

Bijlage bij Agressieprotocol politieke ambtsdragers gemeente Alkmaar: richtlijnen online agressie voor politieke ambtsdragers

Online agressie via e-mail of sociale media neemt toe. Hierbij hebben we het zowel over online verbale agressie (zoals schelden, kleineren of discriminerende opmerkingen maken) als over bedreiging en intimidatie via e-mail of sociale media. Onderzoek heeft ook uitgewezen dat politici negatieve mentale en lichamelijke gevolgen ervaren van online agressie en geweld. Het is dus belangrijk om de kans op (of risico van) online agressie te verkleinen en als er toch incidenten gebeuren snel in actie te komen bij online agressie. Hieronder staan een aantal tips om op zowel preventief als reactief gebied om te gaan met online agressie. Hiervoor is gekeken naar de meest gebruikte social media kanalen: Facebook, Twitter en Instagram.

Preventie

1. Algemeen

- Google uzelf maandelijks. U kunt ook op uw naam zoeken op de socialmediaplatformen.
- Check minimaal één keer per maand uw privacy-instellingen op uw accounts. U kunt een collega waar u geen connectie mee heeft op sociale media vragen u op te zoeken en te laten zien wat allemaal zichtbaar is.
- Maak gescheiden accounts:
 - o 1 privéaccount, alleen voor vrienden (echte vrienden en volledig afgeschermd, niet vindbaar op Google en andere zoekmachines, geen foto's van of bij vrienden etc.)
 - o 1 zakelijk account waar u de partij en het ambt mee promoot.
- Kijk niet op sociale media voordat u gaat slapen, dan blijft het in uw hoofd zitten. Doe dat de volgende dag als u fris bent.

2. Facebook

- Onder het kopje *'Wachtwoord en beveiliging'* via <https://accountscenter.facebook.com/> kunnen de wachtwoorden van het Facebook-profiel gewijzigd worden.
- Onder het kopje *'Wachtwoord en beveiliging'* via <https://accountscenter.facebook.com/> kan ook tweestapsverificatie ingesteld worden. Dit is een extra beveiliging, waarmee de online toegang tot gevoelige zaken beter kan worden beschermd.
- Scherm af! Zorg dat alleen te zien is wat u echt wil dat mensen kunnen zien. Stel de volgende instellingen in om uw profiel af te schermen:
 - Via https://www.facebook.com/privacy/checkup/?source=privacy_center kunt u naar het kopje *'wie kan zien wat je deelt'*. Hier kunt u aangeven wie bepaalde profielgegevens van u kan zien (zoals relatiestatus en geboortedatum), evenals wie uw vriendenlijst kan zien. Het is aan te raden om hier de optie *'alleen ik'* te selecteren.
 - Via https://www.facebook.com/privacy/checkup/?source=privacy_center kunt u naar het kopje *'Hoe mensen je kunnen vinden op Facebook'*. Hier kunt u aangeven wie u vriendschapsverzoeken kan sturen (iedereen, of alleen vrienden van vrienden). Ook kunt u hier aangeven of zoekmachines (zoals Google) kunnen doorverwijzen naar uw Facebook-profiel. Het is aan te raden om deze optie uit te zetten.
 - Sluit de messenger of DM-functie van de profielen zodat mensen u niet persoonlijk en direct kunnen benaderen via social media. Reacties onder posts kunt u openlaten (dit is voor iedereen zichtbaar).

3. Instagram

- Onder het kopje *'Wachtwoord en beveiliging'* via <https://accountscenter.instagram.com/> kunnen de wachtwoorden van het Instagram-profiel gewijzigd worden.
- Onder het kopje *'Wachtwoord en beveiliging'* via <https://accountscenter.instagram.com/> kan ook tweestapsverificatie ingesteld worden. Dit is een extra beveiliging, waarmee de online toegang tot gevoelige zaken beter kan worden beschermd.
- Via https://www.instagram.com/accounts/settings/v2/account_privacy/ kunt u uw account op 'Privé' zetten. Op deze wijze kunnen alleen de volgers die u heeft goedgekeurd zien wat je deelt, waaronder je foto's en video's op hashtag- en locatiepagina's, en je lijsten 'Volgers' en 'Volgend'. Bepaalde gegevens zoals uw profielfoto en gebruikersnaam blijven zichtbaar.
- Via https://www.instagram.com/accounts/settings/v2/message_controls/ kunt u aangeven wie u berichten kan sturen.

4. Twitter/X.com

- Via <https://x.com/settings/password> kunt u uw wachtwoord aanpassen.
- Via <https://x.com/settings/security> kunt u de beveiliging van uw account verbeteren, door bijvoorbeeld tweestapsverificatie in te stellen.
- Via https://x.com/settings/privacy_and_safety kunt u uw privacy-instellingen aanpassen.
- Via https://x.com/settings/audience_and_tagging kunt u de optie 'protect your posts' aanzetten zodat uw posts alleen zichtbaar zijn voor mensen die u volgen.
- Via https://x.com/settings/direct_messages kunt u aanpassen wie u via de DM (direct message) functie kan benaderen. Aan te raden is om de optie 'No one' aan te zetten.
- Via <https://x.com/settings/contacts> kunt u aanpassen hoe mensen u op Twitter kunnen vinden.

Reactie

- Als er sprake is van grensoverschrijdend gedrag (zie hiervoor de matrix in het agressieprotocol): meldt dit!
- Bewaar alle intimiderende of bedreigende berichten, of laat dat doen. Maak screenshots.
- Neem online agressie serieus. Een verhaal dat gedeeld wordt op social media kan snel zijn eigen leven gaan leiden. Dat betekent dat u direct actie moet ondernemen volgens de afspraken die in dit Agressieprotocol opgeschreven staan.
- Je kunt op social media een bericht 'rapporteren' of op twitter 'Reporten'. Wees u ervan bewust dat de meeste platformen terughoudend zijn met het verwijderen van berichten. Ga er dus niet van uit dat het hiermee is opgelost.
- Blokkeer mensen die haatdragende berichten sturen. Dit kan zowel op Facebook, Instagram als op Twitter.
- Let op uw mentale gesteldheid.

Reactie vanuit de gemeente

Bovenstaande hoofdstukken zijn met name gericht op acties die politieke ambtsdragers zelf kunnen uitvoeren. In voorkomende gevallen (in gevallen van digitale agressie die gemeld worden) kan de gemeente aangifte doen. In dit geval kunnen, naar aanleiding van de aangifte, de volgende stappen genomen worden door de politie of het OM.

1. Strafrechtelijke vervolging

Een aangifte kan als startpunt dienen van strafrechtelijke vervolging. Gelet op de overwegingen die hebben gespeeld over het al dan niet doen van aangifte worden in onderstaande paragrafen de mogelijk toepasselijke strafbare feiten uiteengezet. Het is van belang om te benoemen dat een aantal van deze strafbare feiten slechts kunnen worden vervolgd op klacht van het slachtoffer: in het geval van delicten die het karakter van een belediging dragen (zoals smaad, laster en strafbare belediging) en bij belaging. In situaties waar er geen sprake is van dergelijke klachtdelicten is er geen aangifte noodzakelijk om over te gaan op vervolging: er kan dan ambtshalve door de officier van justitie worden vervolgd.

1.1. Strafbare feiten gericht op een persoon

Smaad en Laster

Voor een bewezenverklaring van smaad is van belang dat er sprake is van een a) opzettelijke b) aantasting van iemands eer of goede naam, door c) tenlastlegging van een bepaald feit, met d) als kennelijke doel om daaraan ruchtbaarheid te geven. Aanvullende vereisten bij laster zien op het plegen van smaad(schrift) met de kennis dat het in strijd is met de waarheid.

Belediging

Naast smaad en laster kan een openbare uiting strafbaar zijn in de vorm van een eenvoudige belediging. Daarbij hoeft geen sprake te zijn van de tenlastlegging van een bepaald feit, maar is voldoende dat iemands eer of goede naam wordt aangetast.

Belaging

Belaging wordt ook wel als stalking omschreven en ziet op het opzettelijk en herhaaldelijk lastigvallen van iemand, waardoor een inbreuk wordt gemaakt op diens persoonlijke levenssfeer. Daarbij dient de opzet zowel gericht te zijn op die inbreuk, als op het feit dat het

slachtoffer door die inbreuk wordt gedwongen iets te doen, laten, te dulden of degene vrees aan te jagen.

Doxing

Doxing wordt beschreven als het zich verschaffen, verspreiden of anderszins ter beschikking te stellen van persoonsgegevens voor intimiderende doeleinden. Daarbij is vereist dat het oogmerk van het verspreiden ziet op het vrees aan (laten) jagen, het aandoen van overlast of het ernstig hinderen in de uitoefening van een ambt of beroep. Er hoeft volgens de delictsomschrijving expliciet nog geen sprake te zijn van het verspreiden: het enkele verschaffen is voor het aantonen van dat bestanddeel voldoende. Daarbij moet worden opgemerkt dat bij het verschaffen, verspreiden of ter beschikking stellen het oogmerk dient te liggen op het aanjagen van vrees of aandoen van overlast.

1.2. Strafbare feiten gericht op de openbare orde

Opruiing

Strafbare opruiing ziet op het in het openbaar, mondeling of bij geschrift of afbeelding, opruien tot enig strafbaar feit of gewelddadig optreden tegen het openbaar gezag. De openbaarheid van de opruiing uit zich in deze situatie door het delen van de uitingen op een openbaar platform, waarbij de openbaarheid onder andere wordt bepaald aan de hand van de feitelijke openheid en verwachting van vertrouwelijkheid.

Verspreiding opruiend geschrift

Opruiing op zichzelf is een uitingsdelict, en kent geen expliciete strafbaarstelling van de verspreiding van opruiende uitingen. Bij het delen van door anderen geformuleerde digitale uitingen hebben wij het over ‘verspreiding opruiend geschrift’. Daarbij kan onder andere gedacht worden aan het herplaatsen van berichten op sociale media. Herplaatsers van berichten die op grond van voorgaande paragraaf als strafbare opruiing kunnen worden aangemerkt zouden daarmee ook strafrechtelijk vervolgd kunnen worden.

2. Het (verplichten tot) laten verwijderen van content

2.1. Redelijk verzoek tot verwijderen van content

De Internet en Ondersteuningsgroep (hierna ‘IOG’) is een groep binnen de politie die bestaat uit internetspecialisten met verschillende expertises. Indien er een melding wordt gedaan van digitale agressie bij de politie kan de IOG adviseren en onderzoek doen naar de aard en

herkomst van deze digitale agressie en aan de hand hiervan een zogeheten ‘redelijk verzoek’ doen aan social media platformen om berichten te verwijderen. De IOG heeft een contactpersoon bij de sociale mediaplatformen voor dergelijke situaties. Aan dit contactpersoon wordt ‘in redelijkheid’ verzocht om bepaalde reacties te verwijderen, zonder dat hierbij sprake is van een op een verzoek dat gebaseerd is op wet- en regelgeving of de algemene voorwaarden van zo’n platform. Het laten verwijderen van de berichten door platformen zelf heeft als voordeel dat het voor de plaatser lijkt alsof het initiatief tot verwijdering bij het platform ligt – en niet bij een gemeentelijk orgaan.

2.2. Notice & Takedown-procedure (NTD-procedure)

De NTD-procedure is ingericht door internetplatformen en is bedoeld voor het inrichten van een meldingsprocedure om aansprakelijkheid voor content op dienst platformen te beperken. Deze procedure is vastgelegd in de NTD-code (noticeandtakedown.nl). Door middel van de NTD kan een platform verzocht worden inbreukmakende, onrechtmatige of strafbare inhoud op dat platform te verwijderen. De aansprakelijkheid die op dergelijke platformen rust als er sprake is van dergelijke inhoud, vervalt indien platformen prompt de nodige maatregelen nemen om de informatie te verwijderen of de toegang daartoe onmogelijk te maken. Een dergelijk verzoek kan worden gedaan door de gemeente, maar ook door de getroffen als privépersoon. Binnen de procedure toetst het platform of in hun perceptie inderdaad sprake is van dergelijke inhoud, en indien dat het geval is wordt overgegaan tot verwijdering of ontoegankelijkmaking van de inhoud. Het platform kan ook tot de conclusie komen dat ze geen aanleiding zien om over te gaan tot verwijdering of ontoegankelijkmaking. In die gevallen kan verwijdering privaatrechtelijk worden afgedwongen, waarbij getoetst wordt aan de vrijheid van meningsuiting als neergelegd in art. 7 van de Grondwet en art. 10 Europees Verdrag betreffende de Rechten van de Mens.

2.3. Bevel aan aanbieder communicatiedienst om gegevens ontoegankelijk te maken

In gevallen waarin de NTD-procedure niet volstaat, kan als alternatieve interventie gedacht worden aan een bevel aan de aanbieder van een communicatiedienst om gegevens ontoegankelijk te maken. Van deze bevoegdheid kan gebruik gemaakt worden door de officier van justitie indien er sprake is van een als zodanig aangeduid misdrijf en er uit de feiten en omstandigheden blijkt dat deze ontoegankelijkmaking noodzakelijk is om strafbare

feit te beëindigen of nieuwe strafbare feiten te voorkomen. Voor het geven van het bevel is voorafgaande schriftelijke machtiging nodig van de rechter-commissaris. Het bevel kan niet voor alle strafbare feiten worden gegeven, maar is behouden voor (verdenking) van misdrijven bedoeld in artikel 67, eerste lid, Wetboek van Strafvordering. Uitgangspunt is dat er sprake moet zijn van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld, of misdrijven die specifiek worden genoemd in dat artikel. In paragraaf 5.1 is aandacht besteed aan het doen van aangifte en de mogelijke strafbare feiten waarvan sprake kan zijn. In de tabel hieronder is samengevat weergegeven of, en waarom, een bevel tot ontoegankelijkmaking van inhoud mogelijk is.

<i>Strafbaar feit</i>	<i>Bevel mogelijk?</i>	<i>Toelichting</i>
Smaad	Nee	Maximale gevangenisstraf < 4 jaar
Laster	Nee	Maximale gevangenisstraf < 4 jaar
Belediging	Nee	Maximale gevangenisstraf < 4 jaar
Belaging	Ja	Specifiek opgenomen in artikel 67, eerste lid onder b, Sv (wetboek van strafvordering)
Doxing	Ja	Specifiek opgenomen in artikel 67, eerste lid onder b, Sv
Opruiing	Ja	Maximale gevangenisstraf > 4 jaar
Verspreiding opruiend geschrift	Ja	Specifiek opgenomen in artikel 67, eerste lid onder b, Sv