bestuurders-openbaar?tid=TIDP2044173X22153319804C4EC5BEB817EACB9C7B17YI5&utm_campaign=BB_NB_Digitaal&utm_medium=email&utm_source=binnenlandsbestuur

	Onderwerp:	Stand van zaken:	Actie(houder):	Planning:	Gereed
Afspraken stellingname:					
1.	***Beschermen van de medewerker tegen fysieke vormen van agressie en geweld:***				
a.	Buiten reikwijdte				
2.	***Beschermen van de medewerker tegen online agressie:***				
a.	Srafbaarstelling van het 'kale feit' doxing.	Consultatie afgerond ; consultatieadviezen verwerken en dan naar RvS	J&V- 5.1.2.e DWJZ en 5.1.2.e DGRR en 5.1.2.e (DGPenV) (wetsvoorstel)	Voor 2022 wetsvoortel naar TK.	
b.	Onderzoek overige maatregelen om doxing en privacyinbreuken politieagenten tegen te gaan, waaronder gesprek met providers en tech-bedrijven.	Politie heeft gesprekken gevoerd met providers over ? (navragen bij 5.1.2.e) online evil	5.2.1		
c.	Interne voorlichtingscampagne over veiligheidsrisico's aanwezig- en vindbaarheid op internet.		Politie		
d.	Hinderlijk volgen politiecollega's (inclusief filmen/foto's) en observeren van politiebureaus tegengaan.		Politie		
3.	Buiten reikwijdte				
a.	Buiten reikwijdte	Buiten reikwijdte	Buiten		
4.	Buiten reikwijdte				

a.	Buiten reikwijdte		Buite		
Voorstellen bijlage stellingname: te toetsen/verkennen op proportionaliteit /wenselijkheid/ haalbaarheid/ uitvoerbaarheid:					
1.	***Maatregelen om diender te beschermen tegen 'kale doxing' (iedereen die zonder redelijk doel foto's/filmpjes plaatst):***				
a.	Strafbaarstelling doxing	Zie onder punt 1 hierboven.	JenV		
b.	Verplichting tot blurren van gezichten politiemensen op foto's en filmpjes sociale media.	Zie voorstel werkgroep onder punt 2 hierboven.	JenV en poliitie		
c.	Verwijderen van filmpjes en foto's speciale media door providers.	Op verzoek van politie als werkgever? Zie punt e hieronder. Mogelijk eerst te bespreken in voorgestelde subwerkgroep, zie	JenV en politie		
d.	Plaatsen van een waarschuwing dat informatie cq wat te zien is in filmpjes/foto's met duiding voorzien worden van: niet geverifieerde feiten.	Door politie?			
e.	Onderzoek naar inzetten wetgeving schenden privacy.	politie als werkgever? Mogelijk eerst bespreken in voorgestelde subwerkgroep, zie onder punt 2	JenV.Mogelijk 5.1.2.e (Taskforce onze hulpverleners veilig)		
f.	Collega's worden soms hinderlijk gevolgd waarbij ook opnamen worden gemaakt en geplaatst op sociale media. maatregelen om dit tegen te gaan.	Zie afspraak 1d. stellingname.	Politie		
g.	Plaatsing foto's/filmpjes etc. alleen mogelijk als individu bekend is bij provider cq alleen op naam.	Vraag nemen zodra reactie komt op petitie 5.1.2.e 5.1. heeft bij ontvangst petitie aangegeven dat voor volgend kabinet is. Bespreken in voorgestelde subwerkgroep?	JenV en politie.		

2.	Buiten reikwijdte				
a.	Buiten reikwijdte				
b.	Buiten reikwijdte	Buiten reikwijdte			
c.	Buiten reikwijdte	Buiten reikwijdte			
d.	Buiten reikwijdte	Buiten reikwijdte			
e.	Buiten reikwijdte				
f.	Buiten reikwijdte				
g.	Buiten reikwijdte	Buiten reikwijdte			

h.	Buiten reikwijdte	Buiten reikwijdte			
3.	Buiten reikwijdte				
a.	Buiten reikwijdte	Buiten reikwijdte			
b.	Buiten reikwijdte	Buiten reikwijdte	Buiten		
c.	Buiten reikwijdte	Buiten reikwijdte	Buite		
d.	Buiten reikwijdte		Buiten		
e.	Buiten reikwijdte	Buiten reikwijdte	Buit		
f.	Buiten reikwijdte	Buiten reikwijdte	Buit		
4.	Buiten reikwijdte				
a.	Buiten reikwijdte	Buiten reikwijdte	Bu		

b.	Buiten reikwijdte		Buite		
c.	Na rechterlijke uitspraak verwijderen beeld en tekstmateriaal van internet en sociale media. Verdere verspreiding strafbaar stellen.	Bespreken in voorgestelde werkgroep onder 2.	JenV en politie		

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 21 juni 2021 16:57
Aan: 5.1.2.e
Onderwerp: RE: juiste versie

Zie een paar opmerkingen en suggesties.

Van: 5.1.2.e
Verzonden: maandag 21 juni 2021 16:44
Aan: 5.1.2.e <5.1.2.e @politie.nl>
Onderwerp: juiste versie

Met vriendelijke groet,

5.1.2.e
juridisch adviseur

Politie | Korpsstaf | Bestuursondersteuning | Juridische Zaken en Project modernisering WvSv

behalve de 5.1.2.e
M 06 5.1.2.e | E: 5.1.2.e @politie.nl | **Postbus 17107, 2502 CC Den Haag**

Over het Project modernisering WvSv: zie **Agora**

Van: 5.1.2.e
Verzonden: maandag 21 juni 2021 16:33
Aan: 5.1.2.e <5.1.2.e politie.nl>
Onderwerp: 6-ogen nog even? andere 2 waren 5.1.2.e, maar ik hecht toch nu wel aan 6

5.1.2.e blijft toch te gaan voor mail namens pfh Peije, en 5.1.2.e is namens Peije okay
OM heeft geen brief gestuurd. Heb met 5.1.2.e nog over hun invalshoek gesproken

---

Met belangstelling heeft de politie kennis genomen van het ontwerpwetsvoorstel strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden. U heeft ons gelet op de hoge spoedeisendheid in de gelegenheid gesteld om binnen enkele dagen nog een reactie in te brengen. Binnen de gegeven context wordt graag aan dit verzoek voldaan.

Algemeen
Bij eerste lezing kan worden vastgesteld dat in het voorstel en de ontwerptoelichting aansluiting wordt gezocht ~~zoekt~~ bij het recent door de korpschef aan u gedane voorstel de strafbaarstelling van 'kale doxing' te onderzoeken, in het bijzonder in verband met de toenemende, ingrijpende ervaringen van politiemedewerkers bij dit fenomeen en de gevolgen voor henzelf en gezinsleden in de privésfeer van de woon- en leefomgeving.

1. Privésfeer
Het voorstel kent in beginsel gelet op de aard van de gedragingen een brede reikwijdte van de strafbaarstelling, waarbij vanuit de maatschappelijke ontwikkelingen terecht ook aandacht is voor slachtoffers die los van ambt of professie met deze gedragingen worden geconfronteerd.

Uiteraard kunnen de strafbare gedragingen tot gevolg hebben dat bijvoorbeeld binnen de politie de medewerker zijn reguliere activiteiten of werkzaamheden in zijn of haar functie tijdelijk of blijvend niet meer ongestoord kan voortzetten. De toelichting vermeldt daartoe als voorbeeld al het werken onder dekmantel en de aanhoudingseenheden, waarbij medewerkers 'dienst doen in burger'. Een door doxing veroorzaakte onveiligheid voor de betreffende medewerker en de in die gevallen noodgedwongen wijziging van werkzaamheden heeft zowel voor de medewerker als de organisatie grote gevolgen.

Met instemming wordt geconstateerd dat het voor een strafbaarstelling al voldoende dient te zijn, dat in het algemeen de gedraging geschikt en geëigend zou zijn om een bepaalde opstelling teweeg te brengen. Feit is dat in de praktijk de aangejaagde vrees ernstige impact heeft op het slachtoffer en zijn omgeving. Dit kan ook over langere tijd aanhouden en weer opleven, indien de door doxing verspreide gegevens door hernieuwde aandacht (zoals via social media) met de vrees en ernstige overlast inbreuk maakt op de privésfeer van bijvoorbeeld ~~de~~ politieagenten en hun gezinsleden. 5.2.1

De politie geeft u in overweging in de toelichting nader te verduidelijken dat ook voor personen die een ambt of functie vervullen met een publieke taak geldt dat de handelingen die als doxing zijn te duiden zich tot heden vooral lijken richten op het vrees aanjagen en ernstige hinder veroorzaken in hun privésituatie en - niet in de laatste plaats - dat van hun gezinsleden.

De politie gaat er overigens daarbij van uit dat ook voor de strafbaarstelling van doxing de bestaande strafvorderingsrichtlijnen en landelijke afspraken ten aanzien van de opsporing en vervolging conform het beleid Veilige Publieke Taak van toepassing wordt, met bij vervolging een verhoogde strafeis conform de zogeheten ELA/VPT.

2. Online en offline
Het voorstel richt zich vooral op handelingen die zich langs de lijnen van publiek toegankelijke bronnen en social media voordoen. Het advies is ook aandacht te bieden [5.2.1 aan gevallen waarin dit handelen in de fysieke wereld zich voordoen, bijvoorbeeld bij en rond manifestaties met grote groepen personen, waar personen met een ambt of functie met een publieke taak werkzaam zijn.

3. Strafwaardigheid
In de toelichting wordt vanuit diverse invalshoeken kort beschreven ~~ingegaan~~ op de verwerpelijkheid en strafwaardigheid van de strafbaar te stellen handelingen. 5.2.1 Het advies is de strafwaardigheid van de handelingen nader toe te lichten. Daarbij kan worden ingegaan op de ernst van de impact op slachtoffers van doxers nader te duiden, zoals die zich ook manifesteren in vergelijkbare situaties bij slachtoffers van thans wel strafbare handelingen zoals bedreiging en belaging etc.

4. Voorwaardelijk opzet
In de voorgestelde delictsomschrijving wordt aangesloten bij het delict belaging, waarbij de opzetvariant van het oogmerk centraal staat 5.2.1]. Het uitgangspunt is dat voor de strafwaardigheid geen afhankelijkheid bestaat van het daadwerkelijk intreden van gevolgen bij slachtoffers. Anderzijds is de vraag of hiermee niet gevallen van zogeheten voorwaardelijk opzet van strafbaarstelling worden uitgesloten. Het verzoek is aan dit aspect bij uw nadere overweging aandacht te geven

5. Strafbaarstelling en (politie)optreden richting derden
Voor de handhaafbaarheid van het delict wordt terecht aandacht gegeven aan de noodzakelijke strafvorderlijke bevoegdheden om te komen tot allereerst de identificatie van de verdachte van doxing zelf. Tegelijkertijd wordt ook aandacht besteed aan de mogelijke effecten van de voorgestelde strafbaarstelling voor het instrument van de vordering tot het verwijderen of ontoegankelijk maken bij derden, zoals verantwoordelijken van platforms waarop de verdachte van doxing zijn handelingen verricht. Hoewel een strafbaarstelling van doxing ook aan die verwijdering een bijdrage zal kunnen bieden, kan niet op voorhand al een thans gegarandeerde toename van effectieve verwijderingen worden geduid.

6. Wettelijke terminologie
Het advies is in de toelichting nader in te gaan op de reikwijdte van een aantal wettelijke termen. Voor identificerende persoonsgegevens rijst in deze context de vraag of ook een foto daartoe kan behoren. Ook de termen van het 'zich verschaffen', 'vergaren' en 'verspreiden' kunnen de vraag oproepen of de nu optredende casuïstiek binnen de reikwijdte van de voorgestelde delictsbepaling vallen.

Valt daaronder het plaatsen van een bericht op social media in een groepsbericht rondom een voortijdig beëindigde demonstratie *'wie weet waar de wijkagent woont'*? En is dit ook het geval indien een herkenbare foto van een politiemedewerker in uniform - of in burger, maar dan met connotatie politie - in een groepsapp op WhatsApp met de zin *'wie weet waar deze man woont*? Of als op Telegram een foto plaatsen en '*biedt € 500, - voor wie zijn gegevens achterhaalt'.* Ook het oproepen om persoonsgegevens te verstrekken of openbaar te maken zonder dat betrokkene het zich feitelijk doet toekomen, lijkt in de voorgestelde bepaling niet onder de strafbaarstelling te vallen.

De politie dient vanuit de politiepraktijk te werken met een duidelijke en daarmee handhaafbare strafbepaling. Duidelijk moet tegelijk zijn dat de nieuwe aanvullende strafbaarstelling de nu zich voordoende ook ernstige gevallen alsnog binnen de reikwijdte van het Wetboek van Strafrecht brengen.

7 Uitvoeringseffecten
Anders dan in de tekst is opgenomen, is ondanks het gegeven dat het een nieuwe strafbaarstelling is te voorzien dat het aantal personen dat aangifte wil doen van deze delicten naar verwachting in omvang zal toenemen, en dat voor de politie daaruit structurele uitvoeringslasten uit zullen voortvloeien om deze aangiften strafrechtelijk te onderzoeken. Momenteel wordt binnen de politie in kaart gebracht of deze gedurende de komende consultatiefase voldoende concreet gekwantificeerd al in kaart kunnen worden gebracht. Mogelijk dat in een later stadium na invoering dit zal moeten worden herijkt.

Tot slot zijn er nog enkele tekstuele suggesties, die afzonderlijk aan uw departement zijn doorgegeven.

Afrondend
Het eerdere verzoek aan u was om de strafbaarstelling van kale doxing te onderzoeken. Nu ligt er op korte termijn een ontwerpwetsvoorstel. De politie is instemmend ten aanzien van de uitgangspunten van dit wetsvoorstel. Het advies is vanuit de invalshoek van de uitvoeringspraktijk bij de politie aandacht voor het bovenstaande en de uitkomsten van de komende maanden nog te houden impactanalyse.

Met vriendelijke groet,

5.1.2.e
juridisch adviseur

Politie | Korpsstaf | Bestuursondersteuning | Juridische Zaken en Project modernisering WvSv

behalve de 5.1.2.e
M 06 5.1.2.e | E: 5.1.2.e @politie.nl | **Postbus 17107, 2502 CC Den Haag**

Over het Project modernisering WvSv: zie **Agora**

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 14 september 2021 13:00
Aan: 5.1.2.e
Onderwerp: 20210913 Consultatiereactie politie doxing 5.1.2.e .docx
Bijlagen: 20210913 Consultatiereactie politie doxing 5.1.2.e .docx

Bel me als mijn suggesties niet duidelijk zijn!

versie 14 april 2021

Format Tekenstuk Korpsleiding

stukken in juiste huisstijl[1] in hard copy aanleveren bij MA van lid KL dat moet ondertekenen

Algemene informatie

Steller (contact- en afdelingsgegevens)	5.1 2 e (TJZ) mede namens 5.1.2.e (DO programma VPT) en Bureau BIA (impactanalyse) en via de portefeuilles met input van experts uit diverse operationele teams uit GGP, Cybercrime, TDO's, alsook Directie HRM.
Onderwerp	Reactie consultatie op Wetsvoorstel Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden (**doxing**)
Betreft	☑ Brief ☐ Overeenkomst ☐ Besluit ☐ Advies ☐ Verzoek ☐ Anders, nl …
Doel ondertekening	Standpunt politie op wetsvoorstel doxing aan Minister overbrengen.
Lid KL dat ondertekent (eindverantwoordelijke)	☑ Van Essen ☐ Huyzer ☐ Kok ☐ Geveke ☐ Ekelmans
Bijlagen	☑ Ja, [aantal en beschrijving] 1. Eerdere brief aan de Minister van 6 april 2021
Reactie op inkomende brief / mail	☑ Ja, kopie bijgevoegd ☐ Nee
Kenmerk brief[2] / mail	2021-0053287
Beschrijving inhoud	Het betreft een formele consultatiereactie op een ontwerp wetsvoorstel dat een ernstige vorm van het fenomeen doxing strafbaar stelt, naast bestaande delicten als bedreiging, belaging, opruiing, belediging etc. **Initiatieven politie.** De politie - langs de lijn van het programma VPT - heeft zich al langere tijd in vele gremia sterk gemaakt om doxing van in ieder geval politieambtenaren strafbaar te stellen. Dit resulteerde ook in een formeel pleidooi op 6 april jl. Tijdens de behandeling van een andere wetsvoorstel Versterking strafrechtelijke aanpak ondermijnende criminaliteit zegde de Minister in reactie toe versneld met een consultatiewetsvoorstel te komen. Daarop is namens de portefeuille in de informele fase eind juni jl. input gegeven. **Kern** van het wetsvoorstel is reeds het in brede zin oproepen en delen van privégegevens met het oogmerk vrees aan te jagen / ernstige hinder te genereren / werk te belemmeren strafbaar te stellen **Extra gereedschap**. Het strafrechtelijk bewijs zal nog steeds vooral in de concrete *context* moeten worden verzameld. Inzet van bob-middelen om überhaupt te kunnen *identificeren*, stopgesprekken te kunnen houden en waar nodig stevig strafrechtelijk te kunnen doorpakken. **Bescherming personeel**. De inbreng sluit aan bij de in de bijlage van het *Arbeidsvoorwaardenakkoord sector politie 2021* (CGOP 31-5-2021 docnr.: CGOPAVA/21.00615.1) opgenomen maatregelen ter verdere bescherming van onze collega's in hun werk, te weten te laten onderzoeken doxing tegen te gaan, waaronder strafbaarstelling van het 'kale feit' doxing als bloot rechtsfeit (zonder redelijk doel openbaar maken van NAW-gegevens van politieambtenaar). Op **inhoud** worden vanuit de politiepraktijk voor een werkbare wet enkele ingebrachte suggesties meegegeven, en er kan in helderheid in de toelichting van de strafbepaling nog worden verduidelijkt. De hoofdlijn van dit concept is echter **positief**.
Toelichting	--
Financiële dekking	☑ Tijdens de zomerperiode heeft Bureau Impact analyse (DO) en JZ samen met OM en politieexperts een **Rapport Impactanalyse** opgesteld, met DGPenV is gedeeld en voor afzonderlijk vervolgtraject afgestemd. De impact zal in een integraal ambtelijk overleg met JenV en OM adhv een 3-tal scenario's (vervanging of ook voorziene uitbreiding?) worden geconcretiseerd.
	☐ Paraaf budgethouder [naam en functie]

[1] Juiste huisstsijl betekent: standaard format (te vinden in de WORD sjablonen), incl. volledig ingevulde linker kolom.
[2] Briefnummer op te vragen bij divknp@knp.politie.nl

Format Tekenstuk Korpsleiding

Reden ondertekening incl. omschrijving mandaat	Gezien de betrokkenheid van de korpschef bij het onderwerp en het belang en de impact van dit wetsvoorstel ligt het voor de hand dat de korpschef zelf reageert.
Deadline ondertekening	16 september 2021
Na ondertekening retour aan	☑ Steller ☐ Anders, nl. …

Instemmings- & afstemmingstraject

(alle kolommen invullen)	**directie / portefeuille / eenheid**[3]	**naam**	**akkoord + datum + opmerking**
Directeur Korpsstaf - JZ e/o BO e/o VIK	…	…	☐ **Ja**, [datum] …
Stafdirecteur	HRM	5.1.2.e	☑ **Ja**, ivm bijlage cao 14 september 2021
Themahouder	Geweld	Peije de Meij	☑ **Ja**, iam progr VPT 14 september 2021
Politiechef/pfh	Crisisbeheersing	Frank Pauw	☑ **Ja**, 15 september 2021
Akkoord lid / leden KL	☑ Van Essen	☐ Huyzer	☐ Kok ☐ Geveke ☐ Ekelmans

Verzending

☑ per post	Uitgaande brief fysiek aanleveren bij Team DIV
☑ per e-mail	Uitgaande brief in BCC aan 5.1.2.i @knp.politie.nl
☐ n.v.t.	…

Invullen door DIV

verzonden datum	…
checklist retour aan	…

[3] Indien meerdere directies, portefeuilles of politiechefs zijn betrokken: voor elke betrokkene een aparte regel in voeren. Dat kan als volgt: (1) selecteer de regel; (2) [Ctr]+[c]; (3) [Ctrl]+[v].

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)

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

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het wenselijk is het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens voor intimiderende doeleinden strafbaar te stellen;
Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

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

Artikel 285d

Hij die zich identificerende persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk om die ander vrees aan te jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel hem door anderen vrees aan te laten jagen, ernstige overlast aan te laten doen of in de uitoefening van zijn ambt of beroep ernstig te laten hinderen, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

ARTIKEL II

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

Artikel 298b

Hij die zich identificerende persoonsgegevens van een ander of een derde

- verschaft,
- deze gegevens verspreidt of anderszins ter beschikking stelt
- met het oogmerk om die ander vrees aan te jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel hem door anderen vrees aan te laten jagen, ernstige overlast aan te laten doen of in de uitoefening van zijn ambt of beroep ernstig te laten hinderen,

wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

ARTIKEL III

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

ARTIKEL IV

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

ARTIKEL V

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

Gegeven

De Minister van Justitie en Veiligheid,

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 gebruik van internet, sociale media en smartphones biedt de mogelijkheid tot het (al dan niet deels) online benaderen van andere personen. Dit kan resulteren in gedragingen die door die andere personen als zodanig intimiderend worden ervaren, dat deze gedragingen in de maatschappij als zeer onwenselijk en strafwaardig worden gezien.

Eén van deze onwenselijke en strafwaardige gedragingen is doxing (ook wel: *doxxing*). Hierbij worden identificerende persoonsgegevens samen- en/of naar buiten gebracht 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 waarvan verondersteld wordt dat zij daartoe behoren, of op de organisatie waarvoor zij werkzaam zijn. Het gevolg daarvan 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 handelwijzen aan te passen. Het ontregelende karakter van doxing heeft op die manier, direct of indirect, invloed op het functioneren van onze democratische rechtsstaat en de instituties die daarvan deel uitmaken.

Tegen deze achtergrond wordt voorgesteld doxing strafbaar te stellen. Hiermee wordt een duidelijk signaal afgegeven dat doxing onacceptabel is, en dat strafrechtelijk optreden aangewezen is.

2. Doxing

Op internet zijn allerlei persoonsgegevens te vinden. Deze gegevens zijn door personen prijs gegeven in contacten met instanties of leveranciers van goederen en diensten. Daarnaast geven veel personen via sociale media direct of indirect veel identificerende persoonsgegevens prijs. Die openheid van het internet biedt kwaadwillenden de mogelijkheid om deze persoonsgegevens te gebruiken om mensen online vrees aan te jagen, te intimideren en te bedreigen. Het begrip 'doxing' is een term die wordt gebruikt door hackers en is afgeleid van het Engelse woord 'documents'. Het houdt in dat identificerende persoonsgegevens worden vergaard om die gegevens vervolgens in te zetten om personen die om ideologische of andere motieven als 'de vijand' of als 'anders' worden beschouwd vrees aan te (laten) jagen of te (laten) belemmeren in hun doen en laten.

Doxing omvat een veelvoud van gedragingen die als strafwaardig, onrechtmatig en zeer ongewenst kunnen worden gekwalificeerd. Het is betrekkelijk eenvoudig om via *open source* bronnen persoonlijke informatie van individuele personen te achterhalen. Enige basiskennis van het internet volstaat om via een zoekopdracht identificerende persoonsgegevens boven water te krijgen. Bovendien zijn er ook veel overheidssites, zoals die van de Kamer van Koophandel, die – weliswaar voor een volstrekt ander doel – dergelijke gegevens beschikbaar stellen. Het slachtofferschap is bij doxing dan ook niet voorbehouden aan bepaalde groepen: een ieder kan ermee te maken krijgen. Dat is ook de reden waarom het onderhavige wetsvoorstel zich niet op een bepaalde (beroeps)groep richt: het stelt een duidelijke norm dat doxing, zoals omschreven in dit wetsvoorstel, maatschappelijk onaanvaardbaar is en als misdrijf wordt beschouwd.

Met opmerkingen [s12] (1): 5.2.1

Doxing kan grote schadelijke effecten hebben op het persoonlijke leven van slachtoffers. In de eerste plaats wordt door middel van doxing de online wereld verbonden met de fysieke wereld, in het bijzonder de fysieke persoonlijke levenssfeer. Bij velen leidt het wegvallen van het onderscheid tussen hetgeen virtueel en in het dagelijks leven plaatsvindt, al dan niet in combinatie met het wegvallen van het onderscheid tussen werk en privé, tot een gevoel van onveiligheid. 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 troetelnaampjes voor 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. "Dat komt wel even binnen," verklaarde een politieagent die online is bedreigd en kort daarvoor had geassisteerd bij het ontmantelen van een

drugslaboratorium in het Korpsblad. "Als die dreiging van zo'n drugsbaas zou uitgaan, dan is dat op z'n minst gezegd spannend."

In de tweede plaats leidt doxing vaak tot anonieme, collectieve en gecoördineerde acties richting het slachtoffer, louter om het feit dat het slachtoffer behoort tot een bepaalde (beroeps)groep. In situaties waarbij de werkomgeving van het slachtoffer gevaar met zich brengt, kan dit het persoonlijke leven van het slachtoffer raken 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. Het zou dan bijvoorbeeld kunnen gaan om een advocaat die als individu wordt aangesproken op het juridisch bijstaan van een bepaalde verdachte, een gemeenteraadslid dat wordt aangesproken op besluiten van een gemeenteraad als geheel of iemand met een Joodse achtergrond die wordt aangesproken op het beleid van de staat Israël. Het maakt dat doxing onvoorspelbaar en ongrijpbaar is.

In de derde plaats treft doxing niet alleen de slachtoffers zelf, maar ook de personen in hun directe omgeving. Daardoor is het voor hen vaak lastig om het risico in te schatten dat zij – of iemand in hun naaste omgeving – slachtoffer worden en waarvoor ze in een dergelijk geval dienen te vrezen. Bij slachtoffers kan hierdoor dan een gevoel van onmacht ontstaan, en van het geen grip hebben op de situatie. Zij ervaren deze vorm van doxing als angstig en bedreigend. Dit wordt nog verstrekt als de identificerende persoonsgegevens zijn verspreid binnen een grote groep (bijvoorbeeld door het delen ervan op social media), waardoor door slachtoffers noch door de politie ingeschat kan worden wie wanneer actie zou kunnen ondernemen.

De gevolgen van doxing in de fysieke wereld zijn zeer uiteenlopend van aard. Onlangs is in de nationale media aandacht geschonken aan gevallen van doxing en de effecten daarvan op slachtoffers. Zo vonden mensen die actief zijn op 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 bedreigingen gericht aan politieambtenaren naar voren.[1] Zo is een tijd lang getracht om de identiteit van undercoveragenten ('romeo's') te onthullen. Dit heeft een grote impact op de politieorganisatie en haar medewerkers. Over dit fenomeen zijn door verschillende leden van de Tweede Kamer schriftelijke vragen gesteld. Daarnaast is een motie aangenomen met de strekking doxing op zeer korte termijn strafbaar te stellen.[2]

Van strafbare feiten kan aangifte worden gedaan bij de politie. Voor onrechtmatige gedragingen staat daarnaast een gang naar de civiele rechter open. In geval van doxing geldt op dit moment echter, dat vooral de uitingsvormen die zich niet concreet openbaren in bedreiging, belediging en dwang niet te kwalificeren zijn als een strafbaar feit. Politie en openbaar ministerie geven aan dat dit in de weg staat aan het kunnen opstarten van een strafrechtelijk onderzoek. Zij kunnen dan ook geen bevoegdheden toepassen, zoals het bevelen van het ontoegankelijk maken van de online content of het vorderen van de gebruikersgegevens van de verdachte waarmee zijn identiteit kan worden vastgesteld. Het slachtoffer zal doorgaans niet weten wie verantwoordelijk is voor het verspreiden of het ter beschikking stellen van zijn persoonsgegevens. Dit bemoeilijkt het starten van een civiele zaak tegen diegene. Het gevolg hiervan is dat de door de slachtoffers ervaren vrees niet kan worden weggenomen. Het onderhavige wetsvoorstel voorziet daarom in een zelfstandige strafbaarstelling van doxing. Daarmee krijgen politie en openbaar ministerie een brede wettelijke grondslag om instrumenten in te zetten om de ervaren dreiging weg te nemen en tegen de schuldigen op te treden.

Bij doxing is het van belang dat de identificerende persoonsgegevens zo snel mogelijk ontoegankelijk 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 aansluiten van tussenpersonen bij de Notice and Take Down gedragscode helpt 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.

Met opmerkingen [s1.2.2] (2): 5.2.1

[redacted]

[1] https://www.politie.nl/binaries/content/assets/politie/onderwerpen/geweld-tegen-politieambtenaren/gtpa-cijfers-2017-tot-en-met-2020.pdf
[2] Kamerstukken II, 2020/2021, 35 564 nr. 13
[3] Zie artikel 1 van de Gedragscode Notice-and-Take-Down 2018.

In veel gevallen zal de directe angst die het slachtoffer ervaart, kunnen worden weggenomen, indien de identificerende persoonsgegevens niet meer publiekelijk beschikbaar zijn. Het is daarom van belang dat voorzien wordt in de mogelijkheid om bij een aanbieder van toegang tot internet de zogenaamde gebruikersgegevens te vorderen van een gebruiker van internet (art. 126na/ua Sv) zodat de identiteit van de verdachte kan worden vastgesteld waarna een verwijderverzoek kan worden uitgevaardigd.

Met opmerkingen 5.1.2.e **(3):** 5.2.1

3. Strafbaarstelling doxing

Hoewel de hierboven beschreven vormen van intimidatie op dit moment zoals aangegeven niet steeds onder een strafbepaling ressorteren, kunnen de consequenties ervan op het leven van de betrokkenen groot zijn. Slachtoffers worden geïntimideerd en voelen zich niet meer veilig. Dit kan ertoe leiden dat zij zich anders gaan gedragen, en niet meer, online maar ook offline, naar buiten durven te treden. Deze ontwikkeling is zeer kwalijk. Eenieder moet zich veilig kunnen voelen in de digitale en fysieke wereld. Het delen van andermans persoonsgegevens mag er niet toe leiden dat anderen daardoor in hun persoonlijke vrijheid worden beperkt. Daarom wordt voorgesteld doxing 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.

Strafbaar wordt 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, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel hem door anderen vrees aan te laten jagen, ernstige overlast aan te laten doen of in de uitoefening van zijn ambt of beroep ernstig te laten hinderen. Hoewel onder omstandigheden sprake kan zijn van overlap met reeds strafbare gedragingen, zoals belaging of bedreiging, is dat zeker niet altijd het geval.

Voor strafbare bedreiging (artikel 285 Sr) is vereist dat iemand wordt bedreigd met bepaalde ernstige misdrijven, namelijk met openlijk in vereniging geweld plegen tegen personen of goederen, met geweld tegen een internationaal beschermd persoon of diens beschermde goederen, met enig misdrijf waardoor gevaar voor de algemene veiligheid van personen of goederen of gemeen gevaar voor de verlening van diensten, met verkrachting, met feitelijke aanranding van de eerbaarheid, met enig misdrijf tegen het leven gericht, met gijzeling, met zware mishandeling of met brandstichting. Voor doxing is evenwel niet vereist dat de gedraging een zodanige bedreiging met een ernstig misdrijf impliceert.

Het wederrechtelijk stelselmatig opzettelijk inbreuk maken op de persoonlijke levenssfeer van een ander met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen is als belaging strafbaar gesteld in artikel 285b Sr. Hoewel het hiervoor vereiste oogmerk deels overeenkomt met dat voor doxing betreft het andersoortige gedragingen. Een belangrijk verschil is dat het bij belaging gaat om het herhaaldelijk lastigvallen van een bepaald persoon waardoor een inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkene, het gaat bijvoorbeeld om achtervolgen of steeds berichten sturen. Bij doxing ligt het zwaartepunt wat betreft de strafwaardigheid niet zozeer bij de inbreuk op de persoonlijke levenssfeer maar veeleer bij de gevaarzetting of ernstige overlast die wordt beoogd met het zich verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens.

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 ergens toe wordt bewogen. 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). 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). Voor strafbaarheid wegens dwang, ambtsdwang, afdreiging of afpersing is vereist dat het slachtoffer ergens toe wordt gedwongen. Ook in relatie tot deze misdrijven onderscheidt de voorgestelde strafbaarstelling van doxing 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 ergens

toe is gedwongen, zal er dus wel sprake kunnen zijn van doxing als aan de daarvoor gestelde 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). 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.

Doxing wordt strafbaar gesteld omdat in sommige gevallen juist geen overlap bestaat met bestaande strafbaarstellingen terwijl strafrechtelijk optreden wel wenselijk is. Het gaat dan met name om situaties waarin wel identificerende persoonsgegevens zijn verzameld of verspreid met het oogmerk een ander vrees aan te jagen, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep te hinderen, maar deze gedraging niet voldoende is voor bedreiging, belaging of mishandeling. De intimiderende werking die van doxing uitgaat kan dan wel zijn bereikt. Doxing zal ook vooraf kunnen gaan aan andere strafbare gedragingen, begaan door degene die zich eerst schuldig heeft maakt aan doxing of door anderen. Deze strafbaarstelling voorziet daarmee in een aanvulling op de strafbepalingen waarmee vormen van intimidatie, zoals bedreiging en belaging, strafbaar zijn gesteld.

Het openbaar ministerie kan een strafrechtelijk onderzoek starten naar aanleiding van signalen van doxing. Vaak 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, immers altijd de beslissing moeten nemen of hij het wenselijk acht dat de dader wordt vervolgd. Van iemand die geïntimideerd is of wordt kan dit niet worden verwacht. Uiteraard zal het openbaar ministerie doorgaans geen strafrechtelijk onderzoek instellen als het slachtoffer dit onwenselijk acht.

Bij het begaan van de strafbaar gestelde gedragingen zal veelal gebruik worden gemaakt het internet, meer bepaald sociale media. Dit vraagt deels om een andere aanpak van de opsporing dan bij gedragingen in de fysieke wereld. Door doxing aan te merken als feit waarvoor voorlopige hechtenis is toegelaten komen extra opsporingsbevoegdheden beschikbaar. De snelheid waarmee het internet en sociale media veranderen, maakt het voor het strafrechtelijk onderzoek noodzakelijk om relevante informatie zo snel mogelijk vast te leggen. 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 is onderzoek op het internet nodig, gericht op het achterhalen van het IP-adres 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. 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. Hiervoor zal in eerste instantie gebruik worden gemaakt van de Notice and Take Down (NTD)-gedragscode. In de gevallen waarin de NTD-gedragscode niet afdoende is voor de verwijdering van de gegevens, bijvoorbeeld omdat verschil van inzicht bestaat over de strafbaarheid van de content, of wanneer sprake is van een aanbieder die de gedragscode niet heeft ondertekend, kan de officier van justitie als aan de daarvoor geldende vereisten is voldaan – ontoegankelijk maken is noodzakelijk ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten en machtiging van de rechter-commissaris - gebruikmaken van de bevoegdheid tot het geven van een bevel om gegevens ontoegankelijk te maken (artikel 125p Sv).

Voor politie en openbaar ministerie wordt het door een op de specifieke gedraging toegesneden strafbaarstelling naar verwachting eenvoudiger om doxing op te sporen, te vervolgen en te bewijzen. De strafrechtelijke aanpak is gericht op situaties waarin iemand bewust de privacy van een ander schendt. 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.

4. De situatie in andere landen

Doxing is geen typisch Nederlands verschijnsel. Ook andere landen, zowel binnen als buiten Europa, worden ermee geconfronteerd. In Duitsland heeft de Bondsregering een wetsvoorstel in consultatie gebracht om een specifieke vorm van doxing tegen te gaan, namelijk de verspreiding van zogenoemde "vijandelijke lijsten". Het nieuwe strafbare feit dient om de bescherming van de algemene rechtszekerheid en het vreedzaam samenleven van burgers te verbeteren, evenals het vertrouwen in de rechtsstaat, dat aanzienlijk wordt aangetast door deze variant. De verspreiding van persoonsgegevens van meerdere personen of zelfs van één persoon op een bepaalde manier moet als strafbaar feit worden geregistreerd, indien dit in het openbaar gebeurt, in een vergadering of fysiek of online.

In Frankrijk werd op 25 mei 2021 de Wet nr. 2021-646 van 25 mei 2021 voor "uitgebreide veiligheidsbehoudende vrijheden" uitgevaardigd. Deze wet voorziet onder meer strengere straffen voor overtredingen gepleegd tegen personen met openbaar gezag en in strafbaarstelling van "het creëren van computerbestanden voor kwaadaardige identificatiedoeleinden van ambtenaren", dat met 5 jaar gevangenisstraf wordt bestraft, zonder de toepassing van strafvermindering.

In Spanje werden in 2015 enkele wijzigingen in wetsartikelen doorgevoerd die een nadere invulling geven aan strafbare feiten die betrekking hebben op het hinderlijk volgen (ook online), het zonder toestemming openbaren van persoonsgegevens en het zich toegang verschaffen tot besloten gegevensbestanden met het doel deze gegevens publiekelijk te delen. Deze wetsartikelen laten zich niet direct vertalen naar een Nederlandse variant, maar hebben elementen in zich die passen bij een strafbaar feit als belaging. Slachtoffers van doxing kunnen hiermee ook te maken hebben of krijgen.

In de Verenigde Staten zijn in verschillende staten initiatieven genomen om doxing strafbaar te stellen. In Utah werd reeds in 2017 een wet aangenomen die strafbaar stelt de persoon die, met de bedoeling dat intimidatie door elektronische communicatie plaatsvindt, de identificerende informatie van een andere persoon bekendmaakt of verspreidt in de verwachting dat anderen de identificerende informatie van de persoon verder zullen verspreiden of gebruiken. Oklahoma heeft het gebruik van een elektronisch communicatieapparaat om bewust identificerende persoonsgegevens openbaar te maken strafbaar gesteld, als dat gebeurt met de bedoeling om een ander te bedreigen, te intimideren of lastig te vallen, of om een ander te helpen om te dreigen, te intimideren of lastig te vallen, resulterend in een redelijke vrees voor dood of ernstig lichamelijk letsel bij het slachtoffer. Het House of Representatives in Alabama nam een wet aan die als doxing strafbaar stelt het opzettelijk elektronisch publiceren, posten of verstrekken van persoonlijke identificerende informatie van een ander, met de intentie dat anderen die informatie zullen gebruiken om de ander lastig te vallen of te schaden, indien de andere persoon daadwerkelijk wordt lastiggevallen of geschaad. Deze wet stelt tevens strafbaar het opzettelijk elektronisch publiceren, posten of verstrekken van persoonlijke identificerende informatie van een wetshandhaver, brandweerman of ambtenaar, met de bedoeling dat anderen die informatie zullen gebruiken om de taakuitoefening van die functionaris lastig te maken, te schaden of te belemmeren, indien de functionaris hierna daadwerkelijk wordt lastiggevallen, geschaad of belemmerd bij het uitvoeren van zijn of haar taak. De Senaat in Alabama moet dit wetsvoorstel nog behandelen. Ten slotte is in Colorado is een wet aangenomen die strafbaar stelt het willens en wetens via internet beschikbaar stellen van persoonlijke informatie over een beschermd persoon of over zijn naaste familie, indien de verspreiding van persoonlijke informatie een onmiddellijke en ernstige bedreiging vormt voor de veiligheid van de betrokkene of zijn naaste familie, en de persoon die de informatie op internet beschikbaar stelt, weet of redelijkerwijs op de hoogte zou moeten zijn van de onmiddellijke en ernstige dreiging. Het departement van Homeland Security heeft een publicatie met de titel "*How to prevent online harassment from "doxxing"*" uitgevaardigd, waarin preventieve maatregelen staan opgenomen om doxing te voorkomen en slachtoffers een handelingsrepertoire wordt geboden.

De beschreven strafbaarstellingen hebben gemeen dat zij steeds betrekking hebben op het verspreiden en/of verzamelen van persoonsgegevens (zonder toestemming van de betrokkene). De overige voorwaarden verschillen zoals hierboven aangegeven per land. De in onderhavig wetsvoorstel opgenomen strafbaarstelling vergt, evenals de (voorgestelde) strafbepalingen in enkele andere landen (Frankrijk, Oklahoma, Alabama en Colorado), 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 van de uitoefening van ambt of beroep. Niet gekozen is voor een beperking tot bepaalde beroepsgroepen of personen, zoals in Frankrijk, Alabama en Colorado, 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

vormgeving van het vereiste oogmerk door hierin expliciet 'het ernstig belemmeren van ambt of beroep' op te nemen. Bijvoorbeeld in het geval van persoonsgegevens van politieambtenaren worden verspreid zal de betrokkene hiermee kunnen pogen het uitoefenen van de functie te belemmeren. Er is voor gekozen de strafbaarstelling niet te beperken tot het zich 'openbaar' verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens. Een dergelijke beperking zou ertoe leiden dat het delen van gegevens in besloten groepen niet strafbaar zou zijn. Dit lijkt gezien het mogelijke effect hiervan geen dusdanige afbreuk te doen aan de strafwaardigheid van de gedraging dat dit niet onder het bereik van de strafbaarstelling zou moeten worden gebracht.

5. Verhouding met fundamentele rechten

Bij doxing wordt veelal gebruik gemaakt van openbare gegevensbronnen. Daarmee rijst de vraag hoe doxing zich verhoudt tot het recht op eerbiediging van de persoonlijke levenssfeer, zoals verwoord in artikel 8 EVRM en artikel 10 van de Grondwet. Van belang is, dat de AVG ook toepasselijk is op persoonsgegevens die in een vrijelijk toegankelijke openbare gegevensbron zijn opgenomen. De AVG ziet op verwerkingen van persoonsgegevens. Ook voor het gebruik van gegevens uit openbare bronnen is in veel gevallen een wettelijke grondslag nodig om deze gegevens te mogen verwerken, waaronder mede wordt verstaan het publiekelijk delen van deze gegevens met anderen. Uit het gegeven dat iemand expliciet toestemming heeft gegeven om gegevens op te nemen in een openbare gegevensbron, kan niet worden afgeleid dat daarmee ook toestemming is gegeven voor hergebruik. Onder de AVG dient de toestemming steeds specifiek te zijn. Verwerking van iemands gegevens zonder toestemming is wel mogelijk indien daartoe een gerechtvaardigd belang bestaat en de schending van de persoonlijke levenssfeer tot een minimum wordt beperkt.

Tegelijkertijd heeft een ieder recht op vrijheid van meningsuiting, zoals verwoord in artikel 10 EVRM en artikel 7 van de Grondwet. Het samenbrengen en publiceren van persoonsgegevens kan wel degelijk een gerechtvaardigd belang opleveren. Bijvoorbeeld wanneer de intentie van de openbaarmaking is gelegen in het aan de kaak willen stellen van misstanden. 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 doxing vallen indien daarbij identificerende persoonsgegevens worden verspreid en degene die dit doet daarbij 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 dan wel hem door anderen vrees aan te laten jagen, ernstige overlast aan te laten doen of in de uitoefening van zijn ambt of beroep ernstig te laten hinderen. Bij het geven van een mening over een bepaald onderwerp zal daarvan geen sprake zijn. Voor zover daarbij al identificerende persoonsgegevens van een ander worden verspreid – bijvoorbeeld de naam van degene op wie wordt gereageerd – zal het vereiste oogmerk immers ontbreken.

De vrijheid van meningsuiting wordt echter ook begrensd. Artikel 10 lid 2 EVRM wijst nadrukkelijk op de plichten en verantwoordelijkheden die in een democratische samenleving noodzakelijk zijn "in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen." In het huidige klimaat van nieuwe fenomenen op internet eist de democratische samenleving dat er terughoudend wordt omgegaan met de vrijheid van meningsuiting als daarmee individuen angst wordt aangejaagd. Daarbij wordt mede overwogen, dat de vrijheid van meningsuiting niet alleen toepasselijk is op het individu, maar ook op de democratische samenleving als geheel. Daarnaast mag het gebruik van de vrijheid van meningsuiting geen instrument zijn om de vrijheid van een ander te beperken.

6. Adviezen

PM

7. Uitvoerings- en financiële consequenties

Het wetsvoorstel zal geen noemenswaardige gevolgen hebben voor de werklast van de rechtspraak, het openbaar ministerie en de politie. De werkzaamheden voor deze organisaties veranderen niet in omvang en frequentie. Het wetsvoorstel verruimt in materieel opzicht uitsluitend het beoordelingskader.

II. ARTIKELSGEWIJZE TOELICHTING

Artikel I (Wijziging Wetboek van Strafrecht)

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, ernstige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel hem door anderen vrees aan te laten jagen, ernstige overlast aan te laten doen of in de uitoefening van zijn ambt of beroep ernstig te laten hinderen. 'Zich verschaffen' betreft het zich doen toekomen van gegevens, hieronder kan met andere woorden worden verstaan het verzamelen van gegevens. 'Verspreiden' is het distribueren van gegevens. Dit hoeft niet in het openbaar te gebeuren. In de context van deze strafbaarstelling betekent dit dat gegevens door meerdere personen kunnen worden ingezien, het gaat dus bijvoorbeeld niet om het aan slechts één ander sturen van gegevens. Voor 'anderszins ter beschikking stellen' is niet vereist dat meerdere personen worden bereikt maar gaat het om de mogelijkheid die de ander hierdoor krijgt om met hetgeen aan hem ter beschikking is gesteld, in dit geval met de 'identificerende persoonsgegevens', naar eigen goedvinden te handelen.

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 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).

Met opmerkingen 5.1.2. (4):5.2.1 [redacted]

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 doxing 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 is de bedoeling 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 opmerkingen 5.1.2. (5):5.2.1 [redacted]

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 1997/1998, 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 1997/1998, 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 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 moet zijn gericht de betrokkene vrees aan te jaren, 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 bij slachtoffer ten gevolge van de gedraging vrees is aangejaagd, 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 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; doxing is een formeel omschreven delict.

Het strafmaximum bedraagt een jaar gevangenisstraf of een 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.

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 aanhouden buiten heterdaad, inverzekeringstelling en voorlopige hechtenis en de inzet van bijzondere opsporingsbevoegdheden als het vorderen van gegevens kunnen nodig 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 doxing 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 doxing 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