Media

KORT

Viruswaarheid-voorman Willem Engel zet adres Kaag op Twitter, D66-leider doet aangifte

■ D66-leider Sigrid Kaag gaat aangifte doen tegen Viruswaarheid-voorman Willem Engel, nadat hij op Twitter adresgegevens van haar heeft gedeeld. Engel deelde een foto van een informatieverzoek bij het Kadaster. Op de foto zijn haar huisnummer en postcode zichtbaar. Vorige week werd een man opgepakt, omdat hij met een brandende fakkel voor het huis van Kaag stond en complotleuzen riep. Engel schrijft te willen weten 'op wie zijn naam deze woning staat', onder meer omdat Kaag volgens hem banden zou hebben met de Open Society Foundation. Deze organisatie, die zich inzet voor 'inclusieve en levendige democratieën', is van de Amerikaans-Hongaarse filantroop George Soros. Hij is vaak het mikpunt van extreemrechtse en antisemitische complottheorieën. Later verwijderde Engel de afbeelding en schreef dat het delen van de foto 'op geen enkele manier' een 'oproep of aanzet tot intimidatie of geweld of bedreiging' was. Volgens hem gaat het om 'transparantie van iemand die minister van Financiën wordt'.

ANP

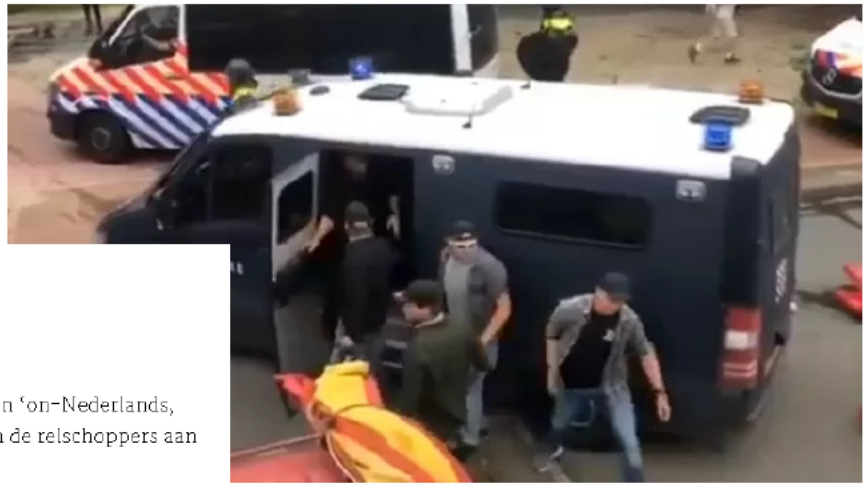
Algemene ontwikkelingen (2)

1. Filmen van politiecollega's
2. Buiten reikwijdte
3.
4.
5.

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

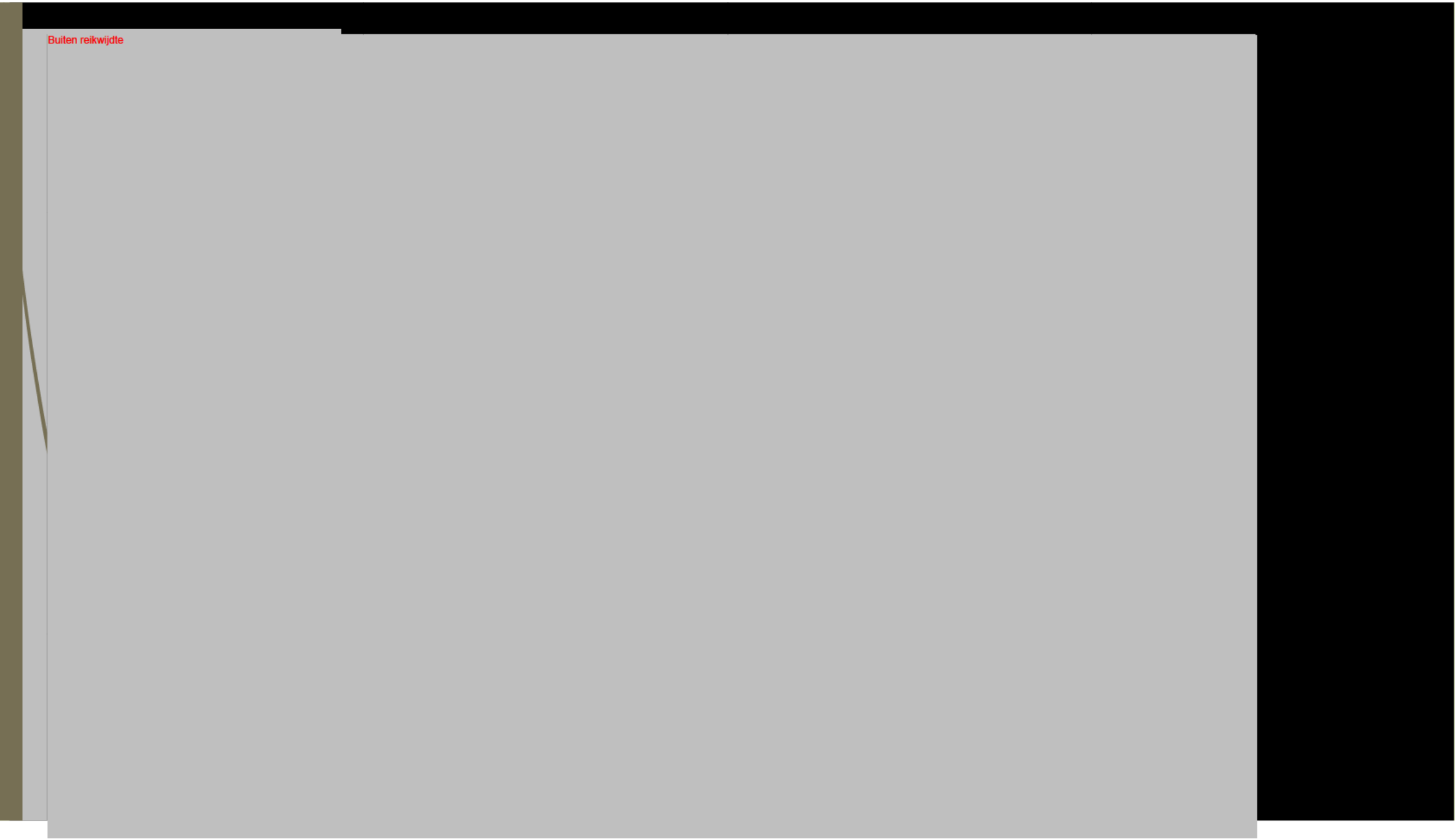
Voorbeelden uitspraken kortgeding

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

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. Buiten reikwijdte
› 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

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

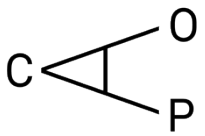
(sub) onderwerp	*Nog nader uit te werken*	*Stand van zaken*	*Actie*
Filmpjes offline halen		Afdeling 5.1.2.e van de LE is 'single point of contact' en 'trusted flagger' voor alle sociale media bedrijven.	NP – communicatie hierover in de organisatie
		'Notice en take down-procedure' is in gebruik.	NP – 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						

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 7 februari 2023 11:29
Aan: 5.1.2.e
Onderwerp: Intranetbericht doxing 29 december

Doxing: wetgeving in de maak

Laatst gewijzigd: 29-12-2022 | 11:04
Bron: Informatiebeveiliging

Collega's worden steeds vaker geconfronteerd met doxing. Het is nu nog niet strafbaar maar wetgeving wordt binnenkort verwacht.

Bij doxing wordt vaak een foto via social media gedeeld en worden andere gebruikers opgeroepen persoonsgegevens als het huisadres te achterhalen. Doxing heeft een forse impact op de collega en het thuisfront. Op dit moment is wetgeving rond doxing in de maak. De verwachting is dat dit binnenkort tot een afronding komt. Doxing is nu dus nog niet strafbaar. Afhankelijk van de casus kan er ook sprake zijn bedreiging, smaad, laster of belediging. En dat is natuurlijk wel strafbaar.

Wat kun je doen tegen doxing?

Een aanpak tegen doxing begint met preventie. Denk daarbij aan de manier waarop je als politiemedewerker of privépersoon social media gebruikt en vindbaar bent via internet. Als een collega wordt gedoxt, is het zaak snel te handelen. Eerst moet worden nagegaan wat de dreiging is en of veiligheidsmaatregelen voor de collega en het thuisfront noodzakelijk zijn. Ook kan worden nagegaan of doxing in een vroeg stadium kan worden ingedamd door de account(s) van waaruit wordt gedoxt te bevriezen of de content door de social media bedrijven te laten verwijderen. Een verzoek hiervoor kan via de interceptiedesk van de eigen eenheid worden gedaan. Die nemen dan contact op met de Landelijke Eenheid. De Landelijke Eenheid heeft contacten met de relevante social media bedrijven. Uiteraard is het ook van belang dat de gedoxte collega emotioneel wordt ondersteund. Zoals gezegd, zien we dat doxing forse impact bij collega's kan hebben.

Aanpak tegen doxing

Binnen de deelportefeuille geweld (onderdeel van de portefeuille CCB/geweld) wordt een aanpak ontwikkeld om de collega's tegen doxing te beschermen en de gevolgen van doxing te minimaliseren. Het gaat om een brede aanpak: van preventie, signalering en quick response tot een partnerstrategie (met de social mediabedrijven) en het verstoren, opsporen en vervolgen van mensen die doxing plegen. Mocht je vragen hebben over de aanpak of ideeën hebben, neem dan gerust contact op met 5.1.2.e of 5.1.2.e

Dit nieuwsbericht is ook gepubliceerd in het Privacy & Security Nieuws van januari 2023.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Politie | Staf korpsleiding | 5.1.2.e

behalve de woensdag

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

Over het 5.1.2.e : zie 5.1.2.i

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.

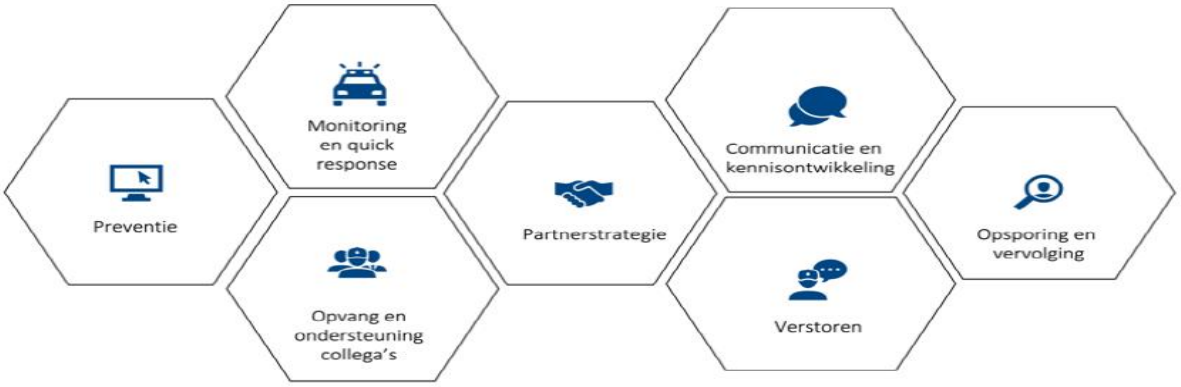
1.3 Voorgeschiedenis

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.

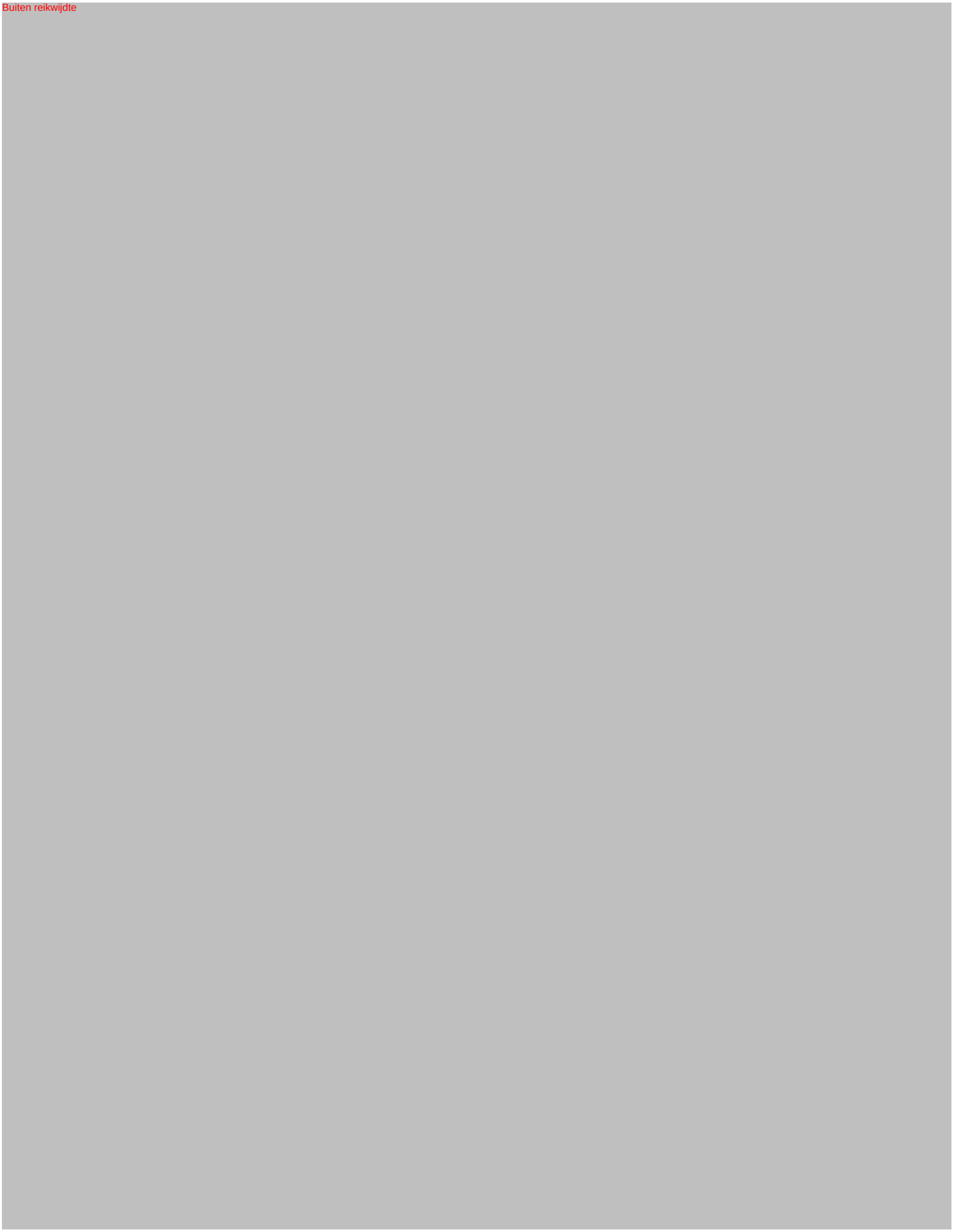
Het ontwikkelde handelingskader voor leidinggevenden geldt als een eenduidig, landelijk werkprocesdocument. Vanwege de (steevast aanwezige) complexiteit qua verloop van politiedoxing en de hieraan verbonden noodzakelijke handelingssnelheid, is het zaak om de binnen het kader betrokken disciplines van 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.

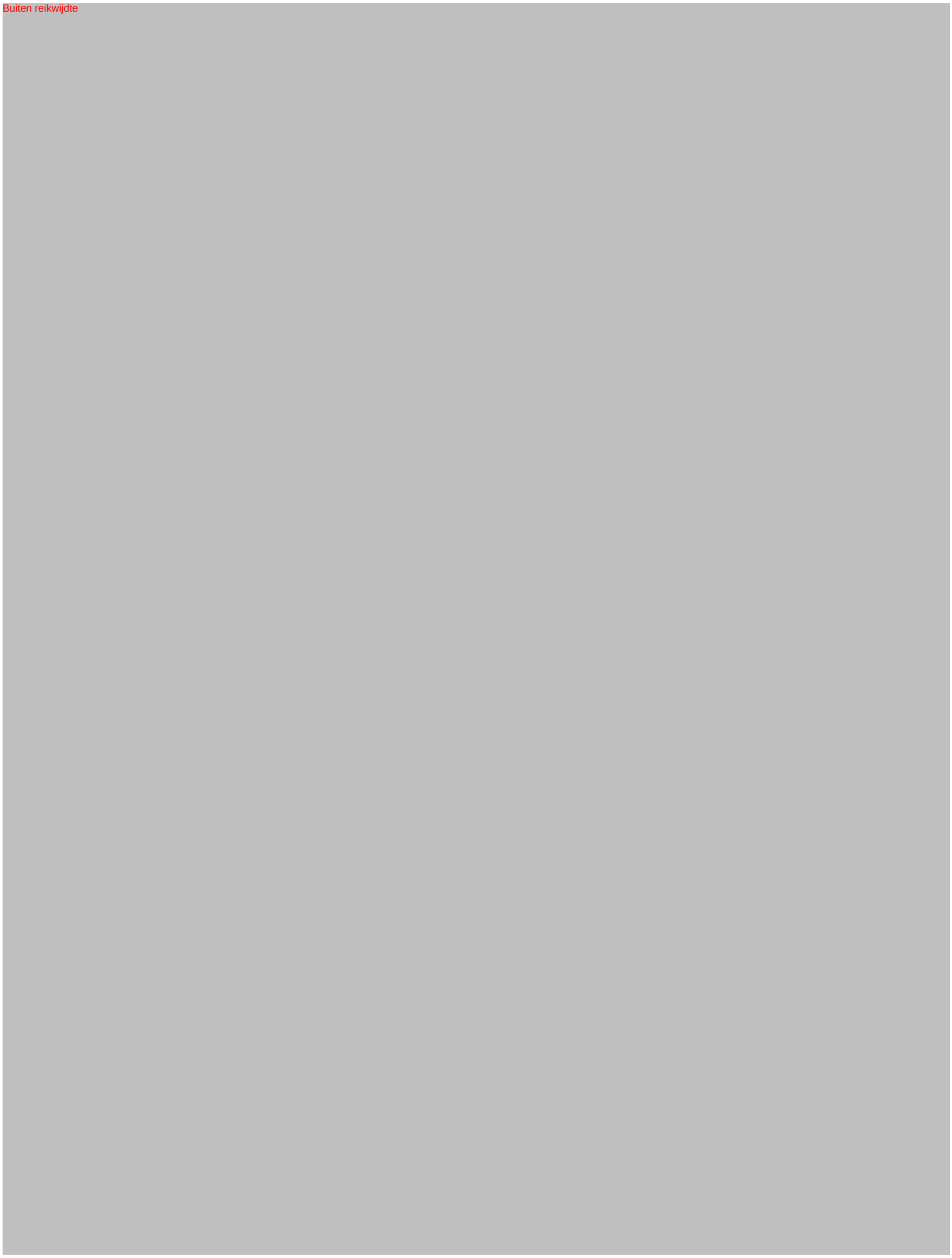
1.4 Projectdoelstelling

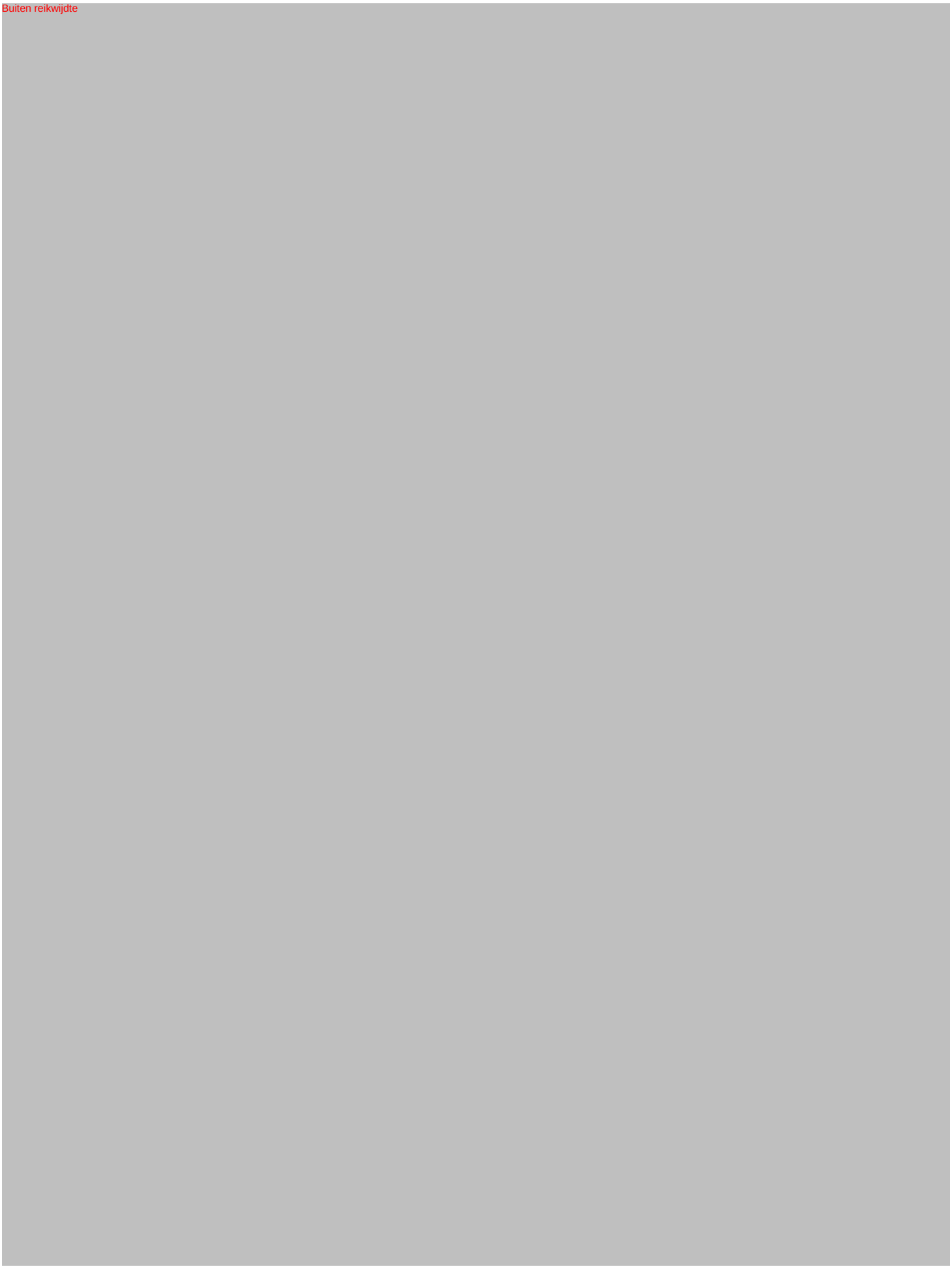
Omdat de strafbaarstelling van doxing echter geldt voor eenieder dient de Politie zich qua implementatie op zowel het generieke deel – de invoering van doxing als nieuw strafbaar feit – als de interne (door)ontwikkeling en procesvoering rond politiedoxing te richten. In bovenstaand verband bezien kent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

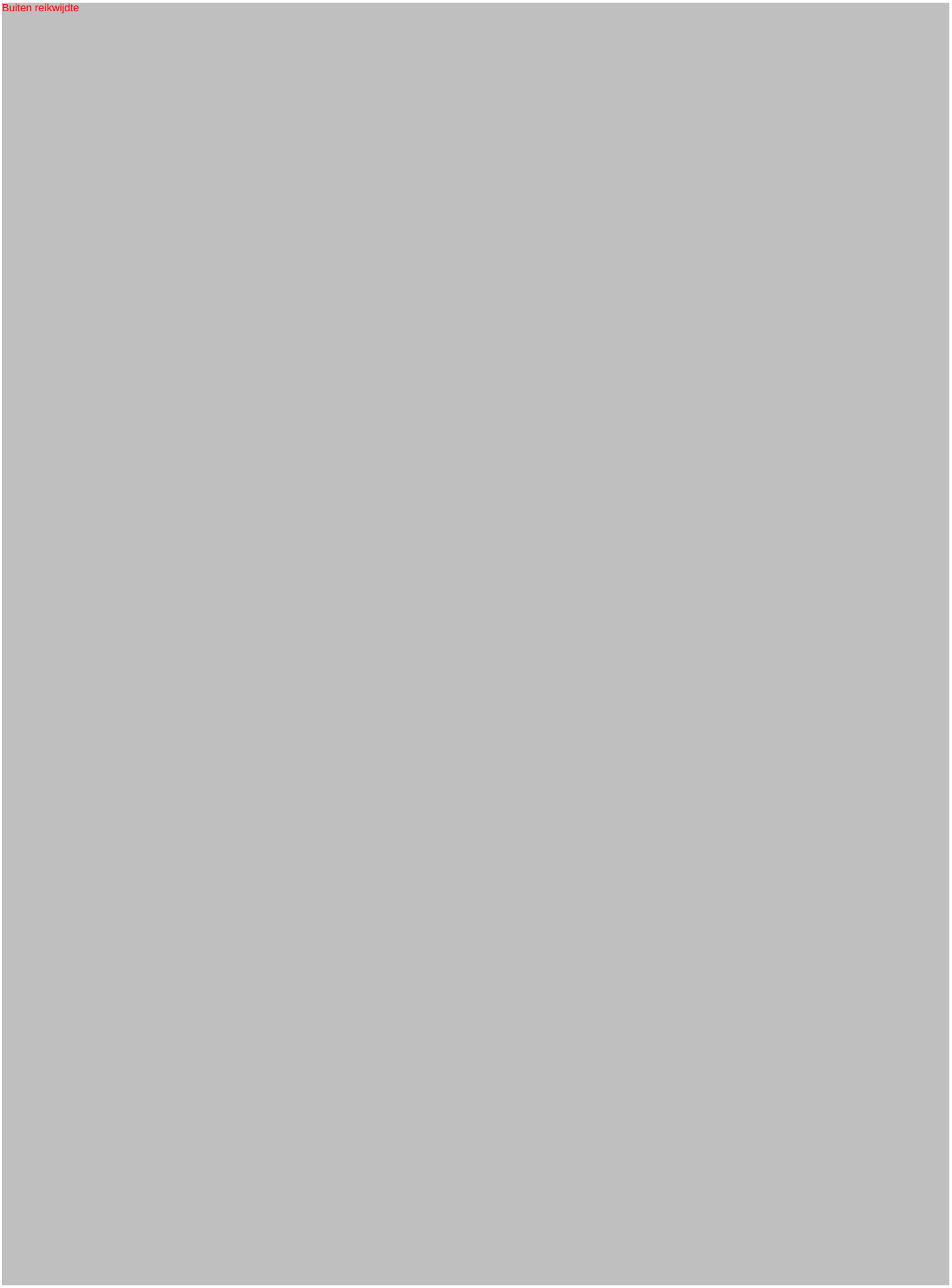
1. Realiseren dat het generieke strafbaar feit doxing in het korps geïmplementeerd wordt, in samenwerking met de betrokken organisatieonderdelen en de portefeuille VPT-GTPA.
2. Zorgdragen dat ten aanzien van GTPA het handelingskader doxing voor leidinggevenden en zijn bedoelde werking gaat linden in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

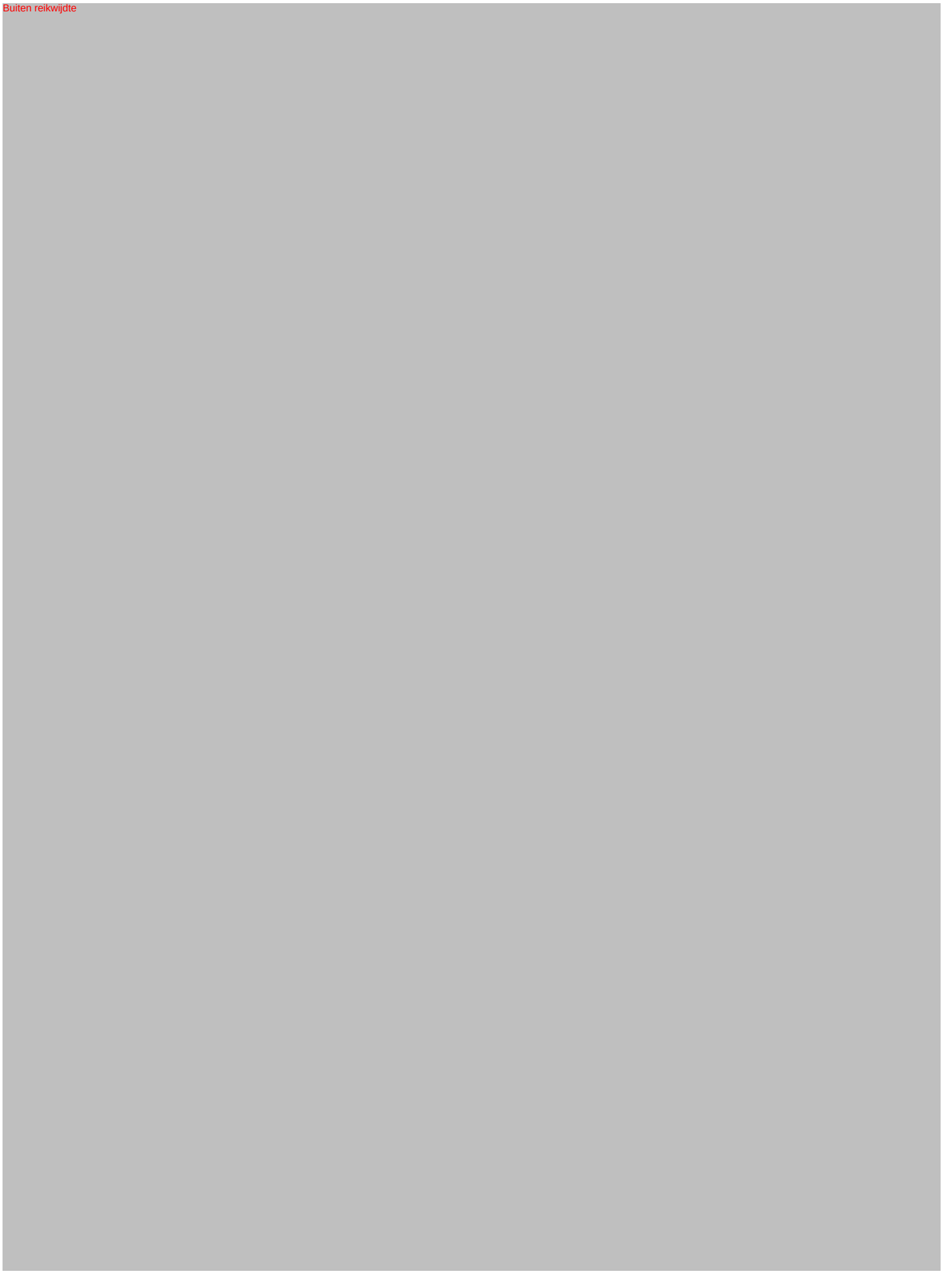
In paragraaf 2.3 zijn de subdoelen per organisatieonderdeel beschreven en uitgewerkt tot concrete, geprioriteerde actiepunten.


Buiten reikwijdte

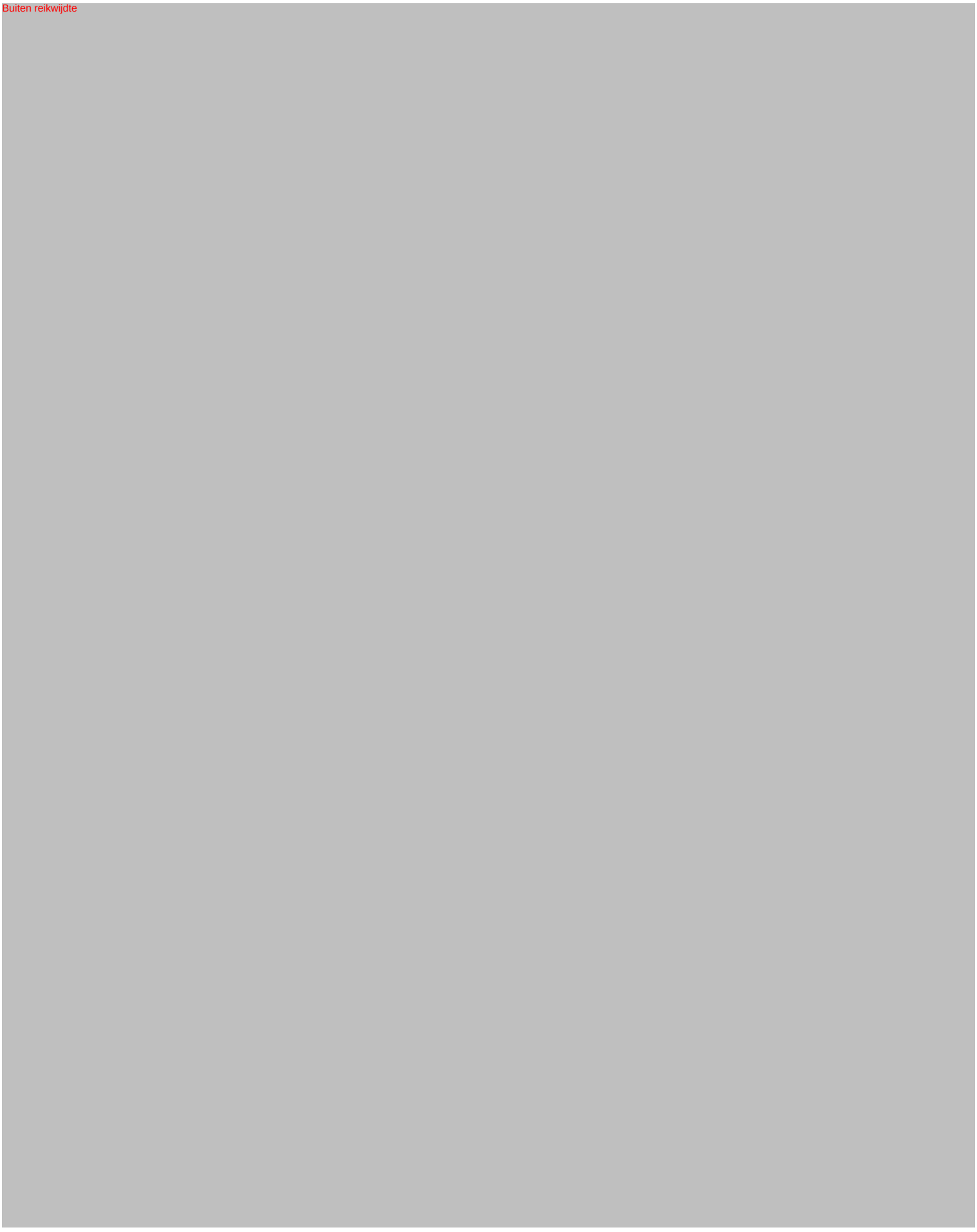

Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte


Buiten reikwijdte

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

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 27 september 2023 12:54
Aan: SK - Korpsstaf - Team Juridische Zaken - Woo
Onderwerp: WOO-verzoek filmen politie.

Ter info en behorend bij het verzoek.

Van: 5.1.2.e 5.1.2.e @politie.nl>
Verzonden: donderdag 24 augustus 2023 17:47
Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: beeldmateriaal Doxing

Hallo heren en 5.1.2.e

Voor de invoering van de wet Doxing heb ik een communicatiestrategie opgesteld.
Deze is inmiddels goedgekeurd en ben de volgende stappen aan het zetten wat betreft de basis aan communicatiemiddelen.
Hier hoort juist beeld bij. Tot op heden maken we gebruik van beeld uit de beeldbank wat nogal beperkt is en wat ik graag uitbreid. Niet alleen voor onze communicatiemiddelen, maar ook voor nieuwsberichten in de toekomst.

Denk bv aan:
- het communiceren op 1 januari bij de inwerkingtreding van de wet waarbij de strafbaarheidstelling niet alleen geldt voor onze medewerkers maar voor iedere burger.
- wellicht het communiceren van cijfers doxing (aantal meldingen/aangifte
- doxing van burgers maar ook VPT (denk aan burgemeesters en andere politicus)
- algemene info wat is doxing op politie.nl voor burgers
- algemene info doxing op intranet voor collega's als ze zelf gedoxt zijn (GTPA) en als ze melding/aangifte/opsporing moeten doen (wij als dienstverlener)

Het beeld wat we nu vooral gebruiken:

Let op, we zien dat er door een aantal partijen (o.a. XR) gesteld wordt dat de politie de indruk wekt dat het filmen openbaar van politie niet meer zou mogen. 5.2.1

Graag verneem ik van jullie uiterlijk 31 augustus welk beeld jullie nodig hebben/gewenst is. Kortom graag ontvang ik zo concreet mogelijk een omschrijving van het beeld dat je wenst.

Groet 5.1.2.

5.1.2.e
Communicatieadviseur
06 – 5.1.2.e
5.1.2.e @politie.nl
Werkdagen: ma, di, wo en do

Politiedienstencentrum | Dienst Communicatie | Team Account & Advies
Marten Meesweg 35, 3068 AV Rotterdam
Postbus 70023, 3000 LD Rotterdam

Meer informatie? Kijk op politie.nl

Van: 5.1.2.e

Verzonden: donderdag 13 juli 2023 17:19

Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>

CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>

Onderwerp: RE: insta post + intranet wet Doxing

Hi 5.1.2.e

5.2.1

5.2.1

Groeten 5.1.2.e

5.1.2.e
5.1.2.e
06-5.1.2.e

Nationale Politie I Staf Korpsleiding
Directie Operatien I Afdeling Programmamanagement
Nieuwe Uitleg 1, 2514BP Den Haag

5.1.2.e (crtl+klik)

Van: 5.1.2.e 5.1.2.e @politie.nl>
Verzonden: donderdag 13 juli 2023 17:13
Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: insta post + intranet wet Doxing

Beste 5.1.2.e en 5.1.2.e

Zie onderstaand alert van 5.1.2.e Zij verzorgt vanuit de landelijke newsroom o.a. de webcare en ziet deze reactie/oproep van CtrlAltDel voorbij komen. We verwachten dat hier wel onder gereageerd gaat worden.

Ik denk dat ons standpunt met name is dat doxing gaat over meer dan filmen en het verspreiden van de gegevens van een ieder met als doel te intimideren straafbaar gesteld gaat worden.
Dat staat los van het filmen van de politie in het openbaar.

Groet 5.1.2.

5.1.2.e
Communicatieadviseur
06 – 5.1.2.e
5.1.2.e @politie.nl
Werkdagen: ma, di, wo en do

Politiedienstencentrum | Dienst Communicatie | Team Account & Advies
Marten Meesweg 35, 3068 AV Rotterdam
Postbus 70023, 3000 LD Rotterdam

Meer informatie? Kijk op politie.nl

Van: 5.1.2.e 5.1.2.e @politie.nl>
Verzonden: donderdag 13 juli 2023 10:56
Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: insta post + intranet wet Doxing

Hai 5.1.2.e & 5.1.2.e

Wij zien zojuist dat ControleAltDelete het volgende heeft gepost op Twitter:

https://twitter.com/CntrleAltDlt/status/1679403884295462912/

Wij zijn hier ook in getagd door hen. We wilden jullie hiervan op de hoogte stellen.
In het artikel staat:

Filmen van politieambtenaren kan strafbaar zijn? Hoe zit het dan met het ambt bemoeilijken? Waarop ziet de controle? Kunnen mensen agenten nog wel filmen? Hoe gaan politiemensen hier in de praktijk op reageren?

Filmen is dus strafbaar als er een "oogmerk" is om "vrees aan te jagen" of "het ambt ernstig te verstoren". Allemaal dingen die in het hoofd van de verdachte of de politieagent zitten. Dus het enige wat je kan zien is het filmen.

Er is dus kritiek op dit stukje omdat mensen niet snappen dat het filmen zelf niet strafbaar is. Wellicht is het handig om hier alvast een Q&A op voor te bereiden.

Denk hierbij aan vragen zoals:

- Is het filmen van politieagenten straks strafbaar?

- Ben ik straks strafbaar als ik mijn (zelfgemaakte opnames van het optreden van de politie) beelden online zet?
- Wat kan ik doen om ‘mezelf te beschermen’?
- Wat wordt er gezien als het hinderen van een politieagent?
- Wat valt onder persoonsgegevens/welke persoonsgegevens zijn strafbaar?

We verwachten wel wat reacties onder deze post. We houden jullie ervan op de hoogte.

5.1.2.e
5.1.2.e

M: 06 5.1.2.e
E-mail webcare 5.1.2.i @politie.nl
Werkdagen: ma, wo, vrij

Directie Communicatie | 5.1.2.e
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107 2502 CC Den Haag

Meer informatie? Kijk op politie.nl

Buiten reikwijdte

Meer informatie? Kijk op politie.nl


Buiten reikwijdte


Buiten reikwidjte


Buiten reikwijdte

Wetsgeschiedenis strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden (doxing)

artikel 285d Sr

Datum	3 oktober 2023
Status	Definitief

Vooraf
Aan de inhoud van dit samenvattend overzicht kunnen geen rechten worden ontleend. Voor een beoordeling van een zaak zal de wet, de wetsgeschiedenis - raadpleeg: (Kamerstukken I 36171) en de actuele rechtspraak vanaf datum inwerkingtreding van de wet moeten worden geraadpleegd.

Artikel 285d Sr Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden
1. Degene die zich persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk om die ander vrees aan te jagen dan wel aan te laten jagen, ernstige overlast aan te doen dan wel aan te laten doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel ernstig te laten hinderen, wordt gestraft met gevangenisstraf van ten hoogste twee jaar of geldboete van de vierde categorie.
2. Indien het feit, omschreven in het eerste lid wordt gepleegd tegen een persoon in diens hoedanigheid van Minister, Staatssecretaris, commissaris van de Koning, gedeputeerde, burgemeester, wethouder, lid van een algemeen vertegenwoordigend orgaan, rechterlijk ambtenaar, advocaat, journalist of publicist in het kader van nieuwsgaring, ambtenaar van politie of buitengewoon opsporingsambtenaar wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.

Artikel 67 Sv: het misdrijf wordt als 'VH-feit' aan dit artikel toegevoegd, zodat bevoegdheden zoals het vorderen van gegevens of bevel ontoegankelijk maken gegevens kunnen worden toegepast.

1 Reikwijdte strafbaarstelling

1.1 Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, onderdeel 1, AVG). Persoonsgegevens zijn bijvoorbeeld naam, adres, woonplaats, postadres, telefoonnummers, IP-adressen of geboortedatum. Het gaat niet alleen om 'identificerende persoonsgegevens', maar om alle persoonsgegevens als bedoeld in de AVG. Ook alleen een foto dus. Er kan sprake zijn van directe of van indirecte herleidbaarheid.

1.2 Een ander
Het slachtoffer; de persoon die men vrees wil (laten) aanjagen, ernstige overlast wil (laten) aandoen of in de uitoefening van zijn functie ernstig wil (laten) hinderen.

1.3 Een derde
Een persoon die in een bepaalde relatie staat tot het slachtoffer, en van wie de verdachte zich de persoonsgegevens verschaft teneinde het slachtoffer te intimideren, zoals de familieleden van het slachtoffer.

1.4. Zich verschaffen
Gedragingen die zijn gericht op het in het bezit krijgen van de persoonsgegevens; met andere woorden: het verzamelen van gegevens. Dit veronderstelt actief handelen van degene die zich persoonsgegevens verschaft.

Het bewijs voor de kwade bedoeling van een persoon bij het 'enkel' verzamelen van gegevens zal inderdaad op voorhand niet altijd duidelijk zijn. Wel als bijvoorbeeld een lijst van persoonsgegevens wordt aangetroffen bij een doorzoeking en de verdachte of een getuige verklaart dat deze zijn verzameld om de betrokkenen thuis te kunnen bedreigen.

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

Wijze van verkrijging niet relevant
Het 'zich verschaffen van persoonsgegevens' voor intimiderende doeleinden kan in samenwerking met diverse betrokkenen plaatsvinden. Onder die omstandigheden zal strafbaarheid kunnen worden aangenomen wegens medeplegen van doxing. Maar het 'zich verschaffen van persoonsgegevens' kan ook geheel zelfstandig gebeuren en ook die delictsvorm dient – zoals hiervoor toegelicht – strafbaar te zijn.

Voor zover het gaat om de strafbaarheid van het aanzetten van anderen tot doxing kan worden volstaan met strafbaarheid op grond van artikel 46a Sr (poging om een ander te bewegen een misdrijf te begaan) en de deelnemingsvorm uitlokking, op grond waarvan degenen strafbaar zijn die iemand door giften, beloften, misbruik van gezag, geweld, bedreiging, of misleiding of door het verschaffen van gelegenheid, middelen of inlichtingen pogen te bewegen tot strafbare doxing of daarmee strafbare doxing opzettelijk uitlokken.

Voor doxing wordt vaak informatie gebruikt die openbaar is, zonder dat opzettelijk en wederrechtelijk een computer wordt binnengedrongen of opzettelijk en wederrechtelijk gegevens worden overgenomen. Het gaat bijvoorbeeld om een combinatie van gegevens over een persoon uit verschillende bronnen. Denk daarvoor aan de gegevens die in een zeer beperkte kring van personen bekend zijn, zoals een huisadres of gegevens over de deelname aan een bepaald sportevenement die online zijn geplaatst. Voor strafbaarheid wegens doxing is de wijze van verkrijging van deze gegevens niet relevant.

1.5 Verspreiden of anderszins ter beschikking stellen

Distribueren of toezenden van gegevens. Dit handelen is niet beperkt tot de door de dader gekende of beoogde ontvangers van de informatie. Het verspreiden van persoonsgegevens, ook het verder verspreiden van gegevens nadat een ander die gegevens openbaar heeft gemaakt, is strafbaar op grond van artikel 285d Sr als degene die dit doet daarbij het oogmerk heeft de ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de beroepsuitoefening.

Omvang verspreiding
Voor strafbaarheid is het niet van belang hoeveel personen kennis hebben genomen of kennis kunnen hebben nemen van de persoonsgegevens. In voorkomende gevallen kan de kring van personen aan wie persoonsgegevens van een ander worden verstrekt wel worden betrokken bij de beoordeling van het oogmerk van de betrokkene bij de verstrekking, bijvoorbeeld bij het bepalen of het oogmerk was gericht op het veroorzaken van ernstige overlast of ernstige hinder. Bij een verzoek tot het plegen van een telefoontje kan het bijvoorbeeld uitmaken of dit aan een persoon wordt gestuurd of aan een grote groep. De omvang van de verspreiding van de gegevens zal daarnaast van belang kunnen zijn bij de beslissing of vervolging wordt ingesteld, bij het bepalen van de strafeis en bij de strafoplegging.

Strafbare poging
Een strafbare poging tot doxing kan bijvoorbeeld aan de orde zijn als het verspreiden van de persoonsgegevens niet zou zijn gelukt vanwege een technisch probleem bij de verspreiding. Een essentiële voorwaarde voor een strafbare poging is namelijk dat het delict (de strafbare doxing) niet wordt voltooid vanwege een van de wil van de dader onafhankelijke omstandigheid. Iemand kan zich echter ook persoonsgegevens verschaffen van een ander om die ander daarmee in de fysieke wereld vrees aan te jagen, ernstige overlast te veroorzaken of ernstig te hinderen in de uitoefening van ambt of beroep. Als het handelen van de betrokkene zich hiertoe heeft beperkt, is er nog geen sprake van een strafbare poging tot verspreiding van persoonsgegevens.

Een strafbare poging tot doxing is niet ondenkbaar. Een voorbeeld is de situatie waarin in een appgroep persoonsgegevens worden gevraagd maar deze gegevens niet beschikbaar bleken. Net als voor alle andere misdrijven geldt dat een poging tot het plegen van een misdrijf strafbaar is als het voornemen van de dader zich door een begin van uitvoering heeft geopenbaard (artikel 45, eerste lid, Sr).

1.6 Oogmerk

De bedoeling van de verdachte ten tijde van de gedraging. Niet vereist is dat het slachtoffer daadwerkelijk is beangstigd, gehinderd of overlast heeft ervaren. Het gaat om het door de dader beoogde effect. Of dit op het slachtoffer ook die uitwerking heeft of zou hebben gehad is voor strafbaarheid niet relevant. De kwade bedoeling is dus bepalend voor strafbaarheid.

Bewijs
Voor het bewijs van het oogmerk kan de rechter acht slaan op onder meer uiterlijk kenbare gedragingen en uitlatingen van de verdachte voor, tijdens of na het zich verschaffen, verspreiden of anderszins ter beschikking stellen van persoonsgegevens van de ander. Het oogmerk zal in sommige gevallen ook uit de context kunnen worden afgeleid. Dat de verdachte heeft deelgenomen aan een chatgroep waarin negatief is gesproken over het slachtoffer of de kring van personen waartoe het slachtoffer behoort, kan voor het bewijs van het oogmerk bijvoorbeeld van belang zijn als de verdachte het strafbare oogmerk ontkent. In dit voorbeeld kunnen berichten uit de chatgroep waarin kwaad wordt gesproken over het slachtoffer als bewijsmateriaal dienen, tezamen met gegevens waaruit blijkt dat de dader lid is van de chatgroep (bijvoorbeeld berichten die hij daar achterlaat) en een bericht van de dader waarin hij persoonsgegevens van het slachtoffer deelt.

Het oogmerk van de dader kan ook worden bewezen met behulp van verklaringen van getuigen aan wie de dader heeft verteld wat hij van plan was met de persoonsgegevens van een ander, uit aantekeningen in een dagboek of in een document waarin de dader persoonsgegevens heeft opgeslagen of berichten van de dader aan derden (bijvoorbeeld “ik heb eindelijk het adres gevonden van X, als ze mij bij haar huis ziet zal ze wel inzien dat ze haar standpunt moet herzien”).
Veel hangt daarom af van hetgeen uit objectieve feiten en omstandigheden blijkt over het oogmerk van de dader

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

Journalisten, publicisten en klokkenluiders

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

Het is niet de bedoeling dat de strafbepaling ertoe leidt dat journalisten terughoudender worden in hun informatiegaring en berichtgeving. In het kader van hun werkzaamheden verzamelen en verspreiden journalisten vaak persoonsgegevens van anderen. Bij journalisten en publicisten die in hun hoedanigheid te goeder trouw zijn, ontbreekt het voor strafbaarheid vereiste oogmerk van intimidatie. Er is daarom geen noodzaak voor een afzonderlijke strafuitsluitingsgrond. Daarmee zou ook de indruk ontstaan dat er situaties zijn waarin het zich verschaffen, verspreiden of anderszins ter beschikking stellen van andermans persoonsgegevens met het doel een ander te intimideren gerechtvaardigd kan zijn omdat het algemeen belang hiermee zou zijn gediend. Dat is nadrukkelijk niet de bedoeling. Personen met niet-kwaadwillende bedoelingen die persoonsgegevens verzamelen of verspreiden, zoals journalisten, maken zich niet schuldig aan strafbare doxing. Personen die daarentegen wel kwaadwillende bedoelingen hebben, kunnen zich niet op een hoger doel beroepen.

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

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

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

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

Minimaal oogmerk van intimidatie
Als de verstrekker geen weet heeft van de intimiderende doeleinden van de ontvanger zal geen sprake zijn van strafbaar handelen van de kant van de verstrekker. De verstrekker heeft namelijk niet het voor de strafbare intimidatie vereiste oogmerk. Om tot een bewezen feit te komen is een vorm van opzet vereist, te weten het oogmerk van intimidatie. Het oogmerk van de verdachte bij de strafbaar gestelde gedragingen met de persoonsgegevens van een ander of een derde moet zijn gericht op het (laten) aanjagen van vrees, het (laten) aandoen van ernstige overlast of ernstig (laten) hinderen in de uitoefening van ambt of beroep. Dit moet worden vastgesteld om tot een bewezen feit te komen.

1.7 Vrees aanjagen

Het gaat om het bang maken. Met vrees wordt een emotie bedoeld, die ieder normaal mens onder vergelijkbare omstandigheden ook zou hebben (geobjectiveerd). Het oogmerk van de dader is gericht op het ontstaan van zo'n emotie, op het bang maken van het slachtoffer. De aan te jagen vrees is niet beperkt tot een bepaalde strekking, zoals vrees voor de veiligheid.

Op basis van de concrete feiten en omstandigheden van een geval zal moeten worden bepaald of sprake is van strafbare doxing. Bij een gedraging die vreesaanjagend is kan in dit verband bijvoorbeeld worden gedacht aan het aan een slachtoffer laten weten dat wordt beschikt over zeer persoonlijke gegevens van diegene of diens naasten, bijvoorbeeld de school van de kinderen en het

tijdstip waarop ze in de ochtend naar school gaan.

1.8 Ernstige overlast aandoen of ernstig hinderen in de uitoefening van ambt of beroep

De overlast of hinder moet ernstig zijn, van zodanige aard dat het slachtoffer hierdoor redelijkerwijs kan worden geacht ernstige overlast aan te worden gedaan of in de uitoefening van zijn ambt of beroep ernstig te worden gehinderd. Hiervan kan sprake zijn in die gevallen waarin een slachtoffer doordat zijn persoonsgegevens bekend zijn bij anderen zijn reguliere (privé)activiteiten of werkzaamheden niet meer ongestoord kan voortzetten, bijvoorbeeld omdat hij wordt lastiggevallen of omdat het risico dat dit gebeurt zeer groot is.

Op basis van de concrete feiten en omstandigheden van een geval zal moeten worden bepaald of sprake is van strafbare doxing. Van ernstige overlast kan bijvoorbeeld sprake zijn als een adres wordt gedeeld met de oproep aan velen om daar op een bepaald tijdstip te verzamelen met zoveel mogelijk hooibalen. Dat kan er immers toe leiden dat de betrokkene de woning niet meer (ongestoord) kan verlaten. Een gedraging die ernstige hinder in de uitoefening van de functie veroorzaakt is het publiceren van functieaanduidingen en foto's van personen die hun functie alleen in anonimiteit kunnen verrichten, zoals bij een undercoveragent het geval is.

Combinatie
Het is niet uitgesloten dat een gedraging zowel vreesaanjagend als ernstig overlastgevend is of ernstige hinder veroorzaakt. In het geval van de undercoveragent kan bijvoorbeeld ook sprake zijn van het aanjagen van vrees als hierdoor een dreiging kan ontstaan vanuit een bepaalde criminele groepering richting de agent.

Gerichte wil om anderen te intimideren
Bij gedragingen die niet voldoende ernstig zijn om vrees aan te jagen, ernstige overlast te veroorzaken of ernstig te hinderen in de uitoefening van ambt of beroep kan worden gedacht aan het voor de werklocatie aanspreken van een persoon met een publieke functie, een enkel irritant telefoontje of onaardig kaartje, of het eenmalig bestellen en bij het slachtoffer laten bezorgen van een ongewenst artikel. Dergelijke gedragingen kunnen vervelend zijn, maar daarbij zal niet bij voorbaat sprake behoeven te zijn van vrees, ernstige overlast of ernstige hinder in de uitoefening in ambt of beroep. Als de betrokkene zich persoonsgegevens verschaft of aan iemand anders persoonsgegevens van een ander stuurt, ten behoeve van het begaan van deze gedragingen, zal dat in die gevallen geen strafbare doxing opleveren.

In de omschrijving van het voor strafbaarheid vereiste oogmerk is een grens getrokken tussen gedragingen die naar de maatstaven van fatsoen als onbehoorlijk moeten worden beschouwd en gedragingen die vallen onder de voorgestelde strafbaarstelling. Strafwaardig zijn de gedragingen waarbij uit het oogmerk blijkt van een gerichte wil om anderen te intimideren. Daarvan hoeft nog geen sprake te zijn in gevallen van 'gewone' hinder en overlast. Of in een specifiek geval het oogmerk aanwezig is om iemand ernstige overlast aan te doen of iemand ernstig te hinderen in de uitoefening van ambt of beroep, zal moeten worden beoordeeld op basis van de omstandigheden die zich in dat geval voordoen.

Beperking van de vrijheid van meningsuiting
De strafbaarstelling betekent een beperking van de vrijheid van meningsuiting. Voor de beoordeling of

een beperking van de vrijheid van meningsuiting gerechtvaardigd is, is onder meer van belang of daartoe een dringende maatschappelijke noodzaak bestaat. In dit geval is de maatschappelijke noodzaak gelegen in de ingrijpende en schadelijke effecten die strafbare doxing kan hebben op het persoonlijke leven van slachtoffers (artikel 10 EVRM). Bij het gebruik van persoonsgegevens voor intimiderende doeleinden wordt een grens overschreden vanwege de ernstige inbreuk op het persoonlijk leven van slachtoffers. Een beperking kan alleen noodzakelijk zijn voor zover deze ook proportioneel is. Daarom gaat de voorgestelde strafbaarstelling niet verder dan strikt noodzakelijk en is deze gericht op gevallen waarin persoonsgegevens van anderen worden verzameld en verspreid met het oogmerk om een ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de uitoefening van ambt of beroep.

2. Verhouding tot andere strafbare feiten

De strafbepaling ziet op gedragingen die op grond van andere bepalingen tot datum van deze strafbepaling nog niet strafbaar waren, maar die door slachtoffers in vergelijkbare mate als angstaanjagend of ernstig overlast- of hinder gevend worden ervaren. Het is ook een delict dat opvolgend tot anderszins strafbaar gedrag kan leiden of samen met die feiten wordt begaan.

Bij **dwang** (artikel 284 Sr) wordt het slachtoffer gedwongen iets te doen, niet te doen of te dulden.
Bij **bedreiging** (artikel 285 Sr) wordt bedreigd met bepaalde ernstige misdrijven. Daarvan is geen sprake in het geval van strafbare doxing in de vorm van het in een appgroep vragen naar het adres van een bepaald persoon zodat diegene ‘de waarheid kan worden verteld’.
Bij **belaging (stalking)** (artikel 285b Sr) wordt stelselmatig inbreuk gemaakt op de persoonlijke levenssfeer van een ander.
Bij **afpersing** (artikel 317 Sr) dwingt iemand, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, een ander door geweld of bedreiging met geweld tot de afgifte van een goed, tot het aangaan van een schuld of het ter beschikking stellen van gegevens. Voor strafbare doxing is niet vereist dat iemand ergens toe wordt gedwongen en is het oogmerk niet gericht op wederrechtelijke bevoordeling.
Bij **aanbieden van medeplichtigheid** (artikel 133 Sr) is sprake van het in het openbaar aanbieden inlichtingen, gelegenheid of middelen te verschaffen om enig strafbaar feit te plegen
Bij **opruiing** (artikel 131 Sr) wordt in het openbaar opgeroepen tot het plegen van een strafbaar feit.
Bij **ambtsdwang** (artikel 179 Sr) gaat het om het uitoefenen van dwang tot het verrichten of doen afzien van een ambtsverrichting.

Van afpersing (artikel 317 Sr) is vereist dat iemand, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, een ander door geweld of bedreiging met geweld dwingt tot de afgifte van een goed, tot het aangaan van een schuld of het ter beschikking stellen van gegevens. Voor de vervulling van de delictsomschrijving van het voorgestelde artikel 285d Sr is niet vereist dat iemand ergens toe wordt gedwongen, maar dat de dader zich persoonsgegevens verschaft, deze verspreidt of anderszins ter beschikking stelt met de bedoeling angst, ernstige hinder of overlast te veroorzaken. Ook wat oogmerk betreft verschilt het voorgestelde artikel 285d Sr dus met artikel 317 Sr waar het in laatstgenoemd artikel is gericht op wederrechtelijke bevoordeling.

3. De strafbedreiging

3.1 Strafmaximum en strafverhogingsgrond

a. Het strafmaximum voor strafbare doxing is een gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
b. Als gepleegd tegen personen in een bepaalde hoedanigheid - namelijk die van

- minister,
- staatssecretaris,
- commissaris van de Koning,
- gedeputeerde,
- burgemeester,
- wethouder,
- lid van een algemeen vertegenwoordigend orgaan,
- rechterlijk ambtenaar,
- advocaat,
- journalist of publicist in het kader van nieuwsgaring,
- ambtenaar van politie of buitengewoon opsporingsambtenaar,

wordt de op het feit gestelde gevangenisstraf met een derde verhoogd. Het strafmaximum bedraagt daardoor in die gevallen maximaal twee jaar en acht maanden.

3.2 Verhoogde strafeis

Het OM verhoogd de strafeis bij agressie en geweld tegen werknemers met een publieke taak en andere functionarissen werkzaam in het publieke domein (zie paragraaf 6 van de OM-Aanwijzing kader voor strafvordering meerderjarigen (2019A003); ook ten aanzien van publieke functies die niet in de strafverhogingsgrond zijn opgenomen.

3.3 Taakstrafverbod

Er is bij doxing geen sprake van een taakstrafverbod (artikel 22b Sr). Er is geen sprake van een misdrijf dat een ernstige inbreuk op de lichamelijke integriteit van het slachtoffer ten gevolge heeft gehad.

4. Inzet van dwangmiddelen

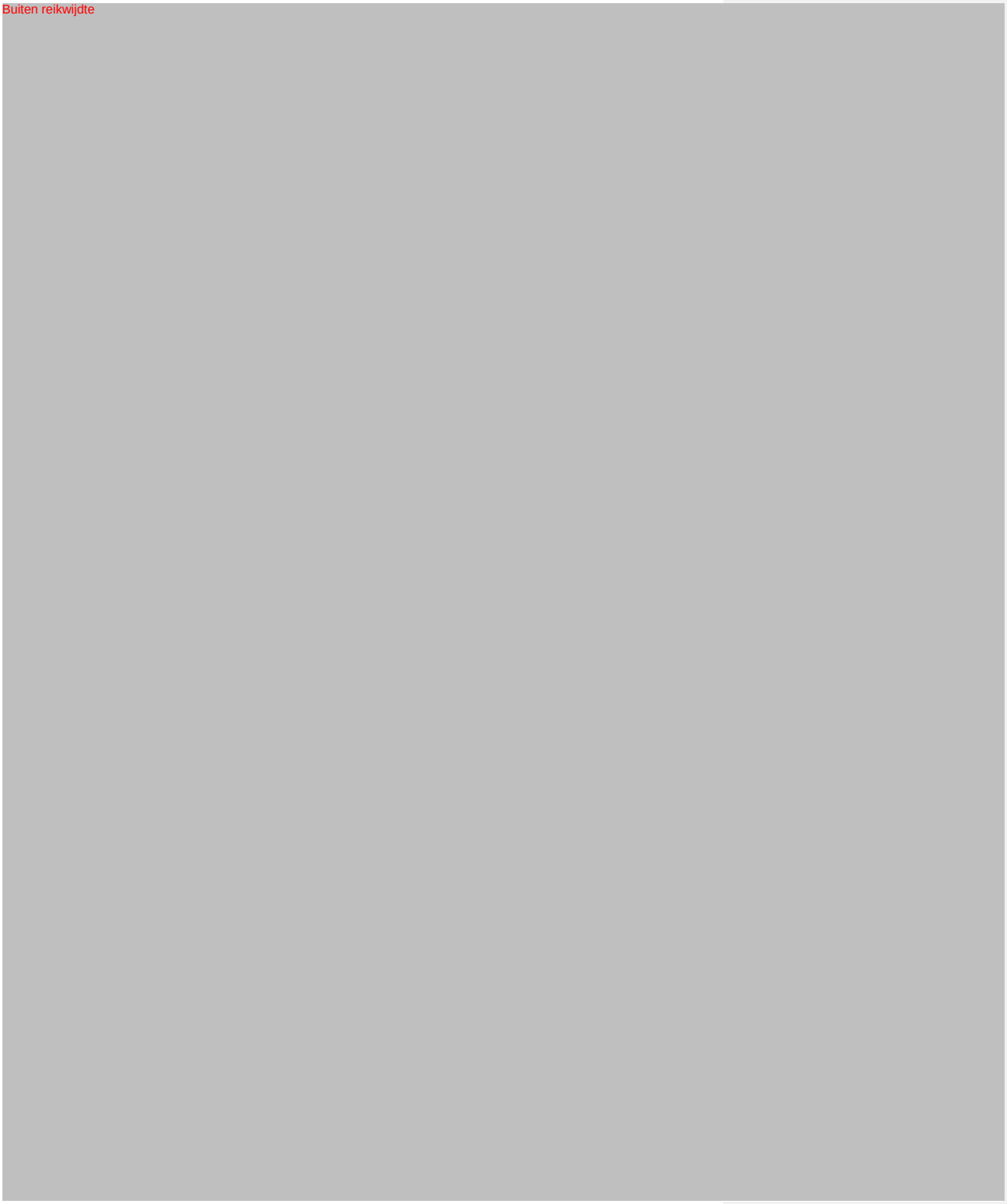
Artikel 67 Sv is aangevuld met het delict strafbare doxing, zijnde een misdrijf waarvoor een bevel tot voorlopige hechtenis kan worden gegeven. Daarmee kunnen strafvorderlijke dwangmiddelen - als de aanhouding buiten heterdaad, inverzekeringstelling en de inzet van bijzondere opsporingsbevoegdheden - zoals het vorderen van gegevens - worden toegepast. Dit is in het bijzonder van belang in een fase waarin de identiteit van de verdachte nog niet bekend is.

Het snel kunnen identificeren kan in bepaalde gevallen ook leiden tot een voortvarende en effectievere interventie, bijvoorbeeld door met de verdachte een bemiddelings- of stopgesprek te voeren in het geval van minderjarige verdachten.

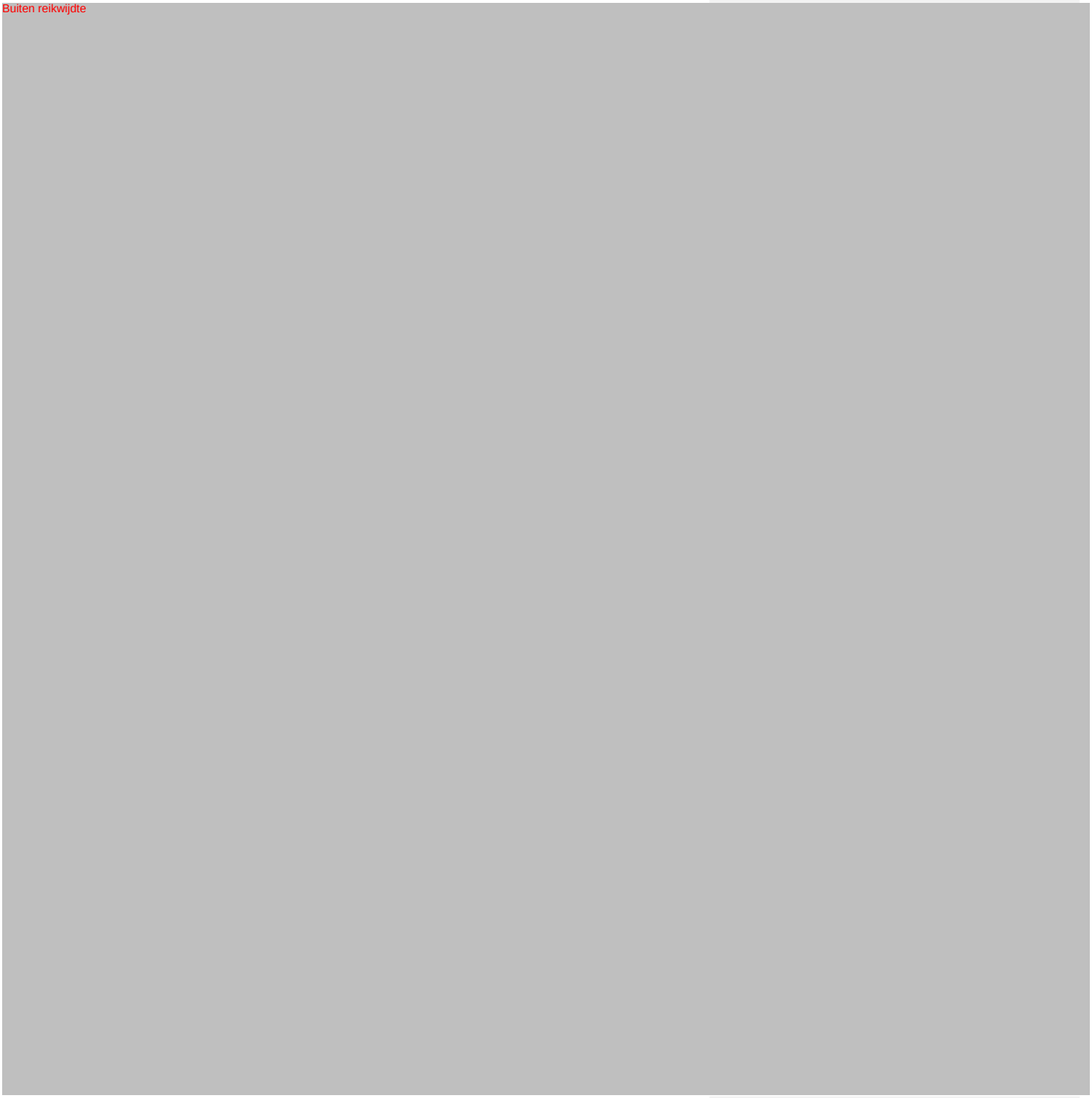
Werkgroep doxing politie en dgpenv

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


Buiten reikwijdte

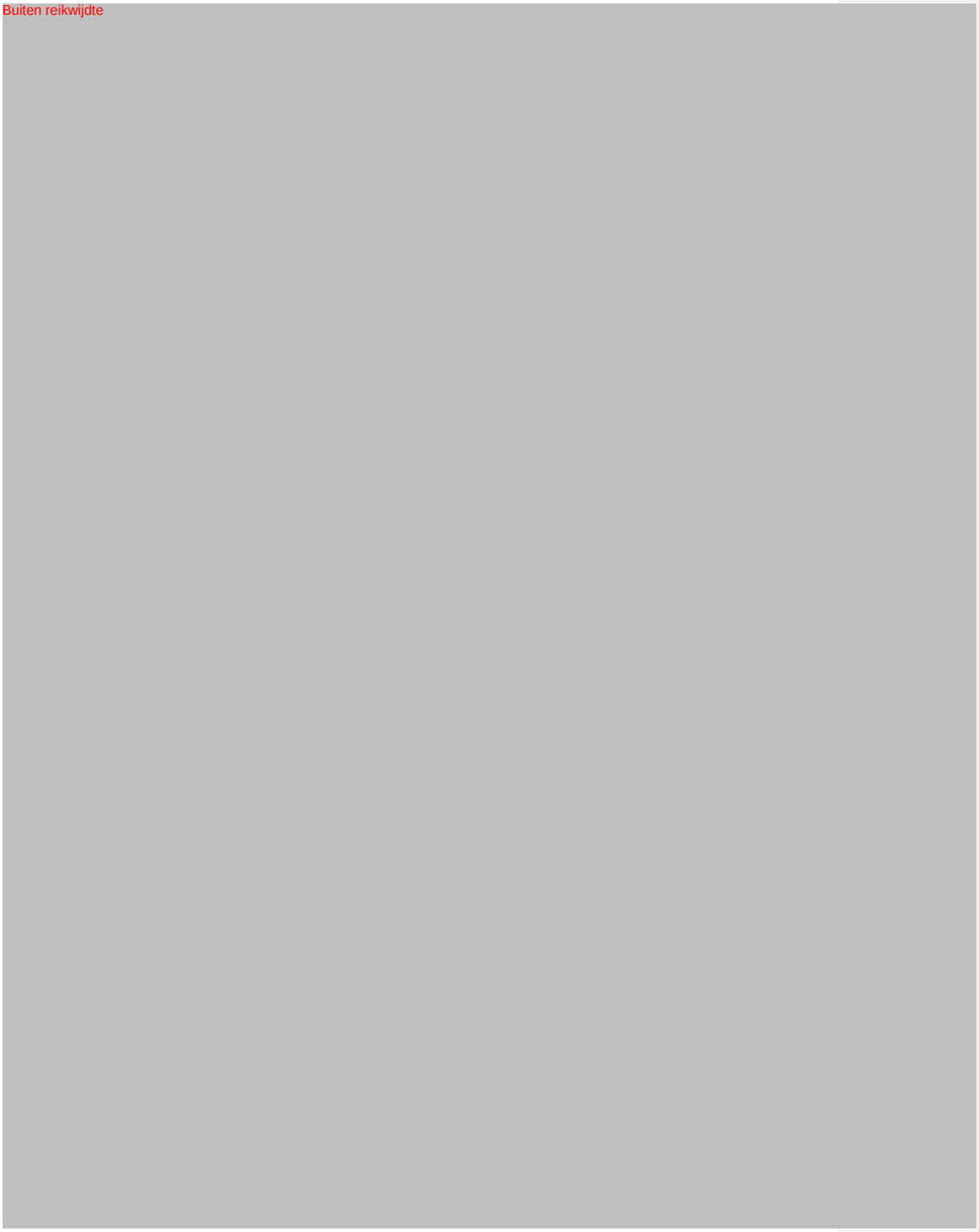

Buiten reikwijdte

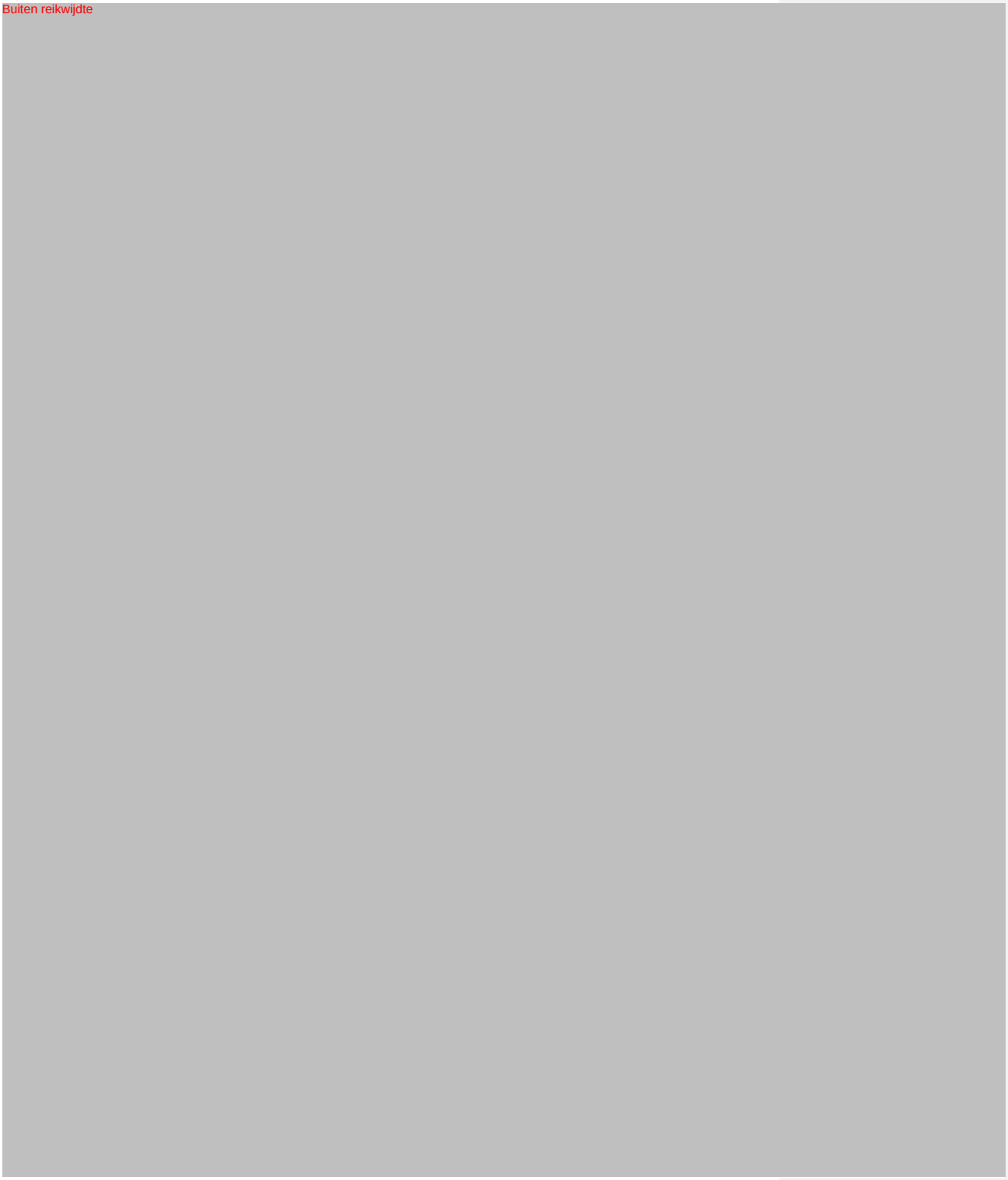
Buiten reikwijdte

	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	

Buiten reikwijdte

Buiten reikwijdte


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.	Buiten reikwijdte		
			Niet onder reikwijdte
2.	Buiten reikwijdte		
a.			Niet onder reikwijdte

c.	Niet onder reikwijdte		
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):***	-	

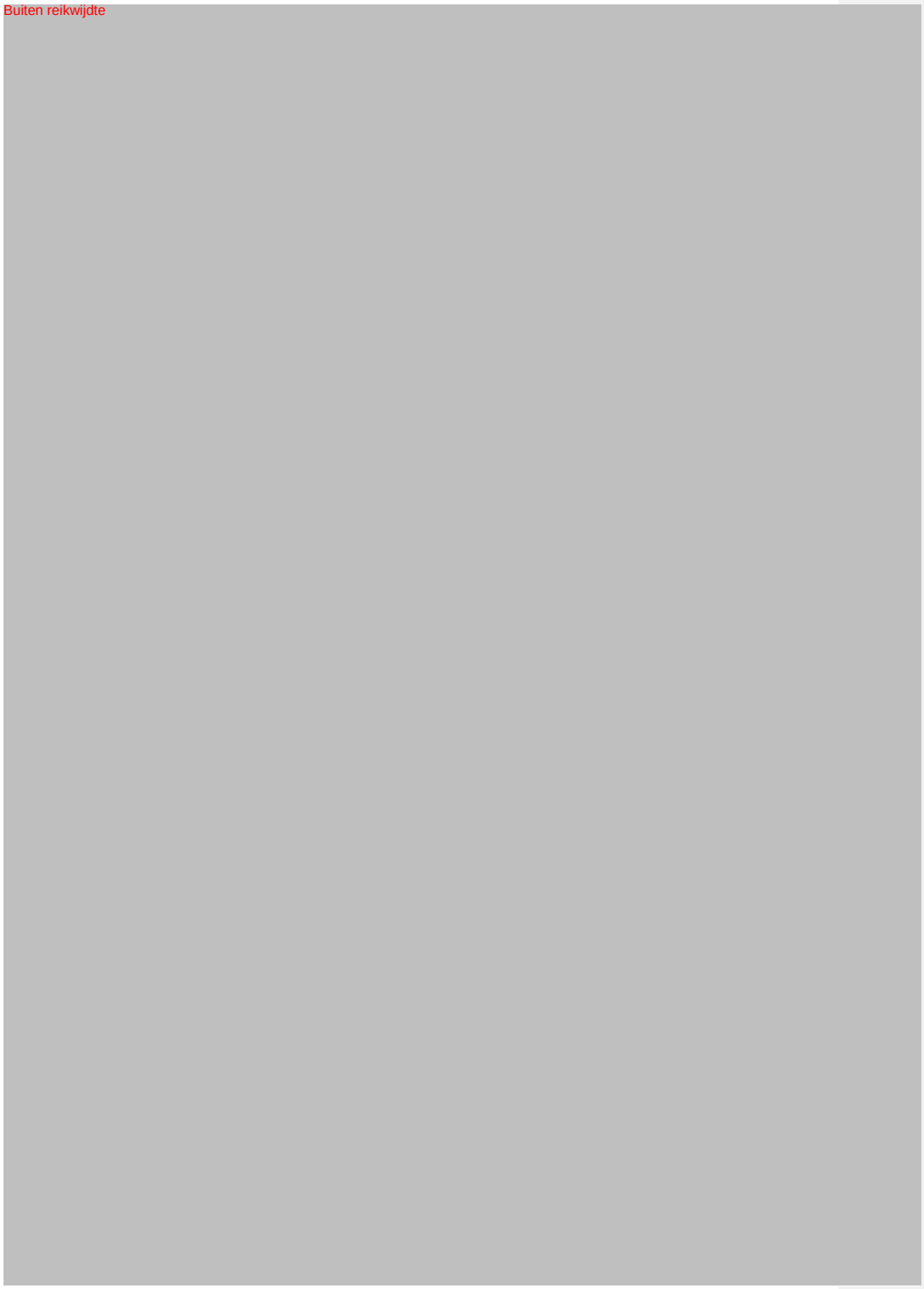
a.	Strafbaarstelling doxing		Zie onder punt 1 hierboven.
-	-	-	
b.	Verplichting tot blurren van gezichten politiemensen op foto's en filmpjes sociale media.	WG Doxing?	Heroverweging standpunt wetgeving tov blurbrief 2017.Zie voorstel werkgroep onder punt 2 hierboven.
-	-	-	
c.	Verwijderen van filmpjes 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		
-	-	-	
-	-	-	

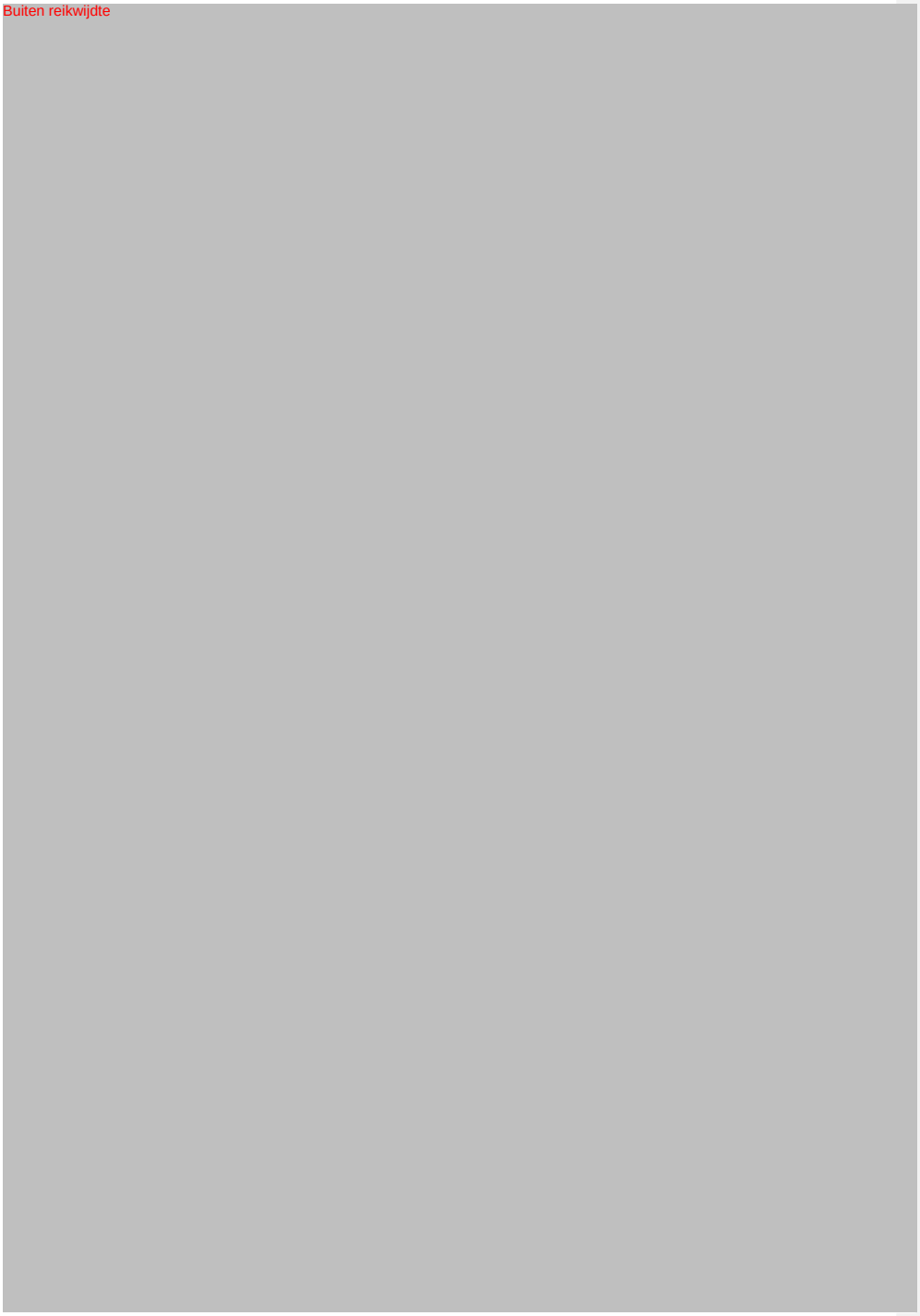
c.			Niet onder reikwijdte

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

Inleiding

Op 20 juli 2017 heeft de Minister van Justitie met een brief aan de Tweede Kamer gereageerd op de wens tot het instellen van een blurgebod van politieambtenaren (brief beelden van politieagenten verspreiden en verspreiden beelden door politie (KS 29628, nr. 724). In de brief is onderbouwd weergegeven dat – nu samengevat in iets andere woorden dan de brief - de noodzaak voor een algemeen of beperkt blurgebod voor politieagenten onvoldoende kan worden aangetoond. In de brief zijn een aantal juridische en niet juridische mogelijkheden beschreven om op te treden tegen enerzijds de aantasting van de persoonlijke levenssfeer van de betrokken politieagent door met name het publiceren van beeldmateriaal en anderzijds het voorkomen dat de politie haar taak tot handhaving van de rechtsorde niet meer ongehinderd kan uitvoeren.

Vanuit de WGRRBD is recent verzocht of een overzicht is te geven van de huidige wetgeving rondom het filmen van politieagenten en de relevante ontwikkelingen daarin. Dit overzicht geeft een algemeen beeld.

Samenvatting:

Strafrechtelijk

De eerste vraag was in hoeverre het filmen van mensen (waaronder politieambtenaren) strafrechtelijk verboden is.

De rode lijn was: Strafrechtelijk gezien mag filmen (in beginsel), zeker als dit openlijk gebeurt. Publicatie mag niet leiden tot strafbare feiten, zoals bedreiging etc. Dit kan alleen achteraf getoetst worden (recht op vrijheid van meningsuiting).

Deze rode lijn zal worden gewijzigd door de strafbaarstelling van doxing: in het concept wetsvoorstel dat nu bij de Raad van State ligt ter beoordeling, zal het filmen en het verspreiden (publiceren) van persoonsgegevens met – kortgezegd - een 'intimiderend oogmerk' worden verboden. Hierbij wordt indirect ook de vrijheid van meningsuiting beschermd, doordat mensen niet meer op deze wijze straffeloos kan worden getracht te mond te snoeren.
Het is denkbaar dat het al dan onherkenbaar in beeld brengen (blurren e.d.) van de persoon die gefilmd is bij publicatie een rol kan gaan spelen bij de strafrechtelijke beoordeling van het oogmerk. Dit is echter sterk afhankelijk van de context en zal per geval (achteraf) kunnen worden beoordeeld.

Bijgevoegd is een overzicht van relevante strafrechtelijke bepalingen.

Het verwijderen van berichten in het kader van de strafrechtelijke aanpak is mogelijk voor bepaalde gevallen met toestemming van de rechter-commissaris, waar de weg van de vrijwillige verwijdering geen uitkomst kan bieden.

Overig

De (U)AVG (opvolger van de Wbp) is van toepassing op bepaalde verwerkingen van persoonsgegevens op het internet, waaronder verwerkingen van burgers die niet onder de zogenaamde huishoudelijke exceptie vallen. Iedere verwerking die onder deze wet valt moet voldoen aan de beginselen van gegevensverwerking, neergelegd in artikel 5 AVG. Dit geldt dus ook voor publicisten (burgers en journalisten) die zich op de zogenaamde journalistieke exceptie kunnen beroepen (zie artikel 43 AVG). Het eerste beginsel stelt dat de wijze van verwerking ten aanzien van de betrokken rechtmatig, behoorlijk en transparant moet zijn. De andere beginselen geven aan dat de uitgangspunten van gegevensbescherming zijn: doelbinding; minimale gegevensverwerking, opslagbeperking; juistheid; integriteit en vertrouwelijkheid en opslagbeperking en verantwoordingsplicht. Onder de AVG is het met intimiderend doel verwerken van gegevens geen rechtmatig verwerkingsgrondslag (Zie artikel 6 AVG). Indien een verwerking van persoonsgegevens strijdig is met de (beginselen van) AVG, kan de betrokkene zich wenden tot de toezichthouder, in Nederland de Autoriteit Persoonsgegevens.

Het kan daarnaast zo zijn dat de verwerking een onrechtmatige daad jegens de betrokkene kan opleveren gepleegd door de plaatser of door het platform, waartegen de gang naar de burgerlijke rechter openstaat. Hierbij dient een betrokkene indien deze kan worden geïdentificeerd eerst iemand op grond van artikel 6:162 BW te sommeren berichten te

Met opmerkingen I 5.1.2.e Zag de brief alleen op beeldopnames in de vorm van film of ook van foto's?

verwijderen en verwijderd te houden. Indien hieraan geen gehoor wordt gegeven, kan de benadeelde de civiele rechter vragen dit met het opleggen van een verbod en gebod af te dwingen. Dit kan in voorkomend geval ook door de korpschef van de politie in hoedanigheid van werkgever in het geval door de publicatie de medewerker diens taken tot handhaving van de rechtsorde niet meer ongehinderd kan uitvoeren (bijv. bij vormen van afgeschermd werken).~~.~~ De rechter kan daarbij ook ~~ook~~ bepalen dat iemand moet stoppen met het publiceren van soortgelijke berichten (ECLI:NL:RBDHA:2021:6769).

Tot slot speelt in het kader van het openbare orde-recht momenteel de discussie of een burgemeester een zogeheten 'online-gebiedsverbod' (last onder dwangsom) zou kunnen~~mag~~ opleggen aan iemand die opruiende berichten verstuurt (Zie ~~oa~~o.a. ~~k~~Kamervragen over het bericht 'Jongen (17) krijgt allereerste 'online gebiedsverbod' in Nederland, maar wat betekent dat eigenlijk?').

Met opmerkingen 5.1.2.e : Uitspraak Bodegraven. Is er al een bodem procedure geweest?

Toelichting strafrechtelijk kader

Filmen

	Bepaling	Belangrijkste elementen
Wijze en waar filmen		
139 f Sr (geen vh-feit)	Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.	*Heimelijk* te filmen of fotograferen op niet-openbare plaatsen
441b Sr (vh-feit)	Met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie wordt gestraft hij die, gebruik makende van een daartoe aangebracht technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, van een persoon, aanwezig op een voor het publiek toegankelijke plaats, wederrechtelijk een afbeelding vervaardigt.	Verboden te filmen met een niet duidelijk kenbare *vaste* camera in de openbare ruimte, tenzij
Doel filmen		
Doxing-bepaling (VH-feit) Tekst consultatieversie wetsvoorstel (de wezenlijke kern van het wetsvoorstel wordt	Artikel 285d (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	

Met opmerkingen 5.1.2.e 46 Sr nog vermelden? 5.2.1 .

Met opmerkingen 5.1.2.e Zeker de poging of de uitlokking ergens wel vermelden. Een oproep om deze handelingen te doen is dat kort gezegd toch, (vgl. bij opruiing in zaak 5.1.2.e)?

niet gewijzigd in de Raad van Staat-versie).	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, '.	
141a Sr	Hij die opzettelijk gelegenheid, middelen of inlichtingen verschaft tot het plegen van geweld tegen personen of goederen wordt gestraft met en gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie	

Met opmerkingen 5.1.2.e is dit nodig hier? je hebt al vh feit linksboven staan

Beeldmateriaal verstrekken aan derde: verstrekking van strafbare inlichtingen		
Deelnemingsvorm: uitlokking strafbaar feit (47 Sr)	Oa opzettelijk verschaffen inlichtingen om opzettelijk het strafbare feit uit te lokken	
Deelnemingsvorm medeplichtigheid misdrijf (48 Sr)	Oa opzettelijk verschaffen inlichtingen tot het plegen van het misdrijf	

Beeldmateriaal voorhanden hebben wetende dat het door een strafbaar feit is verkregen		
139g Sr (dataheling) **(vh-feit)**	Art. 139g. lid 1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die niet-openbare gegevens: **a.**verwerft of voorhanden heeft, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van deze gegevens wist of redelijkerwijs had moeten	

	vermoeden dat deze door misdrijf zijn verkregen; **b.**ter beschikking van een ander stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt, terwijl hij weet of redelijkerwijs moet vermoeden dat het door misdrijf verkregen gegevens betreft. **Lid 2** Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het verwerven, voorhanden hebben, ter beschikkingstellen, bekendmaken of gebruik van de gegevens, bedoeld in het eerste lid, vereiste.	

Publiceren (mn uitingsdelicten)

285 Sr (bedreiging) (vh-feit)		
261/262 Sr (smaad en laster) **(geen vh-feit)**		
266/267 Sr (belediging) **(geen vh-feit)**		
284 Sr (dwang) (lid 1 vh-feit)		
179 Sr (ambtsdwang) (vh-feit)		
131 en 132 Sr (opruiing) (vh-feit)		
318 Sr (afdreiging) (vh-feit)		
317 Sr (afpersing) (vh-feit)		
Initiatief voorstel strafbaar stellen van publicatie van beelden van slachtoffer		Stand van zaken?

Indirect: Gedrag bij filmen (oa hinder)		

184 Sr (geen vh-feit)	Artikel 184. Lid 1. Hij die opzettelijk niet voldoet aan een bevel of een vordering, krachtens wettelijk voorschrift gedaan door een ambtenaar met de uitoefening van enig toezicht belast of door een ambtenaar belast met of bevoegd verklaard tot het opsporen of onderzoeken van strafbare feiten, alsmede hij die opzettelijk enige handeling, door een van die ambtenaren ondernomen ter uitvoering van enig wettelijk voorschrift, belet, belemmert of verijdelt, wordt gestraft met gevangenisstraf van ten hoogste drie maanden of geldboete van de tweede categorie. Lid 2. Met de in het eerste gedeelte van het vorige lid bedoelde ambtenaar wordt gelijkgesteld ieder die, krachtens wettelijk voorschrift, voortdurend of tijdelijk met enige openbare dienst is belast. **Lid 3** Met een vordering of handeling als bedoeld in het eerste lid wordt gelijkgesteld een vordering of handeling van de schipper of gezagvoerder van een luchtvaartuig die een bevoegdheid uitoefent of een verplichting vervult, welke hem als zodanig is toegekend of opgelegd bij een bepaling van het Wetboek van Strafvordering. Onder schipper wordt begrepen hij die het hoogste gezag uitoefent op een overeenkomstig artikel 136*a*, tweede lid, van het Wetboek van Strafvordering aangewezen installatie. **Lid 4** Indien tijdens het plegen van het misdrijf nog geen twee jaren zijn verlopen sedert een vroegere veroordeling van de schuldige wegens gelijk misdrijf onherroepelijk is geworden, kan de gevangenisstraf met een derde worden verhoogd.	Filmen mag niet belemmeren bij rechtmatige uitoefening van een wettelijke taak
441a Sr (geen vh-feit)	Hij die openlijk of door verspreiding van enig geschrift ongevraagd een voorwerp als verkrijgbaar dan wel als bij hem voorhanden aanwijst en daarbij de	

	aandacht vestigt op de geschiktheid daarvan als technisch hulpmiddel voor het heimelijk afluisteren, aftappen of opnemen van gesprekken, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk of als onderdeel van zulk een hulpmiddel, wordt gestraft met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie.	
426bis Sr (overtreding) (geen vh-feit)	Hij die wederrechtelijk op de openbare weg een ander in zijn vrijheid van beweging belemmert of met een of meer anderen zich aan een ander tegen diens uitdrukkelijk verklaarde wil blijft opdringen of hem op hinderlijke wijze blijft volgen, wordt gestraft met hechtenis van ten hoogste een maand of geldboete van de tweede categorie.	Op de openbare weg beperken van vrij beweging van een ander Met een of meer anderen zich aan iemand blijven opdringen of hinderlijk volgen op de openbare weg
426ter Sr (overtreding) (geen vh-feit)	Hij die wederrechtelijk een hulpverlener gedurende de uitoefening van zijn beroep in zijn vrijheid van beweging belemmert of met en of meer anderen zich aan hem tegen zijn uitdrukkelijk verklaarde wil blijft opdringen of hem op hinderlijke wijze blijft volgen wordt gestraft met hechtenis van ten hoogste drie maanden op geldboete van de derde categorie.	
Bepalingen uit de APV		Model-APV: 2:47 Hinderlijk gedrag op openbare plaatsen; 2:50 Hinderlijk gedrag in voor publiek toegankelijke ruimten Sommige gemeenten hebben ook bepalingen ~~tav~~t.a.v virtuele publieke ruimte. De vraag is wel of dat kan (vrijheid van meningsuiting kan alleen worden beperkt door wet in formele zin (7 GW; 10 EVRM)
Indirect: Overtreden voorwaarden in het kader van het strafrecht opgelegd gebiedsverbod of locatieverbod.		Indirecte aanpak: je mag daar niet zijn, dus ook niet om te filmen.

Indirect: Overtreden voorwaarden in het kader van het	ECLI:RBMNE:2021:4854 Rechter legt als bijzondere voorwaarde bij voorwaardelijke straf ex artikel 14c lid 2 onder 14	Traject DGSenB/DGPenV/OM/politie/reclassering?

strafrecht opgelegd publicatieverbod?	op: haar Twitteraccount, haar websites en andere openbare voor haar toegankelijke digitale media, waarin zij schadelijke mededelingen doet over X en Y schonen en geschoond te houden van deze mededelingen. Dit kan overigens niet dadelijk uitvoerbaar worden verklaard op grond van de eisen van de wet. (NB OvJ had maatregel ex art. 38v gevorderd, maar dat is door de rechter nadrukkelijk niet gevolgd). (Ook mogelijk in kader van bijzondere voorwaarden bij schorsing vhs (artikel 80 Sv?). 'Toezicht' bestaat eruit dat de politie binnen de kaders van de bevoegdheden die haar zijn verleend tbv de politietaak of opnieuw een strafbaar feit wordt gepleegd? Of ook nog andere relevante bepalingen? (executiedeel Sv?)	

VH Feit betekent bijvoorbeeld de zogeheten BOB-middelen inzetbaar bij:

67 lid 1 Sv	Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van: a.een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld; **b.**een der misdrijven omschreven in de artikelen 132, 138a, 138aa, 138ab, 138b, 138c, 139c, 139d, eerste en tweede lid, artikel 139h, eerste en tweede lid, 139g, 140, tweede lid, 141a, 137c, tweede lid, 137d, eerste lid, 137e, tweede lid, 137g, tweede lid, 151, 184a, 254a, 248d, 248e, 272, 284, eerste lid, 285, eerste lid, 285b, 285c, 285d(nieuw), 300, eerste lid, 321, 326c, tweede lid, 326d, 340, 342, 344a, 344b, 347, eerste lid, 350, 350a, 350c, 350d351, 395, 417bis, 420bis.1, 420quater en 420quater.1 van het Wetboek van Strafrecht;

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]

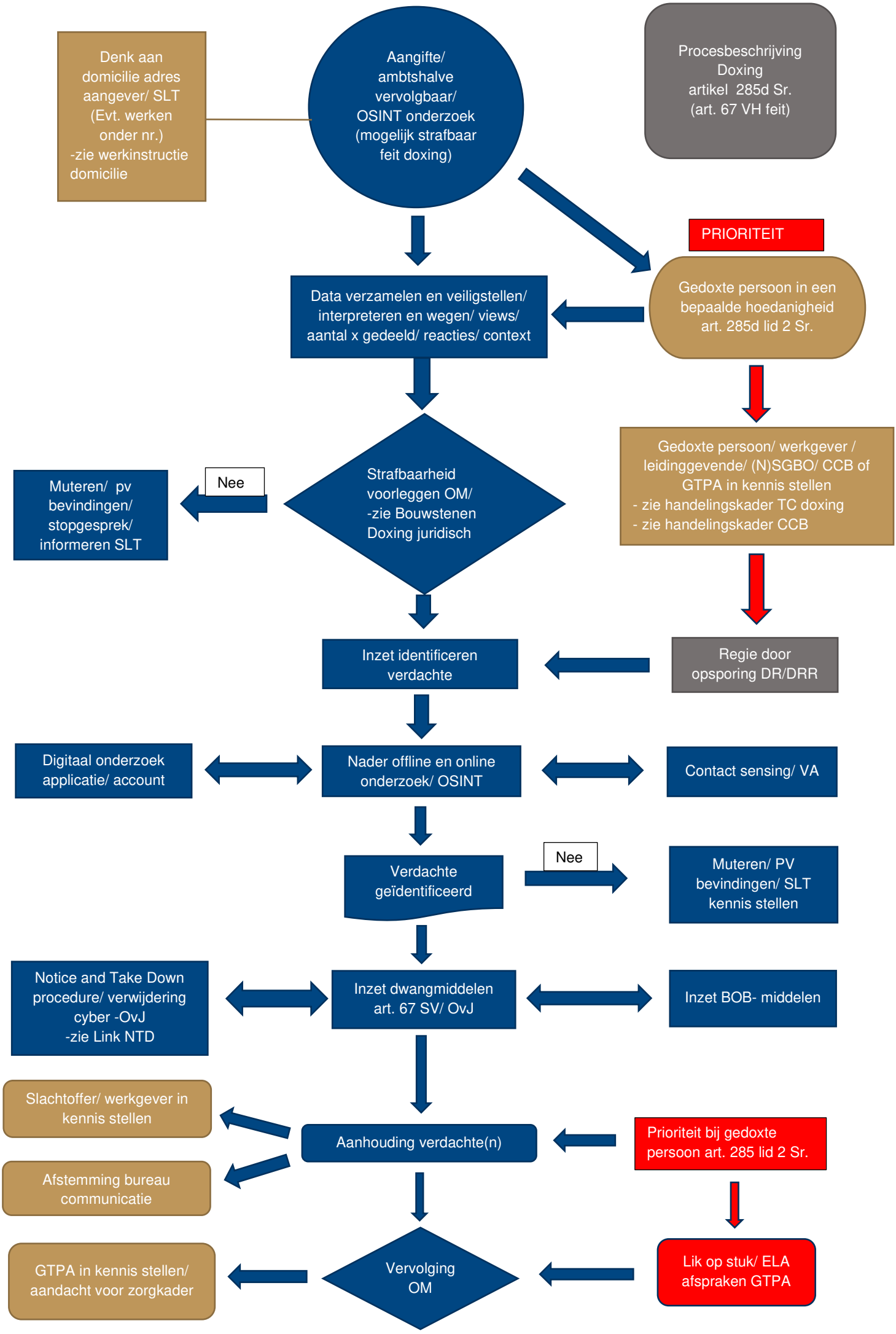
Doxing in deze casus is vanuit het demonstratiemilieu doelgericht ingezet als instrumenteel intimidatiemiddel. 5.1.2.e [redacted]

Buiten reikwijdte

[redacted]

5.2.1

.


Denk aan domicilie adres aangever/ SLT (Evt. werken onder nr.) -zie werkinstructie domicilie
Aangifte/ ambtshalve vervolgbaar/ OSINT onderzoek (mogelijk strafbaar feit doxing)
Procesbeschrijving Doxing artikel 285d Sr. (art. 67 VH feit)
PRIORITEIT
Gedoxte persoon in een bepaalde hoedanigheid art. 285d lid 2 Sr.
Data verzamelen en veiligstellen/ interpreteren en wegen/ views/ aantal x gedeeld/ reacties/ context
Gedoxte persoon/ werkgever / leidinggevende/ (N)SGBO/ CCB of GTPA in kennis stellen
- zie handelingskader TC doxing
- zie handelingskader CCB
Strafbaarheid voorleggen OM/ -zie Bouwstenen Doxing juridisch
Nee
Muteren/ pv bevindingen/ stopgesprek/ informeren SLT
Regie door opsporing DR/DRR
Inzet identificeren verdachte
Digitaal onderzoek applicatie/ account
Nader offline en online onderzoek/ OSINT
Contact sensing/ VA
Verdachte geïdentificeerd
Nee
Muteren/ PV bevindingen/ SLT kennis stellen
Notice and Take Down procedure/ verwijdering cyber -OvJ -zie Link NTD
Inzet dwangmiddelen art. 67 SV/ OvJ
Inzet BOB- middelen
Slachtoffer/ werkgever in kennis stellen
Aanhouding verdachte(n)
Prioriteit bij gedoxte persoon art. 285 lid 2 Sr.
Afstemming bureau communicatie
GTPA in kennis stellen/ aandacht voor zorgkader
Vervolging OM
Lik op stuk/ ELA afspraken GTPA

FACTSHEET DOXING

Sinds 1 januari 2024 is in Nederland de strafbaarstelling *'het gebruik van persoonsgegevens voor intimiderende doeleinden'* van kracht, in de volksmond **doxing** genoemd.

Artikel 285d Sr Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden
1. Degene die zich **persoonsgegevens** van een **ander of** een **derde verschaft**, deze gegevens **verspreidt** of **anderszins ter beschikking stelt** met het **oogmerk** om die ander **vrees aan te jagen** dan wel aan **te laten** jagen, **ernstige overlast aan te doen** dan wel aan te **laten doen** of hem in de **uitoefening van zijn ambt of beroep ernstig te hinderen** dan wel ernstig te **laten hinderen**, wordt gestraft met gevangenisstraf van ten hoogste twee jaar of geldboete van de vierde categorie.
2. Indien het feit, omschreven in het eerste lid wordt gepleegd tegen een persoon in diens hoedanigheid van **Minister, Staatssecretaris, commissaris van de Koning, gedeputeerde, burgemeester, wethouder, lid van een algemeen vertegenwoordigend orgaan, rechterlijk ambtenaar, advocaat, journalist of publicist in het kader van nieuwsgaring, ambtenaar van politie of buitengewoon opsporingsambtenaar** wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.
***Artikel 67 Sv**: het misdrijf wordt als **'VH-feit'** aan dit artikel toegevoegd, zodat bevoegdheden zoals het vorderen van gegevens of bevel ontoegankelijk maken gegevens kunnen worden toegepast.*

Wat is doxing:
Kortgezegd betekent dit het met kwade bedoelingen **verzamelen**, (verder) **verspreiden** of **distribueren** van **persoonsgegevens** van een ander, of een derde **(familieleden!),** zoals: **naam, woon-of werkadres, telefoonnummer, emailadres of foto**. Doxing speelt zich overwegend online af op sociale platformen en neemt soms zeer omvangrijke vormen aan. Doxing kan leiden tot pesterijen, haatberichten en intimidatie en kent klachten als stress, angst, depressiviteit, eenzaamheid en suïcidale gedachten. Online achtergebleven content is extreem lastig te verwijderen waardoor slachtoffers een langdurige confrontatie kunnen ervaren. Doxing gaat vaak gepaard met andere strafbare gedragingen zoals bedreiging, opruiing, belediging of smaad. Doxing is per definitie persoonlijk van aard en kan een sterk ontregelend effect op de privésituatie van het slachtoffer hebben.

Wat is strafbaar:
Het verzamelen, verspreiden of ter beschikking stellen van persoonsgegevens met het oogmerk om een ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of hem in de uitoefening van zijn ambt ernstig te (laten) hinderen.
Voorbeelden van doxing zijn:

- Het delen van namen en telefoonnummers van vrouwen in wraakpornogroepen op Telegram, waarna soms wel honderden haatberichten of intimiderende telefoontjes volgen,
- Het publiceren van het woonadres van een politicus met de oproep hem/haar thuis op te zoeken en angst aan te jagen,
- Het delen van een foto van een politieagent met de oproep hem of haar thuis op te zoeken.

Belangrijk!
De bedoeling - het oogmerk van de dader - moet gericht zijn op het aanjagen van vrees, ernstige overlast of ernstige hinder in diens beroepsuitoefening. Het enkel (verder) verspreiden van bijvoorbeeld beeldmateriaal van politiemensen is dus géén doxing. Soms blijkt deze opzet duidelijk uit het verstuurde bericht. Soms is de opzet niet expliciet aanwezig maar blijkt dit uit de context waaronder het bericht is gepubliceerd.

Wat is doxing niet?
De kwade bedoeling van degene die de persoonsgegevens deelt bepaalt de strafbaarheid van de gedraging. Alleen het delen van persoonsgegevens zoals een naam, een foto of emailadres is dus niet strafbaar en levert **geen doxing op.** Het filmen van politieagenten / politieoptreden en dit online delen of verder verspreiden is eveneens geen doxing.

De rol van de politie

Generieke doxing
De politie heeft een rol als dienstverlener voor iedereen die informatie zoekt, melding wil maken of aangifte wil doen van doxing. Klik **hier** voor de werkinstructie voor I&S, de GGP en Opsporing.

Politiedoxing
De politie heeft vanuit goed werkgeverschap óók een rol in situaties van politiedoxing. Word jij gedoxt? Informeer dan zo spoedig mogelijk jouw leidinggevende en bekijk het '**Handelingskader politiedoxing voor leidinggevenden'.**

Maatwerk
Elk geval van doxing verloopt anders en dit vraagt om maatwerk. In het ene geval worden de persoonsgegevens op kleine schaal gedeeld. In een ander geval is sprake van grote media-aandacht en worden persoonsgegevens op enorme schaal via verschillende sociale platformen verspreid. Soms is een stopgesprek voldoende, soms heeft een opsporingsonderzoek de voorkeur. De wens van het slachtoffer is hierbij belangrijk, evenals de noodzakelijke aanknopingspunten voor de politie om een verdachte op te sporen.

Intake & Service: aandachtspunten aangifteproces: bekijk de Q&A in de servicemodule!

- Doxing ligt politiek gevoelig; wees je hiervan bewust, zeker wanneer de met name genoemde beroepsgroepen slachtoffer zijn.
- Doxing kán een veiligheidsrisico opleveren; hoe groter de online (media)storm wordt hoe meer risico een slachtoffer loopt. Monitor het situatieverloop dus goed!
- I.h.k.v. opsporing: vraag zoveel mogelijk relevante digitale informatie uit over het door de doxer gebruikte account of communicatiemiddel.

Let op!
De **persoonlijke veiligheid** van de gedoxte persoon kán gevaar lopen, bijvoorbeeld als een woonadres is gedeeld; beoordeel dus altijd per casus of sprake is van een (concreet) veiligheidsrisico. De context van een casus is hierbij belangrijk, maar ook de actualiteit en concreetheid van de dreiging.

Persoonlijke veiligheid en maatregelen
In Nederland is eenieder in eerste instantie zelf verantwoordelijk voor zijn/haar veiligheid. Personen kunnen daarbij rekenen op hulp van organisaties en netwerken waartoe zij behoren, zoals bijvoorbeeld een werkgever ingeval van doxing wegens een relatie met de beroepsuitoefening. Er ontstaat pas een verantwoordelijkheid voor de overheid als personen en organisaties op eigen kracht geen weerstand kunnen bieden aan een dreiging. **Tip:** wanneer een doxingsituatie speelt rond personen als omschreven in het 2e lid van artikel 285d, bespreek dan met het slachtoffer welke afspraken gelden voor hun organisatie of taakveld ten aanzien van dreiging.

Soms valt een casus met een concrete en/of ernstige bedreiging niet onder de hierboven omschreven uitgangspunten. In dit geval kan je overleg plegen met de contactpersonen van de vakgroep Bewaken en Beveiligen binnen jouw Eenheid.

Digibewust:
Wist je dat wij als politiemedewerkers zelf het nodige kunnen doen om de kans op doxing kleiner te maken? Denk hierbij aan het afschermen van jouw socials en wees terughoudend met het delen van persoonlijke informatie online. Kijk op DIGIBEWUST **(link toevoegen)** voor tips en advies.

Verwijderen van gegevens van sociale platformen

Generieke doxing
Iedereen kan een online platform verzoeken om een bericht te laten verwijderen, bijvoorbeeld als sprake is van schending van de geldende richtlijnen. De politie kan slachtoffers van doxing voor informatie en advies verwijzen naar **https://noticeandtakedowncode.nl/ en www.helpwanted.nl.**

Let op! Als een burger aangifte doet maar óók zelfstandig een verwijderverzoek indient dan bestaat de kans dat de content is verwijderd, nog vóórdat dit in het belang van opsporing is veiliggesteld. Maak hierover met elke aangever dus altijd duidelijke afspraken.

Politiedoxing en specifieke beroepsgroepen
Wanneer politieagenten en de beroepsgroep uit artikel 285d, 2e lid worden gedoxt, dan geldt een interne NTD-procedure.

De afdeling 5.1 2 e van de Landelijke Eenheid staat in goed contact met sociale media als Buiten reikwijdte en anderen. Opgemaakte verwijderverzoeken worden door de medewerkers van 5.1.2.e rechtstreeks met het betrokken platform gedeeld.

Klik hier voor deze interne **NTD-procedure** en het aanvraagformulier.

Landelijke werkafspraak!
Het is belangrijk om ieder Notice and Takedown verzoek voor te leggen aan het OM. Bespreek dus **altijd** met de cyber-OvJ van jouw eenheid de inzet van dit middel: de spoedige verwijdering van online content kan namelijk botsen met het opsporingsbelang.

Op 20 juli 2017 heeft de Minister van Justitie met een brief aan de Tweede Kamer gereageerd op de wens tot het instellen van een blurgebod van politieambtenaren.

Vanuit de WGRRBD is recent verzocht of ~~aan te geven~~ een overzicht is te geven ~~analyse te maken~~ van de huidige wetgeving en de relevante ontwikkelingen daarin. Dit overzicht geeft een algemeen beeld

Samenvatting:

Strafrechtelijk

De eerste vraag was in hoeverre het filmen van mensen (waaronder politieambtenaren) strafrechtelijk verboden is.

De rode lijn was: Strafrechtelijk gezien mag filmen, zeker als dit openlijk gebeurt. Publicatie mag niet leiden tot strafbare feiten, zoals bedreiging etc. Dit kan alleen achteraf getoetst worden (recht op vrijheid van meningsuiting).

Deze rode lijn zal worden ~~wordt~~ gewijzigd door de strafbaarstelling van doxing ~~bepaling~~: filmen en verspreiden (publiceren) met een daarin opgenomen 'intimiderend doel' wordt verboden. Hierbij wordt indirect ook de vrijheid van meningsuiting beschermd, doordat mensen niet meer op deze wijze straffeloos kan worden getracht te mond te snoeren.
Het is denkbaar dat het al dan onherkenbaar in beeld brengen (blurren e.d.) van de persoon die gefilmd is bij publicatie een rol kan ~~gaan~~gaat spelen bij de strafrechtelijke beoordeling van het oogmerk. Dit is echter sterk afhankelijk van de context en zal per geval (achteraf) kunnen worden beoordeeld.

Vragen~~agstukken~~ waarop dit overzicht ~~deze analyse~~ niet ingaat zijn de mate waarin berichten worden verwijderd in het kader van de strafrechtelijke aanpak nadat strafbare doxing heeft plaatsgevonden (125p Sv; NTC-procedure); of in verband met smaadschrift door de strafrechter bevolen kan worden ~~mensen in het kader van het strafrecht opgedragen kan worden niet meer~~ bepaalde onrechtmatige uitingen te plaatsen (in strijd met censuurverbod of niet; zie ECLI:RBMNE:2021:4854) en hoe en door wie hierop toezicht uitgevoerd kan worden. Dit is belegd in aparte trajecten.

Overig

De (U)AVG is van toepassing op ~~Sinds 25 mei 2018 is daarnaast~~ de AVG in werking getreden. Iedere verwerking die onder deze wet valt moet voldoen aan de beginselen van gegevensverwerking, neergelegd in artikel 5 AVG. Dit geldt dus ook voor (burger)~~journalisten~~ journalisten, de publicisten (zie artikel 43 AVG). Het eerste beginsel stelt dat de wijze van verwerking ten aanzien van de betrokken rechtmatig, behoorlijk en transparant moet zijn. De andere beginselen geven aan dat de uitgangspunten van gegevensbescherming zijn: doelbinding; minimale gegevensverwerking, opslagbeperking; juistheid; integriteit en vertrouwelijkheid en opslagbeperking en verantwoordingsplicht. Onder de AVG is het met intimiderend doel verwerken van gegevens geen rechtmatig verwerkingsgrondslag (Zie artikel 6 AVG). Indien een verwerking van persoonsgegevens strijdig is met de (beginselen van) AVG, kan de betrokkene zich wenden tot de toezichthouder, in Nederland de Autoriteit Persoonsgegevens. Het kan daarnaast zo zijn dat de verwerking een onrechtmatige daad jegens de betrokkene oplevert, waartegen de gang naar de burgerlijke rechter openstaat.

Ook het civiele recht kan (andere) mogelijkheden bieden op te treden tegen filmers en publicisten. Zie de blurbrief. Hierbij kan een betrokkene iemand vorderen berichten te verwijderen, al dan niet via de rechter. Dit kan in voorkomend geval ook door de korpschef van de politie in hoedanigheid van werkgever. De rechter kan ook bepalen dat iemand moet stoppen met het publiceren van soortgelijke berichten (ECLI:NL:RBDHA:2021:6769).

Verder is relevant dat artikel 6:169c van het Burgerlijk Wetboek bepaalt dat informatiemaatschappijdiensten in de zin van artikel ~~ex~~ 15d lid 3 van Boek 3 ~~,~~ waar~~onder~~ social media-platformen als Facebook, Telegramm en ~~t~~Twitter onder vallen ~~,~~ niet aansprakelijk zijn voor het opslaan van informatie met een onrechtmatig karakter en of in het geval van een schadevergoedingsactie, niet redelijkerwijs behoort te weten van de activiteit of informatie met

Met opmerkingen 5.1.2.e **]:** Traject online content moderatie 5.1.2.e

Traject DGSenB/DGPenV (5.1.2.e
Nb 184a Sr (gedragsmaatregel)

Met opmerkingen 5.1.2.e 5.2.1

Met opmerkingen 5.1.2.e 5.2.1

Met opmerkingen 5.1.2.e 5.2.1

Met opmerkingen 5.1.2.e 5.2.1

Met opmerkingen 5.1.2.e **:**5.2.1

Met opmerkingen 5.1.2.e Uitspraak Bodegraven. Is er al een kort geding geweest?

Met opmerkingen 5.1.2.e **:** Check DWJZ

een onrechtmatig karakter, dan wel zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie of de toegang daartoe onmogelijk maakt. Daarbij bepaalt het vijfde lid, dat dit niet in de weg staat aan het verkrijgen van een rechterlijk verbod of bevel. Binnen Europa wordt er momenteel onderhandeld over de zogenaamde Digital Services Act.

Tot slot speelt in het kader van het openbare orde-recht momenteel de discussie of een burgemeester een zogehetennaamd '-online-gebiedsverbod' mag opleggen aan iemand die opruiende berichten verstuurt.

Een nadere analyse van het gegevensbeschermingsrecht, het civiele recht en het bestuursrecht vallen buiten het bestek van deze analyse.

Met opmerkingen 5.1.2.e Vindplaats laatste info aan TK?

Met opmerkingen 5.1.2.e aangenomen door EP

Met opmerkingen 5.1.2.e :5.2.1

Toelichting strafrechtelijk kader

Filmen

	Bepaling	Belangrijkste elementen
Wijze en waar filmen		
139 f Sr (geen vh-feit)	Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.	*Heimelijk* te filmen of fotograferen op niet-openbare plaatsen
441b Sr (vh-feit)	Met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie wordt gestraft hij die, gebruik makende van een daartoe aangebracht technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, van een persoon, aanwezig op een voor het publiek toegankelijke plaats, wederrechtelijk een afbeelding vervaardigt.	Verboden te filmen met een niet duidelijk kenbare *vaste* camera in de openbare ruimte, tenzij
Doel filmen		
Doxing-bepaling (VH~~vh~~-feit) Tekst consultatieversie wetsvoorstel (de wezenlijke kern van het wetsvoorstel wordt niet gewijzigd	Artikel 285d 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	

in de Raad van Staat-versie).	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, '.	
Indirect: Gedrag bij filmen (oa hinder)		
184 Sr (geen vh-feit)	Artikel 184. Lid 1. Hij die opzettelijk niet voldoet aan een bevel of een vordering, krachtens wettelijk voorschrift gedaan door een ambtenaar met de uitoefening van enig toezicht belast of door een ambtenaar belast met of bevoegd verklaard tot het opsporen of onderzoeken van strafbare feiten, alsmede hij die opzettelijk enige handeling, door een van die ambtenaren ondernomen ter uitvoering van enig wettelijk voorschrift, belet, belemmert of verijdelt, wordt gestraft met gevangenisstraf van ten hoogste drie maanden of geldboete van de tweede categorie. Lid 2. Met de in het eerste gedeelte van het vorige lid bedoelde ambtenaar wordt gelijkgesteld ieder die, krachtens wettelijk voorschrift, voortdurend of tijdelijk met enige openbare dienst is belast. **Lid 3** Met een vordering of handeling als bedoeld in het eerste lid wordt gelijkgesteld een vordering of handeling van de schipper of gezagvoerder van een luchtvaartuig die een bevoegdheid uitoefent of een verplichting vervult, welke hem als zodanig is toegekend of opgelegd bij een bepaling van het Wetboek van Strafvordering. Onder schipper wordt begrepen hij die het hoogste gezag uitoefent op een overeenkomstig artikel 136*a*,	Filmen mag niet belemmeren bij rechtmatige uitoefening van een wettelijke taak

	tweede lid, van het Wetboek van Strafvordering aangewezen installatie. **Lid 4** Indien tijdens het plegen van het misdrijf nog geen twee jaren zijn verlopen sedert een vroegere veroordeling van de schuldige wegens gelijk misdrijf onherroepelijk is geworden, kan de gevangenisstraf met een derde worden verhoogd.	
441a Sr (geen vh-feit)	Hij die openlijk of door verspreiding van enig geschrift ongevraagd een voorwerp als verkrijgbaar dan wel als bij hem voorhanden aanwijst en daarbij de aandacht vestigt op de geschiktheid daarvan als technisch hulpmiddel voor het heimelijk afluisteren, aftappen of opnemen van gesprekken, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk of als onderdeel van zulk een hulpmiddel, wordt gestraft met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie.	
426bis Sr (overtreding) (geen vh-feit)	Hij die wederrechtelijk op de openbare weg een ander in zijn vrijheid van beweging belemmert of met een of meer anderen zich aan een ander tegen diens uitdrukkelijk verklaarde wil blijft opdringen of hem op hinderlijke wijze blijft volgen, wordt gestraft met hechtenis van ten hoogste een maand of geldboete van de tweede categorie.	Op de openbare weg beperken van vrij beweging van een ander Met een of meer anderen zich aan iemand blijven opdringen of hinderlijk volgen op de openbare weg
Bepalingen uit de APV		Model-APV: 2:47 Hinderlijk gedrag op openbare plaatsen; 2:50 Hinderlijk gedrag in voor publiek toegankelijke ruimten
Indirect: Overtreden voorwaarden in het kader van het strafrecht opgelegd gebiedsverbod of locatieverbod	*Indirect aanpak*	
Filmen hulpbehoevenden?		

Publiceren

139f Sr (geen vh-feit)	Art. 139f. lid 1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die niet-openbare gegevens: **a.**verwerft of voorhanden heeft, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van deze gegevens wist of redelijkerwijs had moeten vermoeden dat deze door misdrijf zijn verkregen; **b.**ter beschikking van een ander stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt, terwijl hij weet of redelijkerwijs moet vermoeden dat het door misdrijf verkregengegevens betreft. **Lid 2** Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het verwerven, voorhanden hebben, ter beschikkingstellen, bekendmaken of gebruik van de gegevens, bedoeld in het eerste lid, vereiste.	
139g Sr (vh-feit)	Art. 139g sr. Lid 1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft: **a.**hij die opzettelijk en wederrechtelijk van een persoon een afbeelding van seksuele aard vervaardigt; **b.**hij die de beschikking heeft over een afbeelding als bedoeld onder a terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een onder a strafbaar gestelde handeling is verkregen. **Lid 2.** Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft: **a.**hij die een afbeelding als bedoeld in het eerste lid, onder a, openbaar maakt terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een in	

	het eerste lid, onder a, strafbaar gestelde handeling is verkregen; **b.**hij die van een persoon een afbeelding van seksuele aard openbaar maakt, terwijl hij weet dat die openbaarmaking nadelig voor die persoon kan zijn.	
285 Sr (bedreiging) (lid 1 vh-feit)		
261/262 Sr (laster) (geen vh-feit)		
266 Sr (belediging) (geen vh-feit)		
284 Sr (dwang) (lid 1 vh-feit)		
Indirect: Overtreden voorwaarden in het kader van het strafrecht opgelegd publicatieverbod?? (censuurverbod? Publicatieverbod onrechtmatige uitingen?		

BOB-middelen inzetbaar:

67 lid 1 Sv	Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van: a.een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld; **b.**een der misdrijven omschreven in de artikelen 132, 138a, 138aa, 138ab, 138b, 138c, 139c, 139d, eerste en tweede lid, artikel 139h, eerste en tweede lid, 139q, 140, tweede lid, 141a, 137c, tweede lid, 137d, eerste lid, 137e, tweede lid, 137g, tweede lid, 151, 184a, 254a, 248d, 248e, 272, 284, eerste lid, 285, eerste lid, 285b, 285c, 300, eerste lid, 321, 326c, tweede lid, 326d, 340, 342, 344a, 344b, 347, eerste lid, 350, 350a, 350c, 350d351, 395, 417bis, 420bis.1, 420quater en 420quater.1 van het Wetboek van Strafrecht;

Maatwerk
Elke doxingsituatie verloopt anders en vraagt om maatwerk. Soms is een stopgesprek voldoende, soms past enkel een aangifte. De wens van het slachtoffer is hierbij belangrijk, evenals de aanwezige mogelijkheden voor de politie om een verdachte op te sporen.

Onderstaande stappen geven een advies voor te ondernemen activiteiten. Een volledig risicodekkende standaardaanpak is er niet. Bij het beoordelen en behandelen van een casus doxing , ligt de nadruk op afwegingen op basis van gezond verstand.

Aangifte/Ambtshalve vervolgbaar/OSINT onderzoek (mogelijk strafbaar feit doxing)

Intake & Service: aandachtspunten aangifteproces

- Doxing ligt politiek gevoelig; wees je hiervan bewust, zeker wanneer de met name genoemde beroepsgroepen slachtoffer zijn.
- Doxing kán een veiligheidsrisico opleveren; hoe groter de online (media)storm wordt hoe meer risico een slachtoffer loopt. Monitor het situatieverloop dus goed!
- I.h.k.v. opsporing: vraag zoveel mogelijk relevante digitale informatie uit over het door de doxer gebruikte account of communicatiemiddel.
- In beginsel wordt door de aangever of getuige domicilie gekozen. De politie informeert aangevers en/of getuigen over de mogelijkheden hieromtrent. Voor het werken onder nummer moet toestemming worden gevraagd.

Contact met de aangever / gedoxte persoon
Indien bekend is (de aangever) of achterhaald kan worden (nog onbekend) wie de gedoxte persoon is:

- verzoeken vooralsnog niet te reageren op de doxing (zonder plan van aanpak)
- bevragen of de dreiger hem/haar bekend is
- bevragen/helder krijgen in welke mate bedreigde zich daadwerkelijk vrees aanjaagd*
- bevragen of eerder bedreigingen zijn ontvangen

*Het is niet vereist dat het slachtoffer zich daadwerkelijk bedreigd voelt. Voldoende is dat de doxing van dien aard is en onder zodanige omstandigheden geschiedt dat bij de gedoxte persoon ‘de redelijke vrees kan (laten) ontstaan, ernstige overlast aan te (laten) doen of hem in de uitoefening van zijn ambt ernstig te (laten) hinderen’ dat het dreigement wordt uitgevoerd.

Indien de gedoxte persoon niet bekend is (of nog niet is benaderd):

Besluit of je doxing serieus genoeg vind om er zonder contact met de gedoxte persoon iets mee te doen. In het geval dat je het serieus genoeg vind is het belangrijk om de doxing vast te leggen in BVH of eventueel in overleg met het OM ambtshalve te gaan vervolgen.

Het is belangrijk om daarbij als volgt te handelen:

- Maak een incident ‘doxing’ aan
- Hanteer voor ‘datum en tijdstip’: de gegevens van doxing
- Hanteer voor het veld ‘locatie’: nn
- Plaats in het vrije veld ‘Toelichting’ het tekstblok ‘Doxing’
- Vul daar de volgende gegevens in:
  - Gedoxte persoon (indien bekend, betrekt het iemand van 2e lid artikel van 285d)
  - Afzender die de persoon doxt (ook nickname)
  - Op welk sociale media gremia gedeeld

  - telefoonnummer(s);
  - afbeeldingen;
  - chatlogs (check bij aangever of hij/zij deze optie heeft aanstaan).
  - Letterlijk citaat van de doxing (dus incl. schrijffouten en tekens)
  - Categorie (Serieus, Twijfelachtig, Acute/Niet serieus)
- Vul de MO in: doxing
- Vul vervolgens onder toelichting in: DOXING

Maak een mutatieformulier aan (Formutra)

Wanneer doxing voor het eerst ontdekt of gemeld wordt, dan zal een eerste inschatting gemaakt moeten worden van de mate van de dreiging en het risico. Op basis van 'onderwerp' en 'inhoud' kan een eerste indicatie voor prioritering gemaakt worden. Volg daarbij je eigen gevoel en gezond verstand om te bepalen of de doxing voor jou valt in de categorie 'niet serieus' of 'acute/serieus'. Toets bij twijfel de opsporings coördinator.

Is de doxing voor jouw gevoel overduidelijk 'niet serieus' of voldoet het niet aan alle elementen van het artikel, dan is geen directe actie nodig. Dit betekent echter niet dat er geen actie nodig is. Een afhandeling is wel wenselijk. Je kunt bijvoorbeeld overwegen om:

- de verzender (indien bekend) van de doxing aan te spreken op zijn gedrag (stopgesprek)
- de ouders te informeren indien het een minderjarige betreft

<u>Data verzamelen en veiligstellen/ interpreteren en wegen</u>

Data verzamelen en veilig stellen

Zorg dat je zicht krijgt op de context. Verzamel data zoals accountgegevens en alle andere berichten die op sociale media zijn geplaatst. Blijkt uit de context dat de doxing meer is dan onzin, zorg er dan voor dat data z.s.m. veilig gesteld wordt door Digitale Expertise. Uiteraard geldt dit ook voor alle informatie die bij latere stappen verzameld wordt. Het is van belang dat dit via beveiligde computers gaat. Bij voorkeur via het IRN* vanwege automatische logging en autorisatie OM bewijsmateriaal.

Veilig rechercheren en surveilleren op het internet

Rechercheren en surveilleren dient binnen een daarvoor bestemd systeem te gebeuren. Het iRN (Internet Rechearch & Innovatie Netwerk) maakt het de politie mogelijk om op een veilige, forensisch verantwoorde manier op het internet onderzoek en opsporing te doen. Op dit moment beschikt iedere politie-eenheid in Nederland over een of meerdere iRN configuraties.

Data interpreteren en wegen

Bij het maken van een nadere inschatting of de doxing serieus is of niet, kun je inzoomen op een aantal factoren:

1. Inhoud (wat houdt de doxing in?)
   - Wat is de doxing? (welke concrete elementen van doxing)
   - Welke tone-of-voice? Context
   - Straattaal?
   - Gebruik van emoticons?

2. Onderwerp (aan wie is de doxing gericht?)
   - Benoemd persoon?
   - Onbenoemd persoon?
   - Publieke taak?

- Bevolkingsgroep?

3. Profiel (wat is het beeld van de verzender van de bedreiging)
   - Minderjarig?
   - Nationaliteit?

4. Motief (wat lijkt de aanleiding?)
   - Angst aan te jagen?
   - Verveling?
   - Balorigheid?
   - Frustratie?
   - Ruzie?
   - Haat?

5. Online context (welke uitingen zijn nog meer gedaan)
   - Doxing berichten voorafgaand aan de bedreiging?
   - Doxing berichten geplaatst na de bedreiging?
   - reacties van anderen?

Opmerking:
Raadpleeg jouw OSINT medewerkers bij deze stap. Zij hebben kennis in huis om te ondersteunen bij het interpreteren van de online doxing.

Is de doxing gepleegd tegen de persoon in een bepaalde hoedanigheid (art. 285d lid 2 Sr.)
Art. 285d lid 2. Indien het feit, omschreven in het eerste lid wordt gepleegd tegen een persoon in diens hoedanigheid van Minister, Staatssecretaris, commissaris van de Koning, gedeputeerde, burgemeester, wethouder, lid van een algemeen vertegenwoordigend orgaan, rechterlijk ambtenaar, advocaat, journalist of publicist in het kader van nieuwsgaring, ambtenaar van politie of buitengewoon opsporingsambtenaar wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.

PRIORITEIT:
Melding van doxing tegen deze functionarissen krijgen direct opvolging!!!

CCB / GTPA / directe leidinggevende in kennis stellen

De rol van de politie
Die is tweeledig: enerzijds is zij dienstverlener voor iedereen die informatie zoekt, melding wil maken of aangifte wil doen. Daarnaast heeft zij vanuit goed werkgeverschap een verantwoordelijk wanneer politiemedewerkers worden gedoxt: bekijk hiervoor het de **werkinstructie politiedoxing** via het **Handelingskader politiedoxing voor leidinggevenden'.**

Let op!
De **persoonlijke veiligheid** van de gedoxte persoon kán gevaar lopen, bijvoorbeeld als een woonadres is gedeeld; beoordeel dus altijd per casus of sprake is van een (concreet) veiligheidsrisico. De context van een casus is hierbij belangrijk, maar ook de actualiteit en concreetheid van de dreiging.

In Nederland is eenieder in eerste instantie zelf verantwoordelijk voor zijn/haar veiligheid.

Personen kunnen daarbij rekenen op hulp van organisaties en netwerken waartoe zij behoren, zoals bijvoorbeeld een werkgever ingeval van doxing wegens een relatie met de beroepsuitoefening. Er ontstaat pas een verantwoordelijkheid voor de overheid als personen en organisaties op eigen kracht geen weerstand kunnen bieden aan een dreiging.
Tip: wanneer een doxingsituatie speelt rond personen als omschreven in het 2e lid van artikel 285d, bespreek dan met het slachtoffer welke afspraken gelden voor hun organisatie of taakveld ten aanzien van dreiging.

Soms valt een casus met een concrete en/of ernstige bedreiging niet onder de hierboven omschreven uitgangspunten. In dit geval kan je overleg plegen met de contactpersonen van de vakgroep Bewaken en Beveiligen binnen jouw Eenheid. **(tekst & inhoud akkoord bevonden door CCB, 1/9/24)**

Vaststellen strafbaarheid doxing (of poging)
Kortgezegd betekent dit het met kwade bedoelingen **verzamelen**, (verder) **verspreiden** of **distribueren** van **persoonsgegevens** van een ander, of een derde **(familieleden!),** zoals: **naam, woon-of werkadres, telefoonnummer, emailadres of foto**. Doxing speelt zich overwegend online af op sociale platformen en neemt soms zeer omvangrijke vormen aan. Doxing kan leiden tot pesterijen, haatberichten en intimidatie en kent klachten als stress, angst, depressiviteit, eenzaamheid en suïcidale gedachten. Online achtergebleven content is extreem lastig te verwijderen waardoor slachtoffers een langdurige confrontatie kunnen ervaren. Doxing gaat vaak gepaard met andere strafbare gedragingen zoals bedreiging, opruiing, belediging of smaad. Doxing is per definitie persoonlijk van aard en kan een sterk ontregelend effect op de privésituatie van het slachtoffer hebben.

Wat is strafbaar:
Het verzamelen, verspreiden of ter beschikking stellen van persoonsgegevens met het oogmerk om een ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of hem in de uitoefening van zijn ambt ernstig te (laten) hinderen.

Belangrijk!
De bedoeling - het oogmerk van de dader - moet gericht zijn op het aanjagen van vrees, ernstige overlast of ernstige hinder in diens beroepsuitoefening. Het enkel (verder) verspreiden van bijvoorbeeld beeldmateriaal van politiemensen is dus géén doxing.

Leestip: juridische toelichting wetsartikel!
Voor een juridische en praktische toelichting op artikel 285d, lees het document **Bouwstenen Doxing Juridisch**. Handig voor voorbeelden, reikwijdte, de elementen

Bepaal benodigde aanpak, vervolgacties en prioriteit
Afhankelijk van de zwaarte van het risico van de doxing, stel je een aanpak vast in overleg met de opsporings coördinator. Volg daarbij de bestaande werkprocessen en juridische kaders. Voor eventueel advies kun je terecht bij:

- Digitale Expertise
- Opsporing
- OM
- GTPA
- CCB
- afdeling communicatie

Prioriteit bij opsporing en vervolging

De politie en Openbaar Ministerie geven hoge prioriteit aan de opsporing en vervolging van verdachten van doxing tegen functionarissen met een publieke taak die genoemd zijn in het 2e lid van artikel 285d. **De regie van de opsporing ligt bij de DR of DRR**. Daarbij wordt zoveel mogelijk lik op stuk beleid toegepast. Zo neemt de politie bij ernstige vormen van doxing eerst contact op met het Openbaar Ministerie voordat de verdachte wordt heengezonden. Het Openbaar Ministerie stelt in dergelijke zaken in principe vervolging in. Het is ook mogelijk dat werkgevers aangifte doen van Doxing tegen hun werknemers. Het Openbaar Ministerie ondersteunt het slachtoffer bij het uitoefenen van zijn rechten, waaronder het verhalen van schade op de dader. Het Openbaar Ministerie voert over deze zaken een actief communicatiebeleid.

Eventueel nader online en offline onderzoek

Om een beter beeld te krijgen van de verzender van de gedoxte persoon kan nader online onderzoek uitkomst bieden. Wellicht kan op basis van de profielbeschrijving van het sociale media account of uit berichten achterhaald worden:

- Of verzender minderjarig/meerderjarig is
- Wat zijn/haar echte naam is
- Welke omgeving (of zelfs plaats) verzender woonachtig is
- Op welke school/ vereniging/ groepering de verzender zit

Wellicht is de verzender ook te vinden op, Facebook, Instagram, tiktok of andere sociale media platforms.

Offline onderzoek (denk hierbij ook aan overleg met collega's van de DRIO (TOOI/TCI) en veiligheidshuis)

- indien minderjarig; neem contact op met de school om te achterhalen hoe de bedreiger bekend staat.
- is bedreiger eerder in contact geweest met politie/justitie?
- Is er sprake van zorg, bijvoorbeeld is de bedreiger bekend bij Jeugdzorg?

Leestip: Doxing TDO presentatie

Inzet van dwangmiddelen artikel 67 Sv

Artikel 67 Sv: het misdrijf wordt als 'VH-feit' aan dit artikel toegevoegd, zodat bevoegdheden zoals het vorderen van gegevens, BOB-middelen of bevel ontoegankelijk maken gegevens kunnen worden toegepast. Vraag hiervoor toestemming bij de OVJ.

NTD-procedure politiemedewerkers

Weet je dat er een interne verwijderingsprocedure bestaat - voor gevallen van strafbare, online content t.a.v. politieagenten - genaamd Notice And Takedown. Lees hier de door de afdeling 5.1.2.e van de Landelijke Eenheid ontwikkelde **NTD-procedure**. Kies jouw eenheid, selecteer het tabblad database en voer het trefwoord NTD in voor de formulieren en werkwijze.

Let op! Overleg **altijd** met de cyber-OvJ binnen jouw eenheid over de inzet van dit middel: spoedige verwijdering van online content kan botsen met het opsporingsbelang.

NTD-procedure burgers

Ieder slachtoffer van doxing kan zelfstandig een verwijderingsverzoek indien bij een platform waarop de content aanwezig is. De website **https://noticeandtakedowncode.nl** geeft informatie aan eenieder over de werkwijze van dit middel.

Let op! Als een burger zowel aangifte doet als een NTD-verzoek indient dan bestaat de kans dat de content is verwijderd, nog vóórdat dit in het belang van opsporing is veiliggesteld. Maak hierover altijd duidelijke afspraken met elke aangever.

Vervolging OM

Verzamel de benodigde documenten om het dossier compleet te maken. Volg daarbij het gangbare opsporingsproces.

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

5.1.2.e

Niet onder reikwijdte

‘Opeens was het minder leuk, een partner bij de politie’

Enkele leden van de aanhoudingseenheid (AE) Amsterdam krijgen na een inzet bij een demonstratie op het Museumplein te maken met een nieuw fenomeen: doxing. Via social media worden beelden gedeeld van de collega’ s met de oproep hun privégegevens te achterhalen. Suus is de partner van Erik*, een lid van het team. Zij vertelt wat voor impact dit had op haar en het gezin. ‘Opeens was het minder leuk; een partner bij de politie.

Op 2 februari krijgt Erik ’s avonds een belletje van een recherchechef. In een telegram-groep gaat zijn foto rond. ‘Ze boden 500 euro voor wie Eriks gegevens zou achterhalen of hem zou slaan. Wij zijn beiden vrij nuchter en hadden zoiets van ‘’het zal wel’’. Tot er een dag later ineens een onbekende auto met twee verdachte figuren voor de deur stond.’

Vertrouwen

Toen het stel elkaar tien jaar geleden leerde kennen, zat Erik nog niet bij de AE. ‘Ik heb dat proces van dichtbij meegemaakt. We zijn altijd open naar elkaar geweest en hij liet me filmpjes zien van zijn inzetten. Ik zie hoe vaak hij traint dus ik ben eigenlijk nooit bang dat hem iets overkomt tijdens dat werk. Die mannen kunnen blindelings op elkaar vertrouwen. Het normale werk op straat vind ik spannender.’

Wat Suus, die zelf ook bij de politie werkt, wel iets doet zijn de recente beelden van het optreden van de eenheid op het nieuws en sociale media. ‘Dat vind ik heel vervelend omdat ze maar een deel van een situatie laten zien. De AE treedt niet zomaar op en is geen verlengstuk van de overheid, maar door de beelden die getoond worden, denken mensen anders over de eenheid. Ik zeg niet altijd meer dat mijn man bij die groep hoort, ook al ben ik trots op hem.’

Incident

De dag na het belletje van de recherche werkt Suus vanuit huis, in haar pauze valt een auto recht voor de voordeur op. ‘We wonen in een straat waar je niet zomaar komt, je moet een wirwar van straten door. Ik zie twee mannen. Ik raak niet in paniek maar besluit wel om Erik een foto te sturen. Niet veel later ga ik naar boven, terug aan het werk, als er wordt aangebeld. Uit het raam zie ik die mannen staan, ik doe niet open.’

Erik heeft inmiddels in het politiesysteem gezien dat de auto niet op naam staat van de mannen voor de deur, en dat de zoon van de eigenaar enkele bijzondere, mutaties op zijn naam heeft. ‘Daar schrik ik wel van. Hij blijkt een paar keer te zijn aangesproken op demonstraties tegen corona omdat hij politieagenten filmde. Daarom gaan alle alarmbellen af.’

Afgesloten wijk
Twee AE-collega's gaan naar Eriks huis om ervoor te zorgen dat zijn vrouw veilig is. Uiteindelijk sluiten blauwe collega's de wijk af en gaan op zoek naar de personen. Na een tijdje worden ze gevonden en aangehouden. Ook hun telefoons worden in beslag genomen voor onderzoek. Erik komt 's avonds pas thuis'
Het is voor Suus een opluchting dat de politie de situatie snel en adequaat oppakt. 'Ik ben blij dat de kinderen die dag bij de oppas zijn en er weinig van meekrijgen. Uiteindelijk hebben we bijna een maand de gordijnen dichtgehouden en alleen de achterdeur gebruikt. In de supermarkt kijk ik constant achterom of niemand me volgt. Tot het nieuws komt dat de telefoons zijn onderzocht en er niets in onze richting wijst.'

Sociale media
'Je beseft dan dat je gezin kwetsbaarder is dan je denkt. Het heeft ons doen besluiten onze sociale media flink op te schonen. We hebben geen herkenbare profielfoto meer, hebben onze foto's op privé gezet en familie gevraagd niets van ons te plaatsen. Daarnaast hebben we aardig wat vrienden en vage kennissen verwijderd. De hele situatie zet je wel op scherp '

*Erik en Suus zijn gefingeerde namen

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.
5.1.2.d

5.1.2.d

5.1.2.d

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

Jij toetsenbordheld op sokken: zet je koffertje maar klaar….

Koningsdag 2021 was voor velen een stralende dag. Maar niet voor mijn collega's die wederom niet thuis waren bij hun geliefden. Er zijn zelfs collega's die acht weekenden achter elkaar gewerkt hebben. En waar iedereen helemaal klaar is met Corona, is Corona dat alleen nog niet met ons. Gelukkig is het naleven van de maatregelen voor velen vanzelfsprekend. En ik heb best begrip dat, zeker op een zonnige dag, dit naleven niet altijd gemakkelijk is. Maar wat ik niet begrijp is dat als we bezoekers meerdere malen en met veel geduld verzoeken om weg te gaan, we onthaald worden met agressie, verzet, bekogeld worden met flessen en wat al niet meer. Dan is de grens bereikt. 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 'facist', '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. Vanuit de politie is daarom al eerder gepleit voor het strafbaar maken van doxing. De minister heeft gelukkig toegezegd te onderzoeken of hiervoor aanvullende wetgeving nodig is. Tegelijk doe ik persoonlijk een dringend appèl op de social media platforms om deze verwerpelijke posts te verwijderen en een halt toe te werpen aan deze buitengewoon zorgelijke ontwikkeling.

Koningsdag 2021 was een stralende dag, maar voor mij en mijn collega's wel één met helaas een bittere nasmaak. Ik heb tot slot nog een persoonlijke boodschap voor diegenen die al die vunzigheid posten over mijn collega('s). Weet dat wij hoge prioriteit geven aan het achterhalen van je identiteit, samen met het Openbaar Ministerie zal dit beoordeeld worden. Dus. Jij, toetsenbordheld op sokken. Het is niet de vraag *of*, maar *wanneer* we je komen halen. Je komt namelijk bij ons logeren. Zet je koffertje met je pyjama en tandenborstel maar vast klaar.

	Onderwerp:	Stand van zaken:	Actie(houder):	Planning:	Gereed
Afspraken stellingname:					
	Buiten reikwijdte				
1.					
a.					
2.					
a.					
b.					
c.					
d.					
3.					
a.					
4.					

a.	Buiten 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.	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 punt 2 hierboven	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.	Wordt hier bedoeld inzetten door politie als werkgever? Mogelijk eerst bespreken in voorgestelde subwerkgroep, zie onder punt 2 hierboven	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.			
b.			
c.			
d.			
e.			
f.			
g.			

h.	Buiten reikwijdte				
3.	B				
a.					
b.					
c.					
d.					
e.					
f.					
4.					
a.					

b.	Buiten reikwijdte				
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		