POLITIE

Matrix Bevoegdheden informatievergaring op het internet voor niet-strafvorderlijk handelen

Leeswijzer **Oktober 2017**

Introductie

Binnen de politie worden veel vragen gesteld over de mogelijkheden en begrenzingen van het vergaren van informatie op het internet voor de uitvoering van de politietaak. Politieteams die niet-strafvorderlijk onderzoek[1] doen maken in toenemende mate gebruik van het internet. Het internet is een zeer rijke bron van informatie, en het ondersteunt bij het maken van de juiste keuzes en bij de uitvoering van politiewerk. Er zijn wettelijke kaders waarbinnen de politie werkt, maar de huidige wetgeving biedt onvoldoende duidelijkheid voor het verrichten van onderzoekshandelingen op het internet. Problematisch hierin is dat de bevoegdheden die ervoor worden aangewend er niet specifiek voor zijn geschreven en dat de wetgever bij het opstellen van die bevoegdheden de gevolgen daarvan met de uitgebreide mogelijkheden van vandaag niet heeft kunnen voorzien. Bovendien gelden voor de in de politietaak te onderscheiden deeltaken verschillende juridische kaders. Gevolg is dat er veel, maar vooral ook heel verschillend geïnterpreteerd en uitgelegd wordt. Dit is onwenselijk omdat het kan zorgen voor rechtsongelijkheid en risico's ter terechtzitting, en kan leiden tot over- of onderbenutting van de mogelijkheden door de politie. Dit onderwerp is complex en relatief nieuw, wat betekent dat er nog niet veel kennis bestaat of jurisprudentie aanwezig is om de benodigde afwegingen te kunnen maken en om de mogelijkheden en begrenzingen vast te stellen. Vanwege de vele, soms niet scherp af te lijnen, wegingsfactoren is het onmogelijk gebleken om te volstaan met een eenvoudige FAQ.

Het niet-strafvorderlijk vergaren van informatie kent echter amper geschreven rechtsregels – laat staan bevoegdheden – en is daarom nog een vrij onbekend gebied. Informatievergaring zou kunnen op grond van artikel 3 van de Politiewet, mits daarbij geen sprake is van inbreuk op de persoonlijke levenssfeer van meer dan geringe betekenis.[2] Zoals voor de gehele politietaak geldt, gebeurt dit in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels.

Matrix en leeswijzer

Een gemengde OM- en politiewerkgroep is daarom aan het werk gegaan met het onderzoeken en uitwerken van een meer uitgebreid ondersteuningsdocument voor het bepalen van de relevante feiten en omstandigheden en het maken van bijhorende beslissingen. Dat is de matrix geworden die de bevoegdheden weergeeft voor de informatievergaring op het internet ten behoeve van niet-strafvorderlijk handelen.

De matrix heeft als doel om een helpende hand te bieden bij het afwegingsproces, de variatie in de uitkomsten van het afwegingsproces te verminderen en te zorgen voor een meer eenduidige interpretatie van de wet. Dit komt zowel de rechtsgelijkheid als de uitlegbaarheid in de dagelijkse uitvoeringspraktijk ten goede. Om met de matrix te kunnen werken is het van belang een aantal van de uitgangspunten te kennen die niet uitgesproken worden, maar wel ten grondslag liggen aan de werkingswijze.

Voor de inhoud en vormgeving van de matrix en toelichting is zoveel mogelijk aansluiting gezocht bij de matrix voor strafvorderlijk optreden. Toepasselijke en relevante tekstgedeelten zijn daarbij overgenomen.

[1] Voorbeelden van niet strafvorderlijk handelen zijn Toezicht, Openbare orde en veiligheid, Hulpverlening, Ondersteuning (sterke arm), Bewaken en beveiligen.
[2] Wanneer daar wel sprake van is, is daarvoor een wettelijke bevoegdheid vereist, zoals uitgeschreven in Strafvordering.

Uitgangspunten

Verkrijging en verwerking van informatie
De matrix gaat enkel over de titel van **verkrijging**. In de praktijk ontstaat nog weleens verwarring tussen het wettelijk regime voor verkrijging en verwerking. Op basis van de Wpg mag alleen persoonsgerelateerde informatie – zijnde 'politiegegevens' worden verwerkt die op rechtmatige wijze is verkregen. Deze matrix gaat niet over de verwerking onder het regime van de Wpg, maar over de legitieme verkrijging die daaraan vooraf gaat.

Niet-strafvorderlijk handelen
De matrix gaat over informatievergaring in het kader van **niet-strafvorderlijk handelen** en is dus niet bedoeld en niet geschikt als handreiking voor andere zaken dan niet-strafvorderlijk handelen. Deze matrix richt zich dan ook op de taken in het kader van de handhaving van de openbare orde, de hulpverlening, het optreden als de sterke arm, het bewaken en beveiligen van personen en de toezichtstaken op grond van bestuurswetgeving. Te denken is aan wetgeving op het gebied van milieu, transport, Drank- en Horeca, prostitutie, etc. Kortom wetgeving waarbij een bestuursorgaan (minister, college van GS of van B&W, of de burgemeester als bestuursorgaan) belast is met de handhaving ervan – en dus het bevoegd gezag is. Daarbij is de politie in een aantal gevallen als (mede-) toezichthouder aangewezen. De daarbij behorende bevoegdheden zijn bepaald in Hoofdstuk 5 van de Algemene wet bestuursrecht, tenzij in de betreffende wet anders is bepaald.

Taken	Voorbeelden	Bevoegdgezag
Toezicht	• Wet wapens en munitie • Vreemdelingenbeleid • Horeca en coffeeshops • Prostitutie	Bestuursorgaan
Openbare orde en veiligheid	• Preventie van de verstoring van de openbare orde • Ter voorbereiding op politieoptreden • Incidenten (waaronder rampen, crises en branden)	Burgemeester
Hulpverlening	• Vermissingen en andere zoekacties	Burgemeester
Ondersteuning (sterke arm)	• Bijstand aan bestuursorganen, gerechtsdeurwaarder,etc. (bijvoorbeeld bij ontruimingen)	Bestuursorgaan
Bewaken & Beveiligen	• Het beschermen van personen	Burgemeester

Op basis van niet-strafvorderlijk verkregen informatie kan uiteindelijk wel een strafvorderlijk onderzoek worden ingesteld. Indien bijvoorbeeld wordt gemonitord op de heer Wilders en er binnen zijn Facebook- of Twitter-account een directe dreiging wordt aangetroffen, kan dit leiden tot de identificatie van de dreiger en uiteindelijke vervolging. In dat geval geldt vanaf de fase van opsporing het strafvorderlijk kader. Ook sturings- of wegingsinformatie valt hier in beginsel onder, inclusief de "pre-weeg", zelfs als deze geheel is verzameld binnen de kaders van artikel 3 Pw. In dit geval geldt de matrix voor strafvorderlijk optreden.

Stelselmatigheid
Een belangrijk criterium in de strafvordering voor de mate van inbreuk op de persoonlijke levenssfeer die de toepassing van een bevoegdheid maakt, is de stelselmatigheid in de toepassing ervan. **Stelselmatigheid** dient te worden beoordeeld op basis van de **combinatie van** de verschillende inbreuken. Omdat vergaring van informatie in het kader van niet-strafvorderlijke handelen geen expliciete bevoegdheden kent, kan ook het criterium stelselmatigheid niet gebruikt worden. Bij niet-strafvorderlijk handelen zijn de basiscriteria: subsidiariteit en proportionaliteit. Bij monitoring (op basis van artikel 3 van de Politiewet) moet dus afgewogen worden of de inbreuk op de persoonlijke levenssfeer nog voldoet aan deze criteria. Stelselmatigheid c.q. 'het verkrijgen van een min of meer compleet beeld van iemands persoonlijke leven' uit Strafvordering biedt daarbij natuurlijk wel aanknopingspunten voor die afweging.

Het open/openbare internet

Bestaat niet. Althans (de mate van) het openbare karakter is voor de bepaling van de mate van inbreuk op de privacy van geen of beperkte waarde. Het begrip betreft een vereenvoudiging van de in strafvorderlijk kader noodzakelijke privacy afweging die niet meer past in deze tijd. Ook is in het kader van de toekomstbestendigheid van deze handreiking aandacht besteed aan de komende Europese **Richtlijn** betreffende **Dataprotectie**.[3] Deze gaat zeer sterk uit van de **intentie van het datasubject**[4] en de daarmee samenhangende **expectation of privacy**. Tenzij op basis van objectieve feiten en omstandigheden kan worden vastgesteld dat het niet anders kan dan dat **datasubject *zelf*** informatie openbaar heeft willen maken, is het niet openbaar en valt het onder de **bescherming van artikel 8 EVRM**. Het feit dat **derden informatie over een datasubject** hebben **publiek** gemaakt**,** maakt deze informatie voor de privacy-afweging **nog niet zonder meer openbaar.** Van belang is dat de betreffende gegevens door datasubject *zelf* en *bewust* moeten zijn vrijgegeven. Het feit dat de informatie door anderen[5] is vastgelegd of openbaar gemaakt doet niets of weinig af aan de mate van privacy-inbreuk. Het feit dat 'het gewoon via google' te vinden is, is in dit kader niet relevant. Facebook lijkt in eerste instantie een open platform, maar kan niet als zodanig worden beschouwd.
Elke inbreuk op de privacy moet dan voldoen aan de voorwaarden van artikel 8 EVRM, waarbij **artikel 3 Politiewet geen toereikende basis meer biedt zodra er sprake is van een 'verdergaand dan geringe inbreuk'**.

Meerdere/herhaalde weegmomenten

Het zal vaak voorkomen dat een site of app of andere **omgeving meerdere deelgebieden** kent, die allemaal een wat anders bedoelde openbaarheid hebben. Daarvoor moeten dus **aparte afwegingen** worden gemaakt. Ook zal het voorkomen dat de aard/inbreuk van de onderzoekshandelingen gedurende het onderzoek in (gecombineerde) zwaarte toe- of afneemt. Ook dan moet opnieuw een afweging worden gemaakt. Men kan dus niet door blijven werken op de eenmalig (aan het begin) gemaakte inschatting.

Vastlegging

Na een zoekhandeling is het belangrijk om de gevonden informatie te beoordelen en alleen de relevante/noodzakelijke informatie op te slaan. Voor het opslaan van informatie dient geredeneerd te worden vanuit het privacy-perspectief. Hoe meer wordt vastgelegd hoe groter de inbreuk op de privacy. **De enkele vastlegging van opsporingswege** van gegevens te herleiden op personen is op basis van Europese rechtspraak al **per definitie een privacy inbreuk**, die gelegitimeerd moet kunnen worden. Of de gegevens belastend of ontlastend zijn is in dit kader niet relevant.
Bij elke vastlegging moet een **specifiek doel** benoemd kunnen worden en de vastlegging moet daaraan bijdragen. Gezien de taakopdracht van de Nederlandse politie is (mogelijk) bewijs van onschuld per definitie inbegrepen.

Uitdagingen bij informatievergaring op het internet voor niet-strafvorderlijk handelen

Bij niet-strafvorderlijk handelen speelt een aantal problemen die zich niet voordoen bij strafvorderlijk optreden:

- De handhaving van de openbare orde valt onder de verantwoordelijkheid van de burgemeester. In de praktijk is voor de Landelijke Eenheid, waaronder een team OSINT valt, een verantwoordelijk burgemeester veelal moeilijk aan te wijzen.
- Afhankelijk van de deeltaak of het onderwerp waarop het handelen betrekking heeft, moet het bevoegd gezag geïdentificeerd worden. Deze is niet altijd eenvoudig aan te wijzen en heeft mogelijk weinig ervaring met onderzoekshandelingen op het internet.
- Binnen strafvorderlijke opsporing kent men de term stelselmatigheid als er een bovenmatige inbreuk ontstaat op de privacy van een verdachte. In het kader van niet-strafvorderlijke opsporing is er geen sprake van een verdachte en dient men de grenzen van proportionaliteit en subsidiariteit te waarborgen, terwijl deze niet nadrukkelijk zijn aangegeven. Gezien de aard van de taak is een mindere mate van inbreuk op de privacy toegestaan.
- De privacyregeling binnen artikel 8 EVRM, lijkt vrijwel geen ruimte over te laten voor onderzoekshandelingen door de politie.
- Het gebrek aan kennis bij het bevoegd gezag dat ver van de onderzoekshandelingen af staat (zoals een burgemeester).

---

[3] Volledig: RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, *de opsporing en de vervolging van strafbare feiten* of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens - COM(2012) 10 final 2012/0010 (COD) – thans nog in ontwikkeling.
[4] Datasubject is een term uit de Europese Dataprotectieregelgeving. Daarmee wordt bedoeld de persoon over wie de data gaat, zijnde 'de betrokkene' in de Wpg.
[5] Bijvoorbeeld partijen die online data van datasubjecten beschikbaar stellen.

Ook bij niet-strafvorderlijk handelen is het van belang zijn om de voorgenomen onderzoekshandeling vooraf te laten toetsen door iemand die zowel de vereiste deskundigheid daarvoor bezit en voldoende afstand heeft van het onderzoek om tot een onafhankelijke toetsing te kunnen komen. De privacyfunctionaris is hierbij de uitgelezen persoon. Een privacyfunctionaris kan ondersteunen bij de afweging voorafgaand aan de onderzoekshandeling, kan bepalen welk bevoegd gezag van toepassing is en kan indien gewenst helpen bij de afstemming tussen de operationele collega's en het desbetreffende bevoegd gezag.

Uitleg opbouw matrix en het gebruik ervan

Algemeen
De matrix is opgedeeld in twee hoofdcategorieën die oplopen in ernst van de inbreuk. Deze zijn op hun beurt weer opgedeeld in allerlei handelingen die uiteindelijk tot een oordeel leiden over proportionaliteit en subsidiariteit en dus een beslissing over al of niet doorgaan met zoeken op het internet.

Zoals hierboven is aangeven zijn bij de beoordeling van de vraag of gerechtvaardigd inbreuk wordt gemaakt op de persoonlijke levenssfeer van een persoon meerdere factoren van belang. Deze factoren en een aantal andere elementen die van invloed zijn op de mate waarin de privacy wordt geraakt, zijn benoemd en onderverdeeld in hun relatieve zwaarte. In de matrix zijn deze 'inbreuken op de privacy' in de kolommen aangegeven.

Om de matrix toe te passen zoek je in de rijen de handeling, of (combinatie van) zoekhandelingen, die je uitvoert (of degene die daar het meest op lijkt). Vervolgens loop je de kolommen af en vult deze in (per kolom set een keuze). De "zwaarste" inbreuk (af te leiden aan de kleur) is bepalend voor het al of niet stoppen met je onderzoek. Als je bijvoorbeeld ook maar één **paars** blokje treft, is de conclusie dat de handeling als "paars" geldt.

Met gebruik van de zoekfunctie in het programma dat je gebruikt om de matrix te bekijken (in de meeste gevallen ctrl-f of command-f) kun je snel zoeken in de matrix naar kernwoorden die van toepassing zijn op hetgeen je wilt gaan doen. Of je kunt gebruik maken van de beslisboom via Agora.

Gedurende de toepassing van de bevoegdheid kan een verschuiving plaatsvinden in de zoekhandeling die je verricht of een verandering in de zwaarte van de inbreuk (voorbeeld: je bevindt je in een openbaar chatkanaal met als doel het enkel waarnemen wie de andere deelnemers zijn, maar nu word je aangesproken door een van de deelnemers. Er vindt dus een verschuiving plaats van het enkel waarnemen naar een interactie); een heroverweging van de zoekslag dient dan plaats te vinden door de matrix/beslisboom opnieuw te doorlopen. Dit geldt ook indien de hoeveelheid te vergaren gegevens groter blijkt te zijn of gegevens gevoeliger blijken dan was ingeschat. Hiervoor moet opnieuw de matrix worden geraadpleegd. **Men kan niet volstaan met eenmalig een ingang kiezen in de matrix en aan die afweging vast blijven houden**.

Verschillende bevoegdheden:
In het schema wordt onderscheid gemaakt in de volgende bevoegdheidsniveaus aangegeven met een eigen kleur:

	= Blauw →	Handeling op grond van artikel 3 van de Politiewet. Geen afstemming/instemming nodig. Overleg wel met de privacyfunctionaris bij bijzonderheden.
	= Oranje →	Raadpleeg voorafgaand aan de handeling met de privacyfunctionaris af of overleg met bevoegd gezag verplicht is.
	= Paars →	Raadpleeg voorafgaand aan de handeling met de privacyfunctionaris. Overleg met het bevoegd gezag is in dit geval verplicht. Het bevoegd gezag kan bepalen of de handeling op grond van alleen artikel 3 van de Politiewet voortgezet mag worden, dan wel oordelen dat een vergaande inbreuk niet gerechtvaardigd is.
	= Kruis →	Niet van toepassing.

Neem bij twijfel of bijzonderheden altijd contact op met de privacyfunctionaris.

Beoordelingscriteria

De toelaatbaarheid van een concrete zoekhandeling wordt vastgesteld aan de hand van de volgende vragen:

- Op wie of wat is de zoekhandeling gericht?
- Is de met de zoekhandeling te maken inbreuk op de privacy proportioneel ten opzichte van het met de te verkrijgen informatie te bereiken doel?
- Is de zoekhandeling de minst bezwarende wijze waarop de informatie kan worden verkregen (subsidiariteit)?
- In welke mate wordt inbreuk gemaakt op de privacy?

De mate van inbreuk op de privacy wordt bepaald door:

- De mate van openheid van de gegevens (bijvoorbeeld door de aard van het platform en verwachtte privacy door het datasubject).
- De aard en de gevoeligheid van de gegevens.
- De vraag of de gegevens automatisch vergaard worden.
- De duur en intensiteit van het ophalen van de gegevens.
- De hoeveelheid te vergaren gegevens.
- De wijze waarop de vergaarde gegevens vastgelegd zullen worden.
- De vraag of het doel van de vergaring is om een min of meer compleet beeld te verkrijgen.
- De vraag of er sprake is van misleiding.
- De vraag of er sprake is van een combinatie van factoren of een contra-indicatie.

Toelichting op de matrix

In de toelichting hieronder staat uitleg bij een groot deel van de in de matrix gebruikte termen.

Informatie over	
Persoon die een potentieel risico vormt	Indien de te vergaren informatie gericht is op een persoon die een potentieel risico vormt. *Voorbeeld: stalkers, Potentieel Gewelddadige Eenlingen, potentiële recidivisten, jeugdigen*
Persoon die een potentieel risico loopt	Indien de te vergaren informatie gericht is op een persoon die een potentieel risico loopt. *Voorbeeld: bedreigde personen, herleidbare tipgevers en getuigen, vermiste personen, prominenten.* NB: De mate van inbreuk op de privacy van deze personen wordt eerder als ernstig aangemerkt dan die met betrekking tot een persoon of groep die een risico vormt.
Groepen die een potentieel risico vormen	Indien de te vergaren informatie gericht is op groepen die een potentieel risico vormen. *Voorbeeld: hooligans, jeugdgroepen, OMG's, extremistische groeperingen.*
Groepen die een potentieel risico lopen	Indien de te vergaren informatie gericht is op groepen die een potentieel risico lopen. *Voorbeeld: vluchtelingen, religieuze groeperingen.* NB: De mate inbreuk op de privacy van deze personen wordt eerder als ernstig aangemerkt dan die met betrekking tot een persoon of groep die een risico vormt.
Objecten/locaties/gebieden	Indien de te vergaren informatie gericht is op objecten en/of locaties. *Voorbeeld: gebouwen, verkeerspleinen, evenementlocaties.*
Overig	Indien de te vergaren informatie gericht is op andere personen/thema's dan hierboven vermeld. *Voorbeeld: verdachten of personen/thema's gerelateerd aan verdachten.* NB: Wanneer deze optie wordt gekozen betekent dit dat het niet toegestaan is om alleen op grond van de politiewet informatie te verzamelen in het kader van niet-strafvorderlijk handelen.
Proportionaliteit	Past de mate van inbreuk op de privacy van het onderzochte subject bij het doel waarop de onderzoekshandeling zich richt? Algemene beginselen met betrekking tot proportionaliteit: Past het middel bij het doel en de verwachte impact? Daarbij dient in aanmerking te worden genomen dat: • informatievergaring over een dader eerder proportioneel is dan over een derde; • informatievergaring over een derde sneller disproportioneel is, indien reeds een dader in beeld is; • informatievergaring binnen een omgeving die "niet deugt" eerder proportioneel is dan informatievergaring binnen een neutrale omgeving; • informatievergaring die niet gericht is op het vooraf gedefinieerde doel niet of minder proportioneel is (zgn. 'schot hagel').
Subsidiariteit	Kan het resultaat op minder ingrijpende manier worden behaald, bijvoorbeeld op een andere manier?
Mate van inbreuk op privacy m.b.t.:	
Gevoelige aard van de gegevens	Is naar verwachting sprake van gevoelige gegevens als bedoeld in artikel 5 van de Wet politiegegevens: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging.

	In de toekomst zullen hieronder vermoedelijk ook biometrische gegevens gaan vallen. Daaronder worden onder andere ook gelaatskenmerken gerekend.
Herkomst, locatie, afgebakende ruimte (bedoeld om privé te zijn)	Denk hierbij aan: Is aan de plaats/omgeving waar de gegevens gezocht gaan worden al duidelijk af te leiden of de gegevens bedoeld zijn om privé te zijn? Zijn de gegevens duidelijk afkomstig van een misdrijf (bv. hack)
Wijze vergaring automatisch?	Wordt er gebruik gemaakt van specifiek daarvoor ontworpen vergaringssoftware of -technieken? (bv. webcrawlers). Let ook op bij het gebruik van in een applicatie of omgeving ingebouwde functionaliteiten (bv RSS-feeds, automatische alerts op fora of van google)
Duur en intensiteit (kijk daarbij ook terug in tijd - het gaat om de gecombineerde inbreuk! - zie uitgangspunten)	Is de te verwachten duur of intensiteit van de gegevensvergaring dusdanig dat gesproken kan worden van het ontstaan van een min of meer compleet beeld van (aspecten van) iemands persoonlijk leven? Hierbij dienen ook eerdere soortgelijke informatie vergarende handelingen betrokken te worden, daarmee kan een compleet beeld immers ontstaan. Denk bij het beoordelen van intensiteit ook aan: herhaalde handelingen, het gebruik van meerdere zoektermen, het gebruik van geautomatiseerde systemen waardoor structuren, verbanden en netwerken in kaart gebracht worden. Gebruik daarvan maakt al snel dat de intensiteit hoog is. Indien hiervan sprake is controleer dan of nog steeds gebruik wordt gemaakt van de meest van toepassing zijnde activiteit in de matrix (de juiste rij).
Hoeveelheid te vergaren gegevens	Is de te verwachten hoeveelheid gegevens groot of klein.
Vastleggen van gegevens in enig bedrijfsprocessensysteem	Hoe zullen de verkregen gegevens worden vastgelegd in een bedrijfsprocessensysteem: integraal, beperkt voor zover ze relevant zijn of geheel niet. Met integraal opslaan wordt bedoeld dat alle vergaarde informatie wordt opgeslagen, ongeacht of het nuttig is en zonder dat de vergaarde informatie wordt beoordeeld. Integraal opslaan van informatie is in dit kader niet toegestaan. NB: hier dient te worden geredeneerd vanuit het privacy-perspectief. Hoe meer wordt vastgelegd hoe groter de inbreuk op de privacy. Of de gegevens belastend of ontlastend zijn is in dit kader niet relevant. NB: ook als de gegevens zelf niet worden vastgelegd moet wel enige vermelding van de verrichte onderzoeks- of verzamelhandelingen worden vastgelegd/geverbaliseerd met opgaaf van reden niet-opname.
Doel of verwachting verkrijgen min of meer compleet beeld	Is het doel of de verwachting van de informatievergaring het krijgen van een min of meer compleet beeld van (een deel) van iemands leven? *Dit is een controlevraag.*
Misleiding	Zal er op enigerlei wijze sprake zijn van misleiding bij het vergaren van de informatie? Denk hierbij niet alleen aan het gebruik van valse persoonsgegevens in profielen en het gebruik van nicknames, maar ook of er sprake kan zijn van een ruimere toegang tot een bepaalde omgeving door afscherming van de politieafkomst. Het enkele verzwijgen/verhullen van de politieomgeving is al (lichte) misleiding. Informatie van websites kan immers beperkter zijn indien die vanuit een bekende opsporingsomgeving wordt benaderd. Het gebruik van IRN is hiervan een voorbeeld. Ook het gebruik van een webcrawler kan misleiding opleveren. Het gebruik van TOR door een politieambtenaar maakt daarentegen niet dat er sprake is van misleiding, met name niet waar het gebruik van een anoniem/pseudoniem gebruikelijk is. Indien sprake is van actieve/gerichte misleiding (i.t.t. meer passieve misleiding zoals het hanteren van het in die omgeving passend pseudoniem) is vrijwel altijd sprake van een zwaardere inbreuk op de persoonlijke levenssfeer.
Combinatie van factoren of contra-indicatie	Is er sprake van een combinatie van voorgaande criteria of een contra-indicatie waardoor de bevoegdheid zwaarder uitvalt? Bijvoorbeeld in geval iemand zich als een ander heeft voorgedaan, terwijl duidelijk is dat die ander de informatie niet zelf heeft geplaatst.

Omgevingen	
Omgeving zonder deurbeleid	Website, social media, forum, nieuwsgroep o.i.d., of het deel daarvan waarvoor geen enkele vorm van registratie nodig is om gegevens te kunnen benaderen.
Omgeving met deurbeleid	Website, social media, forum, nieuwsgroep o.i.d. of het deel daarvan waar wel een deurbeleid gepretendeerd wordt, maar feitelijk niet gehandhaafd wordt. Bijvoorbeeld als verstrekte identificerende gegevens helemaal niet geverifieerd worden. Ook het moeten doen van een creditcardbetaling die voorts alleen als verkapte leeftijdsverificatie wordt gebruikt valt hieronder. Dit dient dus onderzocht te worden. Indien dit niet uit onderzoek kan blijken dan wordt gehandeld alsof er strikt deurbeleid is.
Omgeving met strikt deurbeleid	Website, social media, forum, nieuwsgroep o.i.d. of het deel daarvan waar een deurbeleid wordt gehanteerd, bv alleen op uitnodiging, aan een of andere eis moeten voldoen (bv. x-aantal posts, materiaal leveren), of daadwerkelijke verificatie van gegevens.
Nog enkele overwegingen	
Wel/geen verdachte omgeving:	Informatievergaring binnen een "strafbare omgeving" levert naar het zich laat aanzien een lichtere inbreuk op, die inbreuk komt aan de orde bij de proportonaliteitsafweging.
TOR	TOR is op zich niet anders dan www, je hebt er alleen (andere) software voor nodig. Privacy schending voor www en TOR is daarom hetzelfde.
Overwegingen beeld- en geluidsites	Er is op zich geen reden om een grotere privacy schending aan te nemen bij beeld - en geluidssites. Het gaat om de te verwachten inhoud van de gegevens, een stuk tekst kan meer gevoelige informatie bevatten dan 100 foto's afkomstig van dezelfde persoon. Bij de criteria "gevoelige aard van de gegevens "en "verkrijgen min of meer compleet beeld" zal dit meewogen moeten worden.

Ter afsluiting

Het gebruik van de matrix en leeswijzer Informatievergaring op het internet voor niet-strafvorderlijk handelen is niet vrijblijvend. Hoewel de matrix en leeswijzer zoveel mogelijk een weergave zijn van de huidige stand van zaken en de in de nabije toekomst te verwachten ontwikkelingen is een aantal ontwikkelingen nog niet geheel te duiden. Als gevolg van deze ontwikkelingen kan de inhoud van de matrix en de leeswijzer nog gewijzigd worden.

De matrix en leerwijzer zijn expliciet bedoeld om 'levende documenten' te blijven. Mochten er ontwikkelingen zijn waarvan de gebruiker meent dat deze niet of niet langer volledig/juist in de matrix en leeswijzer zijn verwerkt dan kunnen deze worden opgestuurd – bij voorkeur via het Landelijk Coördinatie Overleg OSINT- of via het Kennis en Leer Centrum van de Landelijke Eenheid – DLOS. Deze zullen dan bij de volgende update worden verwerkt. Gebruikers wordt gevraagd om dergelijke zaken ook daadwerkelijk door te geven zodat de matrix en de leeswijzer zijn doel kunnen blijven vervullen. Ook andere tips, opmerkingen of verbeteringssuggesties zijn welkom.

Tot slot hoopt de werkgroep met de matrix en leeswijzer producten opgeleverd te hebben die in de dagelijkse praktijk behulpzaam zijn bij het maken van de vele, vaak lastige, noodzakelijke afwegingen.

Bij de totstandkoming van de matrix en leeswijzer zijn betrokken:

Politie

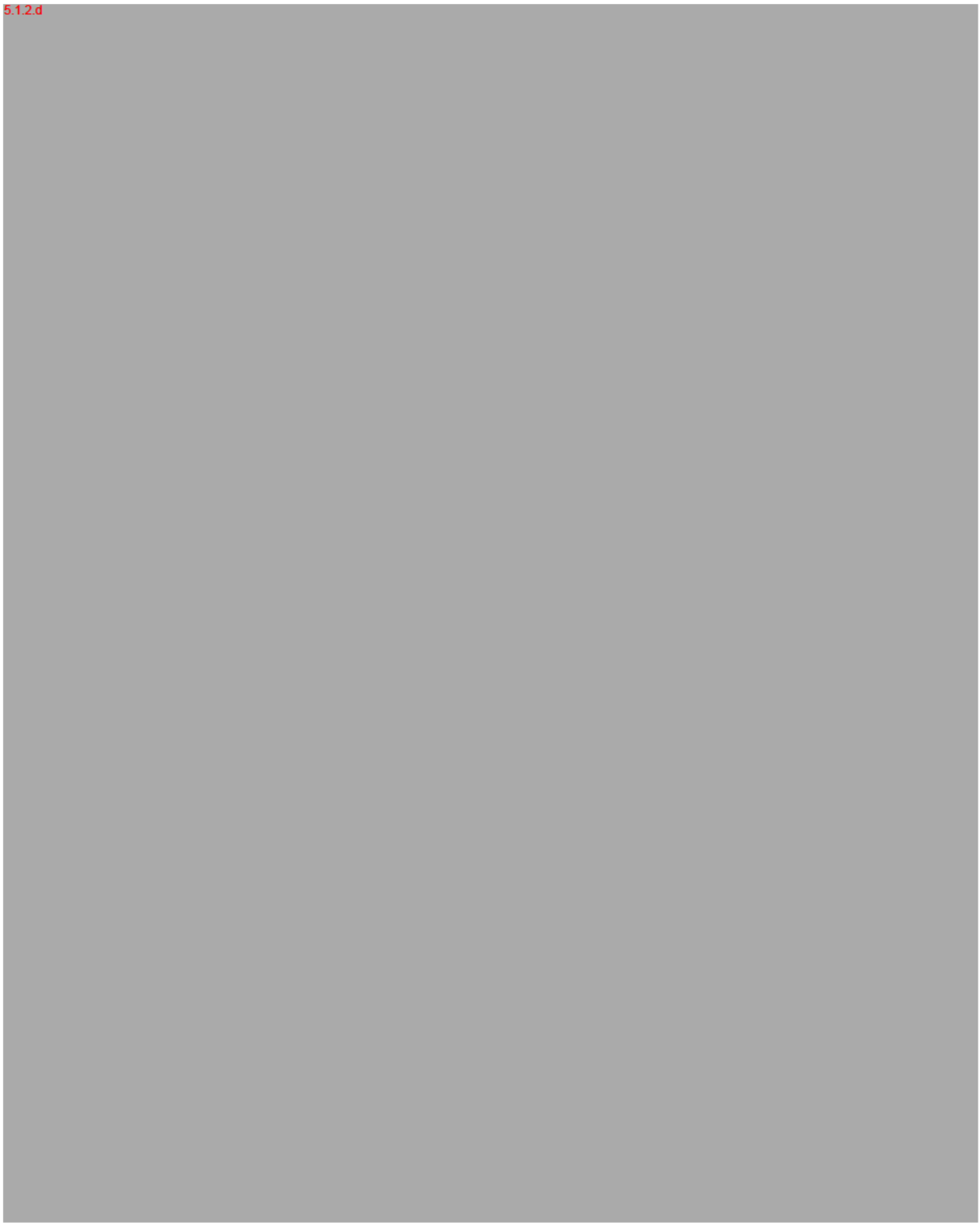
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e (Politieacademie)
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e
- 5.1.2.e

Openbaar Ministerie

- 5.1.2.e

Gemeenten

- 5.1.2.e, gemeente Bergen op Zoom
- 5.1.2.e, gemeente Leeuwarden


5.1.2.d