

Juridische analyse
internetonderzoek
Belastingdienst

Een eerste
verkenning

& team OSINT – dec. 2020



Inhoud

Hoofdstuk 1 Inleiding.....	5
1.1 Aanleiding en context.....	5
1.1.1 Mate van privacy-inmenging.....	5
1.2 Huidige praktijk en probleemstelling.....	6
1.3 Kernvraag.....	7
1.4 Reikwijdte van deze analyse.....	7
1.4.1 Leidraad Juridisch Kader Internetonderzoek.....	7
1.4.2 Geen toetsing op onderzoeksbevoegdheid/legitimiteit.....	8
1.4.3 Internetonderzoek.....	8
1.4.4 AVG.....	8
1.5 Leeswijzer.....	8
Hoofdstuk 2 Wat houdt een internetonderzoek door OSINT in?.....	8
2.1 Begrip internetonderzoek.....	8
2.1.1 Het internet als bron.....	9
2.2.2 Verschillende typen internetonderzoek.....	9
2.2.3 Verder onderscheid aan de hand van diverse factoren.....	10
2.2.3.1 Onderscheid op basis van aanleiding.....	10
2.2.3.2 Onderscheid op basis van onderzoeksdoel.....	10
2.2.3.3 Onderscheid aan de hand van normen.....	10
2.2.3.4 Tussenconclusie.....	11
2.2 Begrip openbare online bron.....	11
2.2.1 Definitie open bron.....	11
2.2.2 Reikwijdte begrip open bron.....	12
2.2.2.1 Betaalde diensten.....	13
2.2.2.2 Gestolen gegevens.....	13
2.2.2.3 Dark web.....	14
2.2.2.4 Inloggen met een account.....	14
2.2.2.5 Herkomst van gegevens: Menselijke bron.....	15
2.2.2.6 Tussenconclusie.....	15
2.2.3 De OSINT-middelen en bronnen.....	16
2.2.4 Conclusie.....	16
Hoofdstuk 3 Wettelijk kader.....	16
	1

3.1 Verwerking van persoonsgegevens bij internetonderzoek.....	16
3.1.1 De AVG.....	17
3.1.2 Tussenconclusie.....	18
3.1.3 Grondwet en artikel 8 EVRM.....	18
3.1.4 Handvest Grondrechten EU.....	18
3.1.5 Conclusie.....	18
Hoofdstuk 4 Rechtmatigheid internetonderzoek.....	19
4.1 Rechtmatig.....	19
4.1.1 Is er sprake van een geldige grondslag bij internetonderzoek?.....	19
4.1.2 AVG grondslag.....	19
4.1.3 Nationale grondslag.....	19
4.1.4 Voorzienbaarheid en artikel 8 EVRM.....	20
4.2 Jurisprudentie.....	20
ANPR.....	20
Cameratoezicht.....	20
Trans link.....	20
Scanauto's.....	21
Compleet beeld.....	21
SyRi.....	21
Museumjaarkaart.....	21
EHRM.....	22
4.2.1 Tussenconclusie.....	22
4.3 Noodzaak.....	23
4.3.1 Noodzaak en internetonderzoek.....	23
4.3.2 Ernst van de inmenging.....	23
4.3.3 Voorafgaande schriftelijke beoordeling.....	23
4.3.4 Factoren.....	24
4.3.4.1 Glijdende schaal ernst inbreuk.....	24
4.3.4.1 Omslagpunt ontbreekt.....	24
4.4 Dataminimalisatie en doelbinding.....	24
4.5 Informatieplicht/transparantie.....	25
4.5.1 Informatieplicht ten behoeve van individuen.....	25
4.5.2 Sectorspecifieke wetgeving mogelijk nodig.....	26
4.5.3 Informatieplicht bij algoritmen.....	26
4.6 Juistheid van gegevens.....	27
4.7 Beveiliging en opslag.....	27

4.8 DPIA.....	27
4.9 Conclusie.....	28
Hoofdstuk 5 Enkele juridische uitdagingen/risico's.....	28
5.1 Geen specifieke wettelijke grondslag voor internetonderzoek.....	28
Tussenconclusie.....	30
5.2 Grote schaal: crawlen.....	30
Tussenconclusie.....	31
5.2.1 Crawlen en de Belastingdienst.....	31
5.3 Grote schaal: scraping.....	32
Tussenconclusie.....	32
5.4 Heimelijk waarnemen.....	32
5.4.1 Grote schaal én heimelijk = DPIA.....	33
5.5 Gefingeerde accounts.....	34
5.6 'Bijvangst'.....	34
Tussenconclusie.....	36
5.7 Bijzondere persoonsgegevens.....	36
Tussenconclusie.....	37
5.8 Bestandskoppeling.....	37
5.9 Verantwoordingsplicht en privacy by design and default.....	37
Tussenconclusie.....	38
5.10 Conclusie.....	38
Hoofdstuk 6 Conclusie en samenvatting.....	38
6.1 De belangrijkste beheersmaatregel: focus op zorgvuldigheid, motivering en aantoonbaarheid.....	38
6.1.1 Noodzakelijk voor algemeen belang.....	38
Proportionaliteit: mate van Inbreuk.....	39
Beoordeling vooraf.....	39
Factoren.....	39
6.1.2 Karakter van internetonderzoek.....	39
6.1.3 Zorgvuldigheid, motivering en aantoonbaarheid.....	40
Enkele beheersmaatregelen.....	40
6.2 Tot slot.....	40
Bijlagen.....	42
17 factoren voor de toets 'mate van inbreuk'.....	42
Vragenlijst protocol.....	44
Mogelijke zoekhandelingen.....	46

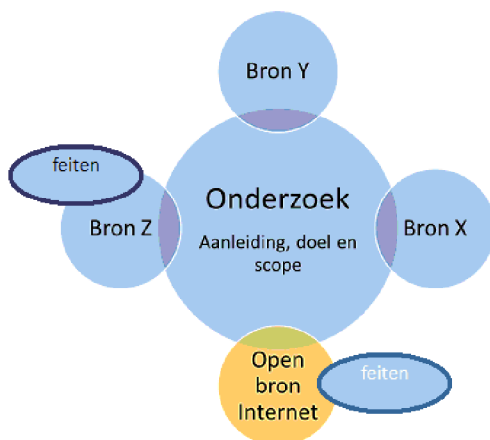
OSINT-tools.....	47
WP29 – Overzicht Verwerkingen met ‘waarschijnlijk een hoog risico’.....	48

Hoofdstuk 1 Inleiding

1.1 Aanleiding en context

De Belastingdienst wil graag via OSINT-middelen¹ internetonderzoek verrichten. De Belastingdienst heeft reeds toegang tot diverse, al dan niet interne, databronnen (zie figuur 1). Echter bestaat een gat tussen de gegevens die de Belastingdienst heeft uit deze databronnen (wettelijke registers, data van banken en aangiften etc., ook wel de administratieve werkelijkheid genoemd) en de economische werkelijkheid. Deze economische werkelijkheid is (deels) goed zichtbaar via openbaar toegankelijke bronnen op internet. Het verschil tussen beide werkelijkheden kan enerzijds verklaard worden door een gebrek aan bewustzijn bij de belastingbetaler. Hier gaat het dan vaak om 'onbewuste onbekwaamheid'. Voor de Belastingdienst is hier een actieve(re) rol weggelegd om de onbekwame belastingplichtigen op juiste wijze te informeren over de verplichting tot het betalen van belasting. Anderzijds is het verschil tussen de administratieve en economische werkelijkheid te verklaren door opzettelijke belastingontwijking of belastingontduiking.

Openbare bronnen op internet vormen een informatiebron die deze werkelijkheid (deels) relatief eenvoudig kan onthullen, zodat handhaving kan plaatsvinden en hiermee de non-compliance van de belastingplichtige deels opgeheven kan worden.² Via OSINT-middelen kan bijvoorbeeld in een korte periode, met relatief weinig capaciteit, een groot aantal gemiste inkomstenbronnen uit kamerverhuur gedetecteerd worden die niet zijn opgegeven bij de aangifte. In korte tijd kunnen veel meer en diverse gegevens onderzocht worden dan handmatig ooit mogelijk zou zijn. Het internet – al dan niet ontsloten via OSINT-middelen – is dus een extra databron die de Belastingdienst op rechtmatige wijze wil ontsluiten. Het team OSINT van DF&A laat een juridische verkenning uitvoeren door middel van onderhavige analyse.



Figuur 1

1.1.1 MATE VAN PRIVACY-INMENGING

De Belastingdienst heeft een wettelijke taak tot heffen en innen van belasting met betrekking tot inkomsten. Het zoeken naar feiten via openbare bronnen op internet ten aanzien van inkomsten, bezit, verblijfplaats van belastingplichtigen etc. kan bijdragen aan dit legitieme doel.

¹ OSINT: Open Source Intelligence. Hieronder wordt verstaan het verzamelen en analyseren van data uit open bronnen met bepaalde (software)technieken. Zie ook: https://en.wikipedia.org/wiki/Open-source_intelligence

² Overigens hoeft onderzoek door de Belastingdienst niet altijd tot punitieve handhaving te leiden. Afhankelijk van de gekozen handhavingstrategie kan gekozen worden voor meer bewustwording bij de belastingplichtige ten aanzien van de regels, zie hiervoor de Handhavingstrategie.

Echter brengt het opsporen van persoonsgegevens via internet een bepaalde mate van privacy-inmenging met zich mee, dat een inbreuk vormt op een grondrecht (recht op privacy). Afhankelijk van de omstandigheden kan een dergelijke inbreuk noodzakelijk zijn en toelaatbaar. Echter kan zo'n inbreuk ook te ver gaan en dus in strijd zijn met de belangen van de betrokkenen³. Waar het omslagpunt ligt is niet altijd duidelijk. Dit stuk betreft een eerste verkenning van deze mate van privacy-inmenging en hoe wet, jurisprudentie en literatuur hiermee omgaan. Niet op alle onderwerpen zal een verdiepingsslag plaatsvinden, daar de tijd ontbreekt. Echter biedt dit stuk een basis voor verdere analyses.

1.2 Huidige praktijk en probleemstelling

Concrete regelgeving over het verrichten van internetonderzoek door bestuursorganen bestaat (nog) niet. Internetonderzoek vindt echter reeds plaats door bestuursorganen⁴ en ook door de Belastingdienst⁵. Zo kan bijvoorbeeld een LinkedIn pagina geraadpleegd worden door een inspecteur van de Belastingdienst om een eerste controle te doen of iemand in loondienst is of niet.^{6 7} Dit leidt tot de vraag wat nu exact het probleem is.

Een *oppervlakkige* beschouwing van de rechtspraak leert ons dat de rechter internetonderzoek niet als een ernstige mate van privacy-inmenging ziet of het beoordeelt als bevoegdheidsoverschrijding. Echter komt dat mede voort uit het feit dat weinig burgers expliciet of nauwgezet beargumenteerd beroep hebben gedaan op hun grondrecht. Tevens is nog niet de bevoegdheid van de Belastingdienst om dit soort onderzoek te verrichten ter discussie gesteld. Dit betekent dat dit onderwerp dan ook niet behandeld zal worden door de rechter.⁸ En in sommige uitspraken lijkt de rechter geen verdiepende analyse te willen verrichten. Al met al is hierdoor weinig jurisprudentie beschikbaar dat helpt bij de specifieke beoordeling wat nu exact wel en wat nu niet mag met betrekking tot internetonderzoek en privacy. Daarentegen bestaat een aantal (internationale) uitspraken waaruit duidelijk blijkt wat absoluut niet mag met betrekking tot het gebruik van persoonsgegevens tijdens een onderzoek⁹. Het grijze gebied tussen wat absoluut niet mag en wat mogelijk wel mag, is het onderzoeken waard voor de OSINT-praktijk. Ook in de literatuur bestaat de wens voor een verdiepende analyse wat betreft gebruik van persoonsgegevens bij internetonderzoek.¹⁰

De Belastingdienst dient voor elk onderzoek de vereisten van proportionaliteit en subsidiariteit in acht te nemen. Dit kan iets lastiger zijn wanneer het internet als bron wordt gebruikt, immers is internet als bron diffuus en ongestructureerd, in tegenstelling tot de interne, afgebakende bronnen zoals de Basis Registratie Persoonsgegevens. Afhankelijk van de te gebruiken zoektechnologie, het doel van de zoekactie en de hoeveelheid en aard van de historische persoonsgegevens die in open bronnen worden gedeeld, kan bij een geavanceerde éénmalige vastlegging van gegevens al sprake zijn van een meer dan geringe mate van inbreuk in iemands privéleven doordat in de gevonden gegevens een min of meer volledig beeld besloten ligt van bepaalde aspecten van het persoonlijk

³ Een natuurlijk persoon wiens persoonsgegevens worden verwerkt.

⁴ Zie bijvoorbeeld een uitspraak van de Rechtbank Den Haag van 27 juni 2017 in het vreemdelingenrecht, waar het bewijs afkomstig van Facebook niet ter discussie staat: ECLI:NL:RBDHA:2017:7852

⁵ Een 'stappenplan' in de vorm van tips is reeds beschikbaar voor de medewerker van de Belastingdienst die een internetonderzoek wil verrichten. De Leidraad Juridisch Kader Internetonderzoek (hierna: de Leidraad) geeft eveneens instructies voor internetonderzoek bij het toezicht op een individuele belastingplichtige.

⁶ Zie bijvoorbeeld uitspraak van Rechtbank Noord-Holland van 12 september 2018 waarin de inspecteur de profielpagina op LinkedIn heeft gebruikt in zijn onderzoek (ECLI:NL:RBNHO:2018:7806).

⁷ Zie instructie voor de medewerkers: stappenplan internetonderzoek

<http://internetservice4u.belastingdienst.nl/zoektipspost/10-stappenplan-internetonderzoek/>

⁸ Art. 8:69 lid 1 Awb

⁹ Zie bijvoorbeeld de ANPR-arresten, waarover later meer.

¹⁰ Zie 'Internetonderzoek door bestuursorganen, p. 7' van hoogleraren J. Oerlemand & Y. Schuurmans en Commissie Koops met aanbevelingen met betrekking tot wijziging van het Wetboek van Strafvordering.

leven van betrokkene. Dit betekent dat het voor de Belastingdienst gewenst is om vooraf te weten of de Belastingdienst een risico loopt met het verrichten van internetonderzoek. Het onderhavige stuk is een eerste juridische verkenning met betrekking tot internetonderzoek en de privacyaspecten hiervan.

1.3 Kernvraag

De vraag die beantwoord dient te worden is:

Aan welke juridische voorwaarden met betrekking tot privacywetgeving dient de Belastingdienst te voldoen om in lijn met wet-en regelgeving een internetonderzoek uit te mogen voeren.

Om bovenstaande vraag te kunnen beantwoorden, zullen onderstaande vragen aan bod komen:

- 1. Wat houdt een internetonderzoek in?**
- 2. Wat houden de wettelijke regels en jurisprudentie in?**
- 3. Wat zijn de mogelijke juridische obstakels?**
- 4. Wat zijn mogelijke maatregelen?**

1.4 Reikwijdte van deze analyse

1.4.1 LEIDRAAD JURIDISCH KADER INTERNETONDERZOEK

Bij het opstellen van de juridische analyse en het protocol is getracht de Leidraad Juridisch Kader Internetonderzoek als startpunt te gebruiken. Het voornemen was om de stellingen en uitgangspunten in deze Leidraad niet ter discussie te stellen. Echter bleek, na interne beraadslaging, dat een zelfstandige analyse de voorkeur had, om drie redenen. De eerste reden betreft dat ten onrechte het beeld wordt geschetst in de Leidraad dat 'toezicht op een *individuele* belastingplichtige' door een medewerker van de Belastingdienst minder impactvol is voor betrokkene dan internetonderzoek door gespecialiseerde teams zoals team OSINT van DF&A. Dit terwijl in de praktijk ook enkele zoekslagen naar één individuele belastingplichtige al een dusdanige privacyinbreuk kunnen opleveren dat de vraag gesteld kan worden of dit altijd is toegestaan vanuit privacy-oogpunt.¹¹

Ten tweede viel op dat een wezenlijk onderdeel van de Leidraad - namelijk de beschrijving van de onderzoeksbevoegdheid van de Belastingdienst in het algemeen - en het onderdeel internetonderzoek specifiek, onvoldoende concreet was uitgewerkt. Dit biedt onvoldoende handelingsperspectief voor de gebruiker, in dit geval team OSINT.¹²

Ten derde wordt in de Leidraad geadviseerd om per OSINT-middel (techniek/softwareprogramma), per zoekmethode (onderzoeksmethode van de inspecteur), per vindplaats én per verwerking te beschrijven wanneer en door wie dit gebruikt mag worden. Deze categorisering blijkt niet opportuun in de praktijk. Zo is het bijvoorbeeld afhankelijk van de instellingen van een technisch OSINT-zoekmiddel als scraping hoeveel persoonsgegevens gevonden zullen worden, en dus hoe ernstig de mate van inbreuk in persoonlijke levenssfeer is met gebruik van deze techniek. Tevens is het in de praktijk niet werkbaar om met protocollen of instructies per zoektechniek te werken, omdat de

¹¹ Tevens kan de zoekslag van de inspecteur op Google ook al beschouwd worden als gebruik van OpenSourceIntelligence (OSINT).

¹² De Leidraad wordt momenteel herzien.

OSINT-middelen geen statische middelen zijn: de 'OSINT-wereld' betreft een dynamische wereld die continue onderhevig is aan verandering.

Gelet op bovenstaande is daarom gekozen voor een zelfstandige analyse van het juridisch kader. De Leidraad is in het onderhavige stuk buiten beschouwing gelaten, al vormen sommige punten uit de Leidraad wel een aanleiding voor een verdiepende analyse. Waar mogelijk komen deze punten later terug in dit stuk.

Onderhavige analyse betreft overigens een eerste verkenning en is geenszins uitputtend bedoeld, maar kan als basis dienen voor verdere verdieping en biedt een overzicht van eventuele obstakels.

1.4.2 GEEN TOETSING OP ONDERZOEKSBEVOEGDHEID/LEGITIMITEIT

Zoals hierboven al is opgemerkt is een wezenlijk onderdeel van een juridische analyse de uitwerking van de onderzoeksbevoegdheid van de Belastingdienst, de rechten en plichten van de Belastingdienst als bestuursorgaan op grond van haar publieke taak in het algemeen en met name ook van het onderdeel internetonderzoek. Deze onderwerpen zijn in deze analyse niet uitgewerkt, omdat het logischer is om dat onderdeel (gelet op de Belastingdienstbrede uitstraling) door de centrale stafdiensten van de Belastingdienst te laten uitwerken. (red.: Dit onderdeel zal naar verwachting begin januari door die diensten worden aangeleverd. Dit kan dan als bijlage bij deze analyse worden gevoegd.)

Dit betekent dat geen vragen worden beantwoord ten aanzien van de bevoegdheid van de Belastingdienst om internetonderzoek te doen, of de betreffende medewerker bevoegd is¹³ en of dit in lijn is met de algemene beginselen van behoorlijk bestuur.

Echter is de bevoegdheidsgrondslag een vereiste vanuit het privacyrecht. Dit zorgt deels voor een overlap met het vraagstuk ten aanzien van de bevoegdheid. Indien nodig worden aannames gedaan, om toch een juridische analyse te kunnen maken.

1.4.3 INTERNETONDERZOEK

'Onderzoek' is een breed begrip. In dit stuk zal met internetonderzoek vooral het internetonderzoek bedoeld worden dat gericht is op toezicht en handhaving (het bevorderen van de naleving van de belastingplichtige). De onderzoeken met als doel om trends en fenomenen te analyseren of het verrichten van onderzoeken ten behoeve van de wetenschap worden in dit stuk nagenoeg buiten beschouwing gelaten.

1.4.4 AVG

Onderliggende analyse is niet bedoeld als uitputtende beschouwing van alle onderwerpen in de AVG. Zo blijven de rechten van betrokkenen buiten beschouwing, evenals onderwerpen als profiling en anonimisering.

1.5 Leeswijzer

Om te kunnen bepalen of internetonderzoek nu mag, zal voor deze analyse eerst gekeken worden naar het internetonderzoek in het algemeen (hoofdstuk 2). Vervolgens zal een globaal overzicht van de wet –en regelgeving behandeld worden in hoofdstuk 3 en 4. Daarna zullen enkele obstakels uit de praktijk belicht worden in hoofdstuk 5 en volgt in hoofdstuk 6 een conclusie en samenvatting van het geschrevene.

¹³ Zo luidt een vraag: is elke medewerker wel bevoegd om een internetonderzoek via OSINT te starten? Zie bijvoorbeeld het woord 'inspecteur' in de Awr, mogelijk heeft niet iedereen die kwalificatie.

Hoofdstuk 2 Wat houdt een internetonderzoek door OSINT in?

2.1 Begrip internetonderzoek

Internetonderzoek is een breed begrip. Internetonderzoek bij het OSINT-team van de Belastingdienst houdt algemeen omschreven een *online* zoektocht in naar informatie uit *openbare* bronnen op het internet. Een digitaal/online openbronnenonderzoek dus. De OSINT-medewerkers hebben beschikking over speciale hardware en softwareprogramma's, die het mogelijk maken om anoniem (indien hier specifieke aanleiding voor is) en beveiligd gegevens te verzamelen via internet die noodzakelijk zijn voor een onderzoek.

2.1.1 Het internet als bron

Een zoekslag op internet houdt zoeken in een grote hoeveelheid informatie in. Het betreft een grote hoeveelheid gestructureerde en ongestructureerde data uit verschillende bronnen. Dat betekent dat van te voren – zonder voorzorgsmaatregelen - vaak niet duidelijk is óf, hoeveel en welke persoonsgegevens gevonden gaan worden. Dit in tegenstelling tot het zoeken in voor de Belastingdienst bekende en afgebakende bronnen.

Ook is bij internetonderzoek niet direct duidelijk of min of meer een compleet beeld van bepaalde aspecten van een persoonlijk leven zal ontstaan en of de privacyinbreuk dus meer dan gering is, iets wat relevant zal zijn voor het beantwoorden van de vraag of het verrichten van internetonderzoek mag. Een eigenschap van internet als bron is dus in zekere mate de onbeperktheid en hierbij de kans dat de Belastingdienst verweten wordt aan een 'fishing expedition' te doen. Al wordt dit niet zomaar aangenomen door de rechter, wanneer dit aangevoerd wordt door een belastingplichtige. Dit bleek recent nog uit een uitspraak van de Hoge Raad waarbij de belastingdienst betrokken was: het opvragen van privacy-gevoelig materiaal door de inspecteur was essentieel voor het onderzoek en daarom noodzakelijk in de zin van artikel 8 EVRM.¹⁴

2.2.2 Verschillende typen internetonderzoek

De Belastingdienst / team OSINT heeft geprobeerd om de verschillende verschijningsvormen van internetonderzoek te categoriseren. Deze categorisering is niet perfect compleet, maar biedt een meer overzichtelijk beeld van de verscheidenheid van typen internetonderzoek. Het betreft een onderscheid in twee typen internetonderzoek, namelijk subject/object georiënteerd onderzoek en niet-subject/object georiënteerd onderzoek.

1. Subject- en object georiënteerd internetonderzoek

- Gericht op één:
 - Natuurlijk persoon
 - Roerende of onroerend goed
 - Rechtsvorm
- Doel:
 - Gericht op het operationele niveau
- Voorbeelden:
 - Woonplaatsonderzoek
 - Persoonsonderzoek
 - Onderzoek naar een object (bezit: huis, auto, boot, vliegtuig, ect...)
 - Onderzoek naar een bedrijf

2. Niet subject- en object georiënteerd internetonderzoek

- Niet gericht op één maar op vele:

¹⁴ Zie Hoge Raad, 25 september 2020 (ECLI:NL:HR:2020:1473)

- Signalering van bewegingen en gebeurtenissen op internet
- Gericht op grotere groepen, focus op individuen is niet van belang
- Ontwikkelingen in de gaten houden
- Doel:
 - Gericht op het tactisch/strategische niveau
- Voorbeelden:
 - Doelgroep analyses
 - Fenomeenanalyses
 - Trendanalyse
 - Gebeurtenisanalyse

Ter toelichting:

Object van heffing gaat over de vragen: waar wordt inkomstenbelasting over geheven? Wat is de heffingsgrondslag?

Subject van heffing: wie is de belastingplichtige voor de inkomstenbelasting?

2.2.3 Verder onderscheid aan de hand van diverse factoren

Bovenstaand overzicht van type internetonderzoeken lijkt een uitputtend onderscheid, echter blijkt in de praktijk dat ook bij deze varianten weer subvarianten mogelijk zijn. Vanwege de variërende intensiteit van het internetonderzoek kan de ernst van de privacyinmenging van geval tot geval verschillen, evenals de rechtmatigheid van het onderzoek zelf. De vraag of een bepaald type internetonderzoek uitgevoerd mag worden, is na bovenstaande categorisering dus nog niet te beantwoorden. Hierna volgen enkele voorbeelden van aspecten of factoren die van invloed kunnen zijn voor het antwoord op de vraag of een internetonderzoek mag worden uitgevoerd of niet.

2.2.3.1 ONDERSCHIED OP BASIS VAN AANLEIDING

Zo is voor zowel subject-als object georiënteerd onderzoek ook nog een onderscheid te maken als we kijken naar de *aanleiding* van het internetonderzoek. Enerzijds is er internetonderzoek in de vorm van een *controle*, namelijk aan de hand van een aangifte onderzocht en controleert men de gegevens, al dan niet met behulp van een bron via internet.

Anderzijds is er internetonderzoek in de vorm van een *handhavingsvraagstuk*, dat start vanuit de vraag hoeveel en welke mogelijke overtreders er zijn ten aanzien van een bepaalde wettelijke verplichting. Dit wordt binnen de Belastingdienst ook wel fenomeenonderzoek genoemd. Hierbij is nog geen concrete belastingplichtige geïdentificeerd. Dit aspect beïnvloedt mogelijk de mate van inbreuk in de persoonlijke levenssfeer en het aantal betrokkenen dat hiermee te maken krijgt. Daarnaast is een juiste omschrijving van de aanleiding ook van belang om te kunnen voldoen aan – onder meer – de algemene beginselen van behoorlijk bestuur (evenredigheidsbeginsel, verbod op willekeur, gelijkheidsbeginsel, etc.).

2.2.3.2 ONDERSCHIED OP BASIS VAN ONDERZOEKSDOEL

Tevens kunnen de internetonderzoeken binnen de Belastingdienst een verschillend doel dienen: het onderzoek kan plaatsvinden ten behoeve van toezicht of handhaving¹⁵, maar het onderzoek kan ook plaatsvinden ten behoeve van informatievergaring in algemene zin voor de Belastingdienst, bijvoorbeeld om de informatiepositie te versterken en de burger beter te informeren. Dit beïnvloedt *mogelijk* de mate van inbreuk in de persoonlijke levenssfeer: een onderzoek naar algemene ontwikkelingen brengt *mogelijk* minder persoonsgegevens met zich mee dan een handavingsonderzoek. Een juiste omschrijving van het doel voorafgaand aan het onderzoek zal

¹⁵ Binnen de Belastingdienst wordt dit ook wel ‘verbijzonderd toezicht’ genoemd.

helpen bij de beoordeling hoe groot de mate van inbreuk is en is van belang om te kunnen voldoen aan – onder meer - de algemene beginselen van behoorlijk bestuur (evenredigheidsbeginsel, verbod op willekeur, gelijkheidsbeginsel, etc.).

2.2.3.3 ONDERSCHIED AAN DE HAND VAN NORMEN

Ook is vervolgens voor al deze varianten in internetonderzoek een onderscheid te maken aan de hand van de normering die getoetst wordt. Grofweg onderscheidt de wet drie type inkomstenbronnen waarvoor belastingwetgeving bestaat: winst, loon en overig. Het internetonderzoek naar een mogelijke overtreding in de categorie ‘winst’ zal wat betreft zoekhandelingen anders verlopen dan een internetonderzoek dat valt onder de categorie ‘overige inkomsten’. Een internetonderzoek naar de rechtmatigheid van het gebruik van bepaalde aftrekposten betreft bijvoorbeeld een andere norm dan het controleren of er sprake is van duurzaam deelnemen aan het economisch verkeer. De verschillende normen zullen verschillende zoekhandelingen, zoekmethoden, zoekresultaten en zoekinstructies opleveren. Wellicht is de kans op het vinden van bijzondere persoonsgegevens (die in principe verboden zijn om te verwerken) groter bij onderzoek die het fiscaal partnerschap in kaart brengt omdat de verplichting is opgenomen in wetsartikel X dan een onderzoek dat enkel bedrijfsgebouwgegevens wil controleren aan de hand van wetsartikel Y.

2.2.3.4 TUSSENCONCLUSIE

De verschillende internetonderzoeken variëren dus in intensiteit, onderzoeksopzet en zoekmethode. Afhankelijk van deze (en andere!) factoren zal ook de mate van inbreuk in persoonlijke levenssfeer verschillen, evenals de beoordeling of de Belastingdienst nog heeft gehandeld overeenkomstig de algemene beginselen van behoorlijk bestuur. Dit zal de uitkomst beïnvloeden van de vraag of een bepaald type internetonderzoek mag of niet.

NB. Dat betekent dat dit juridisch kader in combinatie met de aan te scherpen Leidraad wel een belangrijk startpunt is voor het beoordelen van de rechtmatigheid van een onderzoeksvoorstel, maar dat elke keer dient te worden beoordeeld of dat er aanvullend juridisch onderzoek nodig is voor bepaalde type onderzoeken. Immers kunnen in de literatuur, jurisprudentie of bij de toezichthouder nieuwe inzichten en toetsingscriteria zijn ontstaan.

Ook of iets wel of niet een open bron is, zal de beoordeling in welke mate sprake is van een inbreuk in iemands privéleven, kunnen beïnvloeden. Hierna volgt eerst een verkenning van het begrip open bron.

2.2 Begrip openbare online bron

2.2.1 Definitie open bron

Ook al betreft het internet een open bron, niet alle data op het internet is even ‘openbaar’. De vindplaats van de data zal mogelijk van invloed zijn op de beoordeling wat de mate van privacyinmenging is. De consultatieversie van de memorie van toelichting op het Wetsvoorstel tot modernisering van het Wetboek van Strafvordering verstaat onder ‘open bron’:¹⁶

“Kenmerkend voor een open bron is het feit dat er een onbeperkte kring van personen toegang kan verkrijgen en er geen tussenkomst van een derde nodig is om toegang te verkrijgen. De registratie, het aanmaken van een profiel of de betaling zijn formaliteiten en geschieden vaak volledig

¹⁶ Memorie van toelichting bij het conceptwetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering (consultatieversie), p. 245 (7-02-2017).

geautomatiseerd. Dit in tegenstelling tot besloten of afgeschermd bronnen of websites waarbij bijvoorbeeld een uitnodiging of goedkeuring vereist is om toegang te krijgen. De aard of het doel van de open bron is niet relevant, doorslaggevend is of de open bron door een ieder gebruikt kan worden.

Met het plaatsen van berichten, recensies, foto's en filmpjes op het openbare internet, het bijhouden van weblogs of het deelnemen aan (openbare) nieuwsgroepen of forums is juist openbaarmaking beoogd en wordt de informatie in beginsel beschikbaar voor iedere internetgebruiker. Gegevens of delen van internet die op enigerlei wijze afgeschermd worden, zoals een (via de privacy-instellingen) afgeschermd account op Facebook of LinkedIn of een besloten chat, zijn daarmee dus ook geen open bron.”¹⁷

Bovenstaande is afkomstig uit een ander rechtsgebied dan waar onderhavig stuk over gaat (bestuursrecht). De tekst is afkomstig uit het straf(proces)recht. Niettemin is de omschrijving bruikbaar voor de praktijk van het internetonderzoek van de Belastingdienst, opererend vanuit het bestuursrecht.

Het begrip ‘open bron’ wordt twee jaar later in het conceptwetsvoorstel aangepast naar ‘publiek toegankelijke bron’. De toelichting vermeldt hierover¹⁸:

“Tevens is de term “open bronnen” vervangen door “publiek toegankelijke bronnen”. “Open bron” heeft een connotatie van “vrij” of “onbeperkt” om te gebruiken. Dit resulteert in een uitleg dat de politie geen bevoegdheden nodig heeft om deze gegevens te verzamelen en (verder) te verwerken. De term “open bron” heeft een onbedoeld en ongewenste suggestie in zich als zou een dergelijke bron een rechtenvrije omgeving zijn. Daarom wordt voorgesteld een andere term te gebruiken, die taalkundig dichter bij de aard van het soort bronnen ligt: “publiek toegankelijke bronnen”. Deze term wijst op de feitelijke toegankelijkheid van de gegevens. Er bestaat weliswaar geen beperking vooraf wat betreft de feitelijke beschikbaarheid van de gegevens, maar het gebruik van de gegevens is niet geheel regelvrij.”

Open bronnen staan tegenover afgeschermd bronnen, die zich kenmerken doordat een internetgebruiker er uitdrukkelijk voor kiest andere internetgebruikers al dan niet toe te laten tot die bron.¹⁹

Om voorafgaand aan een onderzoek een zo nauwkeurig mogelijke inschatting te kunnen maken van de mate van privacyinmenging, is het van belang om de mogelijke vindplaatsen te definiëren. Betreft het werkelijk een bron waarvan de gegevens toegankelijk zijn voor publiek? Hierna volgen enkele voorbeelden uit de praktijk waar de Belastingdienst mee te maken kan krijgen.²⁰

2.2.2 Reikwijdte begrip open bron

De Commissie Koops²¹ hanteert het principe dat alle bronnen die op een geautomatiseerd werk staan dat bereikbaar is vanaf het internet, die gepubliceerd (via een webpagina) of gedeeld (bij het delen van bestanden) zijn en niet voorzien zijn van een beveiliging, publiek toegankelijk zijn.

¹⁷ Ter illustratie bij dit voorbeeld: bij de politie is voor deze zoekmethode een ‘goedkeuring’ nodig van de rechter-commissaris of Officier van Justitie.

¹⁸ Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving, p. 46. 7-02-2019.

¹⁹ Regulering opsporingsbevoegdheden in een digitale omgeving, Commissie Koops juni 2018. Zie ook: Internetonderzoek door bestuursorganen, J. Oerlemans & Y. Schuurmans, 20-05-2019.

²⁰ Veel van de voorbeelden en teksten zijn afkomstig uit het rapport van de Commissie Koops.

²¹ Commissie Koops, onder leiding van professor Bert-Jaap Koops, heeft in 2018 een onderzoek verricht naar vraagstukken met betrekking tot het opsporingsonderzoek in het digitale tijdperk (in het strafrecht). Zie ook: <https://www.rijksoverheid.nl/actueel/nieuws/2018/06/26/minister-grapperhaus-neemt-rapport-van-commissie-koops-in-ontvangst>

De term publiek toegankelijk betekent dus niet dat de pagina te vinden moet zijn door een zoekmachine. Er zijn veel plaatsen op het internet die bijvoorbeeld niet door zoekmachines willen worden geïndexeerd (dit geven zij dan aan in een bestandje robots.txt, dat door crawlers van zoekmachines wordt gelezen), maar wel degelijk voor eenieder toegankelijk zijn.²²

Máár het betekent niet dat álle gegevens die online te vinden zijn, een open bron zijn. Indien tijdens een onderzoek bijvoorbeeld een wachtwoord van een e-mailaccount bekend wordt, maakt dit niet dat de e-mailaccount daarmee een open bron is geworden²³.

Tot slot kan bij het raadplegen van open bronnen geen sprake zijn van het doorbreken of ontwijken van beveiliging om toegang te verkrijgen tot de open bron. Dit zijn vormen van afscherming waarmee kennelijk beoogd wordt om de gegevens slechts voor een bepaalde (beperkte) groep personen beschikbaar te stellen en zullen dus niet ingezet worden door het OSINT-team.

Het deep web – het gedeelte van het internet dat niet geïndexeerd is door zoekmachines, maar dat wel feitelijk toegankelijk is als je de website bezoekt (zie figuur 2) – is dus ook een publiek toegankelijke bron: het kent als zodanig geen minimaal niveau van beveiliging.



Figuur 2: Bron: <https://www.independent.co.uk/technology-how-dark-is-dark-web/>

2.2.2.1 BETAALDE DIENSTEN

Het bovenstaande criterium betekent ook dat bronnen die financiële drempels kennen voor de toegang maar niet anderszins aan toegangscontrole onderworpen zijn, zoals toegang tot SIDN, LexisNexis, de Kamer van Koophandel of bestanden die op de markt tegen betaling beschikbaar zijn, een publiek toegankelijke bron zijn, ook als de financiële drempel dusdanig is dat niet iedereen het zich zou kunnen veroorloven, aldus de Commissie Koops.²⁴

²² Commissie Koops, p. 153.

²³ Commissie Koops, p. 154.

²⁴ Commissie Koops, p. 154.

2.2.2.2 GESTOLEN GEGEVENS

Het houdt ook in dat een publiek toegankelijke webpagina waarop iemand onrechtmatig verkregen gegevens (bijvoorbeeld accountgegevens of vertrouwelijke stukken die iemand door hacken heeft verkregen) heeft geplaatst, als publiek toegankelijke bron geldt wanneer deze pagina op een normale wijze wordt bezocht.²⁵ In het verlengde hiervan: in 2019 oordeelde de Hoge Raad dat de Belastingdienst gestolen gegevens (maar niet via internet) – waarvoor betaald werd door de Belastingdienst – mochten worden gebruikt als bewijs.²⁶ Dat dit een potentieel grote privacyinbreuk kan betekenen, doet daar niet aan af volgens de Commissie Koops. De aard van de gegevens is een kwestie die de normering van het onderzoek in de publiek toegankelijke bron beïnvloedt, niet de definitie of afbakening ervan.

2.2.2.3 DARK WEB

Een vergelijkbare redenering is van toepassing op toegang tot gegevens op het dark web (zie figuur 2), het gedeelte van het deep web waartoe alleen toegang kan worden verkregen met speciale software, instellingen of autorisatie zoals Tor²⁷. Men zou dan kunnen redeneren dat dergelijke software onder een “technische ingreep” valt, en daarmee dat het dark web geen publiek toegankelijke bron is. De Commissie Koops hanteert echter een andere redenering: het feit dat gegevens alleen met bepaalde software toegankelijk zijn, vormt nog geen beveiliging van deze gegevens in de zin dat er enige vorm van toegangscontrole plaatsvindt. Eenieder kan de benodigde software downloaden en gebruiken. In die zin is er geen conceptueel verschil tussen Tor en andere browsers, en tussen het dark web en het geïndexeerde web: de toegang vindt niet plaats door een technische ingreep, maar met een technisch hulpmiddel in de maatschappelijke zin van het woord.²⁸

2.2.2.4 INLOGGEN MET EEN ACCOUNT

De inhoud die waargenomen wordt nadat is ingelogd met een ‘nep-account’ is publiek toegankelijk. Al bestaan ook hier differentiaties: inloggen onder de naam ‘Belastingdienst’ (open-vizier) zal wellicht anders beoordeeld worden dan het inloggen met een gefingeerd account (fake-account). Daarentegen is het verkrijgen van toegang tot sociale media via het aanmaken van een nep-account waarmee wordt gepoogd vrienden te worden van verdachte personen, veel ingrijpender. Daarmee beoog je immers toegang te krijgen tot gegevens die niet voor eenieder toegankelijk zijn, maar enkel voor “vrienden”. Bijzonder hoogleraar Oerlemans benadrukt in zijn stuk dat Het Europees Hof voor de Rechten van de Mens (EHRM) heeft benadrukt dat burgers het recht moeten hebben om ‘to engage in relationships with others’, zelfs in het openbaar, zónder de inmenging van de overheid: *The ECtHR has made it clear in case law that as part of the right to privacy, individuals must be able to engage in relationships with others – even in public – without the interference of the government.*²⁹

Indien enkel gekeken wordt naar de mate van privacy-inmenging, zou betoogd kunnen worden dat bij gebruik van fake-accounts waardoor infiltratie ontstaat in privésfeer, de ernst van de inbreuk ook groter zal zijn. En wél inloggen, maar niet interacteren of ‘vrienden worden’ is wellicht weer minder

²⁵ Zie bijvoorbeeld bij de Belastingdienst het project gericht op *Cayman National Bank Hack*, waarbij gestolen gegevens online staan.

²⁶ Zie uitspraak Parket bij Hoge Raad ECLI:NL:PHR:2019:295, waarbij Belastingdienst heeft betaald voor gestolen gegevens. Deze gegevens mochten gebruikt worden als bewijs.

²⁷ Zie over ‘Tor’: [https://nl.wikipedia.org/wiki/Tor_\(netwerk\)](https://nl.wikipedia.org/wiki/Tor_(netwerk))

²⁸ Commissie Koops, p.155.

²⁹ Bron: ECtHR 12 January 2010, Gillian and Quinton v. The United Kingdom, appl. no. 4158/05, § 61 en ECtHR 2 September 2010, Uzun v. Germany, appl. no. 35623/05, § 44.

ingrijpend. Ook kan een vraag zijn of in hoeverre de betrokkene ‘geraakt’ wordt door het gebruik van een fake-account door de Belastingdienst.³⁰

Echter zal met betrekking tot fake-accounts een ander bevoegdheidsvraagstuk gaan spelen, namelijk dat raakt aan de algemene beginselen van behoorlijk bestuur en het recht op een eerlijk proces (artikel 6 EVRM): was de Belastingdienst als machtig overheidsorgaan (denk hierbij aan: *détournement de pouvoir*) bevoegd om zich voor te doen als iemand anders, en was dit wel nodig voor het onderzoek? Of was er een minder ingrijpend middel voorhanden om het doel te bereiken?³¹ Dit vraagstuk omtrent fake-accounts verlangt een Belastingdienst-breed beleid en blijft in dit stuk verder buitenscope.

2.2.2.5 HERKOMST VAN GEGEVENS: MENSELIJKE BRON

Tevens is inherent aan internet als bron dat niet *alle* gegevens over een betrokkene ook *gepubliceerd* zijn door de betrokkene. En veel mensen hebben niet de bedoeling om zijn of haar gegevens ongelimiteerd ter beschikking te stellen aan de overheid. Ook worden gegevens soms niet bewust op het internet gezet, maar komen hier onbedoeld wel op terecht. Het enkele feit dat gegevens op internet staan, betekent dus geenszins dat zij doelbewust ongelimiteerd zijn prijsgegeven aan anderen.³²

Ook onderdeel van het onderwerp ‘herkomst van gegevens’ is de ontwikkeling van Internet of Things (IoT). We leven in een sterk gedigitaliseerde samenleving waarbij steeds meer sensoren ‘data creëren’ op basis van onze dagelijkse levens. Onze bewegingen, activiteiten, samenkomsten en keuzes worden steeds meer vastgelegd door computers. Deze computers staan vaak (niet altijd) in verbinding met elkaar. Deze ‘door de computer gegenereerde data’ wordt gedeeld tussen computers via het internet. Een deel van deze data is publiek toegankelijk, daar het wel vaak om geaggregeerde informatie gaat. Het zijn vaak statische gegevens die niet herleidbaar zijn tot individuen. Deze gegevens behoren ook tot het terrein van een OSINT specialist en ook tot de bronnen van het internet.

2.2.2.6 TUSSENCONCLUSIE

Een open bron is dus niet altijd een publiek toegankelijke bron waaruit persoonsgegevens zijn te verzamelen zonder inbreuk te maken in iemands persoonlijke levenssfeer. Ook al doet het begrip ‘open bron’ dit wel vermoeden. Financiële drempels en gestolen gegevens vormen over het algemeen geen belemmering om te worden gekwalificeerd als publiek toegankelijke bron. Wel kan de vindplaats en de menselijke bron van invloed zijn op de beoordeling hoe groot de mate van inbreuk in de privésfeer is, evenals het gebruik van gefingeerde accounts waarmee interactie wordt aangegaan met betrokkene.

³⁰ Hier zal ook het vraagstuk gaan spelen of de Belastingdienst zich dient te houden aan de Voorwaarden die de platforms stellen ten aanzien van het inloggen: platforms kunnen immers ‘fake-accounts’ verbieden middels hun eigen Algemene Voorwaarden.

³¹ Zie hiervoor de jurisprudentie en literatuur, waaronder: ‘Justitiële Verkenningen, Facebookvrienden worden met de verdachte, over undercoverbevoegdheden op internet’ van J. Oerlemans, BJ Tijdschriften, afl. 5 2018.

³² Commissie Koops, p.152.

2.2.3 De OSINT-middelen en bronnen

Tientallen type software en hardware staan ter beschikking van het OSINT-team. Voor een eerste indruk van de verschillende tools wordt voor nu verwezen naar de bijlage. Kenmerkend voor de OSINT-tools is dat het zoekproces vaak grotendeels wordt overgenomen door een computer, waardoor efficiënter, sneller en nauwkeuriger gezocht kan worden. Het bevragen van internet als bron door middel van specifieke zoekmachines kan gezien worden als een venster waarmee naar een bron gekeken wordt. Het reikt te ver voor dit stuk om een analyse te bewerkstelligen van de verschillende OSINT-tools. Wat voor de juridische analyse van de OSINT-tools belangrijk is, is dat de inspecteur en/of de OSINT-medewerker voorafgaand aan een internetonderzoek onder andere bepaalt of de zoekslag noodzakelijk is. Tevens is het van belang om na te gaan wat gebeurt met de gevonden data. En of de gegevens van de medewerker van OSINT die de tool gebruikt daarin wordt vastgelegd. De inspecteur kan aan de hand van een aantal factoren (waarover later meer) bekijken hoe groot de mate van inbreuk in iemands privésfeer is, het relevante criterium in de jurisprudentie.

2.2.4 Conclusie

Internetonderzoek door OSINT omvat een brede verscheidenheid aan soorten onderzoeken is dus niet eenduidig te definiëren. De type internetonderzoeken variëren op allerlei vlakken, van zoekmethoden, zoekresultaten tot aan bronnen en zijn tevens onderhevig aan verandering. Deze verandering komt vanwege de aard van het type onderzoek dat verricht wordt op internet. OSINT beslaat een dynamische werkgebied waarbij de nieuwe technologische invloeden al snel van invloed zijn op de wijze waarop informatie verzameld kan worden. Aan te bevelen is alvorens OSINT-tools te gebruiken daarop een privacy risico analyse uit te voeren om de hiervoor genoemde privacy risico's in beeld te brengen.

Hoofdstuk 3 Wettelijk kader

3.1 Verwerking van persoonsgegevens bij internetonderzoek

De definitie van 'verwerking' in de Algemene Verordening Gegevensbescherming (AVG) is zeer ruim. Het raadplegen, gebruiken, opvragen, verzamelen, opslaan, combineren, wissen etc. van persoonsgegevens wordt beschouwd als *verwerking*. In de praktijk betekent dit dat elke zoekhandeling op internet beschouwd kan worden als de start van de verwerking van persoonsgegevens.³³ Dit betekent dat vanaf dat moment een mate van inmenging plaats vindt in de persoonlijke levenssfeer. Zie de *Mogelijke zoekhandelingen* uit de bijlage voor een indicatie van mogelijke zoekhandelingen in de praktijk bij internetonderzoek.

³³ Een uitzondering betreft een zoekslag waarin géén persoonsgegevens worden ingetypt of tevoorschijn komen in het zoekresultaat. Deze uitzondering blijft in dit stuk buiten beschouwing, maar zou zich wellicht kunnen voordoen bij bepaald type onderzoeken.

Definitie persoonsgegevens volgens de AVG (artikel 4 lid 1) ³⁴:

“Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.”

Juridisch betekent dit ook dat zódra sprake is van verwerking van persoonsgegevens, bepaalde wetgeving van toepassing is, zoals onder meer de AVG en de Grondwet, maar ook internationale regelgeving, zoals artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele vrijheden (EVRM) en het Handvest van de Grondrechten van de Europese Unie.

3.1.1 De AVG

De AVG³⁵ verlangt dat er bij gegevensverwerking sprake is van een geldige grondslag en wettelijke basis. Daarnaast vereist de AVG dat de gegevens voor een bepaald doel worden verzameld en niet meer dan noodzakelijk zijn om dat doel te bereiken. Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij dat noodzakelijk is voor het te bereiken doel. Bovendien vereist de AVG dat de bewaartermijn zo beperkt mogelijk is, hebben betrokkenen recht op inzage en correctie en dient de verwerkingsverantwoordelijke te kunnen verantwoorden dat elke verwerkingsactiviteit geschiedt overeenkomstig de wet.

Ook geldt het principe van doelbinding: de gegevens mogen niet op een onverenigbare wijze met het doel worden verwerkt. Gegevensverwerking mag niet excessief zijn en beperkt worden tot wat noodzakelijk is voor het doel van de verwerking (beginsel van dataminimalisatie). Ook dienen de gegevens passend te worden beveiligd.

De verwerkingsverantwoordelijke dient volgens de AVG te kunnen aantonen dat aan de regelgeving is voldaan (zie artikel 5 en 24 AVG). Dit betekent dat niet alleen bij een controle van de toezichthouder de mate van compliance aangetoond moet kunnen worden, maar óók dat een actieve inspanning wordt gevraagd van de verwerkingsverantwoordelijke om continue transparant te zijn over de mate van compliance en dit actief – intern - te onderzoeken.

Daarnaast dient de verwerkingsverantwoordelijke bij verwerkingen met een hoog risico voor de rechten en vrijheden van personen een beoordeling uit te voeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens. Dit wordt ook wel een gegevensbeschermingseffectbeoordeling (GEB) genoemd, of, een Data Protection Impact Assessment (DPIA). Als uit een DPIA blijkt dat de verwerking een hoog risico meebrengt voor de rechten en vrijheden van personen, en dat dit risico niet te beperken is door het nemen van maatregelen, dient de Autoriteit Persoonsgegevens te worden geraadpleegd. Dit wordt ook wel een Voorafgaande Raadpleging genoemd.³⁶

³⁴ Een uiteenzetting wat persoonsgegevens nu exáct zijn, blijft in deze analyse buiten beschouwing. Dit onderwerp brengt namelijk weer complexe vraagstukken met zich mee, zie bijvoorbeeld het document Advies 5/2014 over anonimiseringstechnieken van de WP29.

³⁵ De Uitvoeringswet AVG (UAVG) wordt niet apart behandeld in dit stuk, tenzij zij voor een specifiek onderwerp van waarde is.

³⁶ Bron: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging>

3.1.2 Tussenconclusie

De AVG hanteert diverse voorschriften teneinde de privacyinbreuk te minimaliseren, echter wordt niet expliciet in de AVG wanneer sprake is van een ernstige mate van inbreuk. Daarom zal hierna kort de andere wetgeving aanbod komen die mogelijk raakt aan het onderwerp ‘mate van inmenging’.

3.1.3 Grondwet en artikel 8 EVRM

Volgens artikel 10, lid 1, van de Grondwet heeft eenieder, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

Artikel 8 EVRM stelt dat geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van het recht van eenieder op respect voor zijn privéleven, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Uit de eis dat een inmenging in de uitoefening van het recht op respect voor het privéleven moet zijn voorzien bij wet vloeit voort dat die inmenging moet berusten op een naar behoren bekend gemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt.

3.1.4 Handvest Grondrechten EU

Artikel 7 van het Handvest van de Grondrechten van de Europese Unie is een artikel dat het recht op eerbiediging van iemands privéleven regelt. Artikel 8 van het Handvest regelt het recht op bescherming van iemands persoonsgegevens.

Zodra persoonsgegevens gezocht worden via internetonderzoek, dient de Belastingdienst rekening te houden met bovenstaande grondrechten. In een zaak tussen een vluchteling en de Nederlandse Staat deed de vluchteling een beroep op o.a. artikel 7 van het Handvest en artikel 8 EVRM³⁷. Naar de mening van de vluchteling had de Nederlandse Staat onrechtmatig gehandeld door gegevens van zijn Facebookaccount te gebruiken als bewijs waaruit zijn geaardheid/seksuele oriëntatie bleek en verzocht om een schadevergoeding zoals bedoeld in artikel 8:92 Awb. De rechter komt – voor dit stuk niet relevante redenen - niet aan de inhoudelijke beoordeling toe in deze zaak, echter dienen de inspecteur en de OSINT-medewerker zich bewust te zijn van de grondrechten van de belastingplichtigen en de kans dat hierop een beroep wordt gedaan door de belastingplichtige.

3.1.5 Conclusie

Dat bij internetonderzoek door de Belastingdienst sprake is van verwerking van persoonsgegevens, en dus van een bepaalde mate van privacy-inmenging, is evident.³⁸ Om nu te kunnen beoordelen wanneer een internetonderzoek rechtmatig is, ondanks deze inmenging, dient duidelijk te worden *hoe groot* de inbreuk is die wordt gemaakt op het persoonlijke leven. Bovenstaande algemene beschouwing geeft nog onvoldoende aanknopingspunten, echter zal in het volgende hoofdstuk een verdieping plaatsvinden en een poging gedaan worden om de rechtmatigheidstoets voor internetonderzoek verder in te vullen.

³⁷ Zie uitspraak Rechtbank Den Haag van 12 augustus 2014 ECLI:NL:RBDHA:2014:10266

³⁸ Uitzonderingen daargelaten: bij een onderzoek naar fenomenen, rechtspersonen is de kans op persoonsgegevens kleiner, maar zeker niet uitgesloten.

Hoofdstuk 4 Rechtmatigheid internetonderzoek

4.1 Rechtmatig

4.1.1 IS ER SPRAKE VAN EEN GELDIGE GRONDSLAG BIJ INTERNETONDERZOEK?

Om persoonsgegevens te mogen verwerken, dient voldaan te zijn aan een aantal beginselen. Ten eerste dienen persoonsgegevens verwerkt te worden op een wijze die ten aanzien van de betrokkene rechtmatig is. Rechtmatig houdt hier in dat er een deugdelijke rechtsgrondslag voor de verwerking moet zijn, bijvoorbeeld toestemming van de betrokkene of een wettelijke verplichting. Voor internetonderzoek geldt dat de betrokkenen in dit geval geen expliciete toestemming hebben gegeven aan de Belastingdienst voor het raadplegen van hun persoonsgegevens. Ook is er geen wettelijke plicht die de belastingdienst 'dwingt' tot het doen van internetonderzoek. Echter oefent de Belastingdienst wel een taak uit van algemeen belang. De AVG heeft hiervoor een verwerkingsgrond opgenomen.

4.1.2 AVG GRONDSLAG

De grondslag voor de verwerking van persoonsgegevens door de Belastingdienst betreft namelijk artikel 6 lid 1 sub e van de AVG, zolang de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. Deze taak van algemeen belang moet echter wel weer zijn gespecificeerd in nationale wetgeving. De publieke taak zal altijd moeten blijken uit sectorspecifieke regelgeving die op de verwerkingsverantwoordelijke van toepassing is.

4.1.3 NATIONALE GRONDSLAG

Voor de Belastingdienst is in artikel 2 lid 1 van de Uitvoeringsregeling Belastingdienst 2003 de algemene taakstelling omschreven:

Er is een rijksbelastingdienst onder de naam Belastingdienst. Deze dienst is belast met de heffing en invordering van rijksbelastingen en met andere bij of krachtens de wet opgedragen taken.

Daarnaast zijn in de Algemene Wet Bestuursrecht (Awb) en de Algemene Wet inzake Rijksbelastingen (AWR) specifieke onderzoeksgrondslagen opgenomen voor de inspecteurs. De Belastingdienst heeft op basis van het algemene zorgvuldigheidsbeginsel de bevoegdheid om de benodigde kennis te achterhalen (artikel 3:2 Awb). Daarnaast heeft de inspecteur onderzoeksbevoegdheden toegekend gekregen teneinde de naleving van de verplichtingen van belastingplichtigen te waarborgen. De wettelijke grondslagen voor deze bevoegdheden zijn in de AWR bijeengebracht in de afdeling 'Verplichtingen ten dienste van de belastingheffing'. In art. 47 t/m 56 AWR van deze afdeling zijn voor de belastingplichtige bijkomende verplichtingen neergelegd op grond waarvan de inspecteur bevoegd is om ten dienste van de belastingheffing informatieverplichtingen op te leggen. De inspecteur kan ingevolge art. 47 AWR informatie vorderen van de belastingplichtige zelf, en ingevolge art. 53 AWR, respectievelijk 55 AWR, ook van administratieplichtigen en overheidslichamen. Ook kan de inspecteur ingevolge art. 50 AWR waarnemingen ter plaatse (WTP) verrichten.

Bovenstaande bevoegdheden zijn geschreven in het tijdperk dat internetgebruik nog ongewoon was. Toch lijkt de rechter hier vooralsnog geen probleem van te maken en worden bovenstaande grondslagen over het algemeen niet als ontoereikend gezien voor het toezicht op internet. Pas wanneer de inbreuk in iemands privéleven dusdanig ernstig is, zijn bovenstaande algemene grondslagen niet meer voldoende. Dit blijkt onder meer uit de rechtspraak van het EHRM. In dat geval zal (sector)specifieke wetgeving noodzakelijk zijn.

4.1.4 VOORZIENBAARHEID EN ARTIKEL 8 EVRM

Het is echter niet noodzakelijk dat in de sectorspecifieke regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden, aldus de Memorie van Toelichting op de AVG.³⁹ Volgens de Memorie van Toelichting wordt dus geen expliciete wettelijke taak verlangd waarin letterlijk staat dat de Belastingdienst gegevens mag verwerken.

De vraag is hoe dat zich verhoudt met de eis uit artikel 8 lid 2 EVRM. Artikel 8 lid 2 EVRM hanteert het vereiste van voorzienbaarheid. Hierin is opgenomen dat de beperking van het privéleven *voorzienbaar* moet zijn bij wet. Het gaat erom dat voor het individu kenbaar moet zijn dat zijn persoonsgegevens met betrekking tot een specifieke publieke taak worden verwerkt. Het begrip 'publieke taak' moet dus breed worden gelezen, maar die publieke taak moet wel voldoende blijken uit nationaal recht.

Uit artikel 8 lid 2 EVRM vloeit voort dat de inmenging moet berusten op een naar behoren bekendgemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt.

Daarin lijkt de Nederlandse Staat nu nog tekort te schieten: er is geen wettelijk voorschrift waaruit blijkt welke gegevens voor een overheidstaak (zoals die van de Belastingdienst) kunnen worden verwerkt.

4.2 Jurisprudentie

ANPR

In de ANPR-arresten van de Hoge Raad was er sprake van systematisch verzamelen, vastleggen, bewerken en jarenlang bewaren van gegevens over de bewegingen van voertuigen op diverse plaatsen in Nederland. Dit gebeurde op zodanige wijze dat de gegevens tot een bepaald voertuig en daarmee ook tot een bepaald persoon konden worden herleid. Uit de bewoording van artikel 10 Grondwet en artikel 8 EVRM blijkt dat een dergelijke beperking op het recht op eerbiediging van de persoonlijke levenssfeer slechts kan worden gerechtvaardigd door of krachtens een wet in formele zin. Artikel 20 AWR bood onvoldoende precieze wettelijke grondslag voor de gevolgde handelswijze. Volgens de Hoge Raad gold dit ook voor de regeling over belastingheffing wegens privégebruik ex. art. 13bis Wet Loonbelasting 1964. De Hoge Raad kwam tot het oordeel dat er ook geen andere wettelijke voorschrift was die de inspecteur een voldoende precieze grondslag bood voor de gevolgde handelswijze bestaande uit het jarenlang stelselmatig, systematisch verzamelen, vastleggen, bewerken en jarenlang bewaren van gegevens over de bewegingen van voertuigen.

CAMERATOEZICHT

Ook het stelselmatig observeren in verband met mogelijke fraude bij socialezekerheidsuitkeringen door middel van cameratoezicht kan tot onrechtmatig verkregen bewijs leiden waarvan, gelet op de norm van artikel 8 EVRM, het gebruik zozeer indruist tegen wat van een behoorlijk handelende overheid mag worden verwacht dat dit ontoelaatbaar moet worden geacht.⁴⁰

TRANS LINK

Het opvragen van dagelijks vastgelegde in- en uitcheckgegevens van reizigers bij Trans Link Systems door de minister om studiefinanciering (naar de norm voor uitwonende studenten) vast te stellen was daarentegen wel een gerechtvaardigde inbreuk op het respect voor het privéleven van de

³⁹ Zie Memorie van Toelichting op AVG, kamerstuk 34851, nr. 3, p.10 e.v., paragraaf 4.2.2

⁴⁰ CRvB 13 september 2016, ECLI:NL:CRVB:2016:3479

betrokken student.⁴¹

SCANAUTO'S

Dit gold ook in een recente uitspraak van de Belastingkamer van de Hoge Raad: hierin oordeelt zij dat er bij de inzet van scanauto's om via kentekens van geparkeerde auto's te controleren of er parkeerbelasting is voldaan, sprake is van inmenging door de gemeente in het recht van belanghebbende op respect voor zijn privéleven als bedoeld in artikel 8 EVRM. In dit geval is de inmenging echter gerechtvaardigd, omdat de eis van het opgeven van het kenteken "bij wet is voorzien" in de Parkeerverordening 2013 van de gemeente in combinatie met de Gemeentewet⁴².

COMPLEET BEELD

In een arrest van de Hoge Raad (Strafkamer) van 4 april 2017⁴³ werd duidelijk dat indien de door het onderzoek gemaakte inbreuk op de persoonlijke levenssfeer beperkt is, de algemene bevoegdheid van opsporingsambtenaren in art. 94 jo. 95 en 96 Wetboek van Strafvordering voldoende legitimatie biedt. Indien het onderzoek zo verstrekkend is dat een *min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven* van de gebruiker, in het bijzonder als het gaat om onderzoek met technische hulpmiddelen van alle opgeslagen of beschikbare gegevens, kan het onderzoek jegens hem onrechtmatig zijn.

SYRI

Voor gebruik van het Systeem Risico Indicatie (SyRi) voor bestandkoppeling om sociale zekerheidsfraude te achterhalen van het Ministerie van SZW was een wettelijke regeling opgesteld met allerlei waarborgen teneinde de privacy te waarborgen. De rechtbank oordeelde⁴⁴ dat dit analysesysteem niet voldeed aan de vereisten van artikel 8 EVRM en verklaarde de wet- en regelgeving waarop dit systeem gebaseerd was onverbindend. Er was volgens de rechtbank strijd met artikel 8 lid 2 EVRM, met name vanwege het feit dat er geen *inzicht* was in de risico-indicatoren en het risicomodel. En verder werden betrokkenen, ook niet achteraf, geïnformeerd dat een risicomelding was gedaan aan de socialezekerheidsinstantie.

MUSEUMJAARKAART

In deze zaak⁴⁵ vroeg de Belastingdienst de gebruiksgegevens van een museumkaarthouder op om vast te kunnen stellen of diegene in Nederland verbleef in plaats van in het buitenland. En dus ook hier belastingplichtig was. Maar de Stichting Museumkaart wilde die gegevens niet verstrekken. Dat zou een veel te grote inbreuk maken op de privacy van de kaarthouder. De stichting verwees o.a. daarbij naar de ANPR-arresten. Bovendien vond de stichting dat de bezoekgegevens niet erg relevant waren voor het vaststellen van iemands woonplaats.

De rechtbank oordeelde eerder al dat de ANPR-arresten niet van toepassing zijn omdat het hier ging om een individueel geval. Daarnaast vond de rechter dat het algemene belang van juiste belastingheffing zwaarder moest wegen dan de privacy van de kaarthouder. Dus moest de stichting de gegevens verstrekken. Ook in hoger beroep heeft de stichting haar gelijk niet kunnen halen. Het gerechtshof stelde dat de bevoegdheid van de fiscus om inlichtingen te vragen in het kader van een derdenonderzoek zeer ruim was. Die bevoegdheid van de fiscus wordt echter wel beperkt als de vragen om informatie de activiteiten van de stichting in gevaar brengen. Maar het hof vond dat de stichting niet met duidelijke bewijzen was gekomen waaruit dit gevaar zou blijken.

⁴¹ CRvB 5 februari 2018, ECLI:NL:CRVB:2018:269.

⁴² HR 10 april 2020, ECLI:NL:HR:2020:639

⁴³ HR 4 april 2017, ECLI:NL:HR:2017:592

⁴⁴ Rechtbank Den Haag van 5 februari 2020, ECLI:NL:RBDHA:2020:865.

⁴⁵ Gerechtshof Amsterdam, 5 november 2019 ECLI (verkort): 3967.

EHRM

Het EHRM besloot eerder al dat “public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities”.⁴⁶ In de zaak Rotaru⁴⁷ overwoog het EHRM dat het voor betrokkenen voorzienbaar moest zijn onder welke voorwaarden de overheid op systematische wijze persoonsgegevens mag verwerken. In de zaken Uzun en Ben Faiza overwoog het Hof met betrekking tot GPS-tracking dat een algemene rechtsbasis voldoende kan zijn, voor zover in jurisprudentie of beleid de gronden en de voorwaarden voor de toepassing van de maatregel voorzien zijn. Ook dient het nationale recht voor de betrokkenen te bieden. Of er sprake is van adequate en effectieve waarborgen hangt onder meer af van de aard, de reikwijdte en de duur van de maatregelen, de vereiste gronden, de autoriteiten en de geboden rechtsmiddelen.⁴⁸

4.2.1 TUSSENCONCLUSIE

De vraag is of voor internetonderzoek door de Belastingdienst via OSINT bovenstaande voldoende grondslag biedt. De Awr biedt algemene grondslagen die vooralsnog voldoende lijken in de huidige jurisprudentie, al gaat niet alle jurisprudentie over het verkrijgen van informatie via internet. De Memorie van Toelichting op de AVG benadrukt echter dat de algemene taakstelling van een overheidsdienst niet in alle gevallen kan dienen als rechtsgrond voor de verwerking.⁴⁹ Dat bleek ook uit de ANPR-arresten. Echter betrof het bij de ANPR-arresten *systematisch* verzamelen van persoonsgegevens. Ook het verkrijgen van een min of meer compleet beeld van bepaalde aspecten van het persoonlijk leven zal vaak onrechtmatig zijn.

Of er voldoende grondslag voor internetonderzoek is zal dus mede afhangen van *de manier* van het verzamelen van gegevens: indien het systematisch plaats vindt of een compleet beeld ontstaat zal de mate van inbreuk in iemands privésfeer groter en dus waarschijnlijk onrechtmatig zijn. In dat geval zal specifieke wetgeving nodig zijn die voor de Belastingdienst de bevoegdheid creëert tot dit type onderzoek. Voor de gevallen waarin internetonderzoek plaatsvindt dat niet systematisch verzamelen betreft en waarin niet een compleet beeld ontstaat van aspecten van iemands privéleven, zal het afhangen van de omstandigheden van het geval of de rechter dit toelaatbaar acht of niet. Dit betekent dat enige voorzichtigheid geboden is voor de Belastingdienst, maar dat met de juiste waarborgen - denk aan zorgvuldige motivering met betrekking tot de noodzakelijkheid (waarover hierna meer), zorgvuldige voorbereiding en vastlegging én aantoonbaarheid - pilotinternetonderzoeken gestart kunnen worden.

Rest nog wel artikel 8 lid 2 EVRM, waarin duidelijk staat dat de inmenging in privésfeer door de overheid *voorzienbaar* moet zijn voor de burger. Dit lijkt nu niet het geval: de belastingplichtige lijkt nog niet duidelijk te worden geïnformeerd door de Belastingdienst welke gegevens kunnen worden verwerkt bij internetonderzoek en onder welke voorwaarden dit plaatsvindt. Het is dan ook aan te bevelen om hier nader onderzoek naar te doen (wat zijn de exacte eisen die blijken uit de jurisprudentie van het EHRM met betrekking tot de voorzienbaarheid?) en de informatie hierover richting de burger te optimaliseren.

4.3 Noodzaak

Het doel van de verwerking van de persoonsgegevens moet noodzakelijk zijn voor de vervulling van de publieke taak volgens de AVG. In de vraag of een verwerking noodzakelijk is ligt besloten of de

⁴⁶ Zie het EHRM van 6 Juni 2006, Segerstedt-Wiberg en anderen v. Zweden, nr. 62332/00, § 72 Met verwijzing naar EHRM 4 Mei 2000, Rotaru v. Romania, nr 28341/95, § 43.

⁴⁷ Zie bijlage voor een samenvatting van de zaak Rotaru.

⁴⁸ EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 63 (Uzun/Duitsland) m. nt. De Hert en Van Caeneghem en EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, par. 63 (Ben Faiza/Frankrijk)

⁴⁹ Zie Memorie van Toelichting op AVG, kamerstuk 34851, nr. 3, p.10 e.v., paragraaf 4.2.2

verwerking van gegevens 1) proportioneel is en 2) of de verwerking voldoet aan de eis van subsidiariteit.

Allereerst moet de verwerking proportioneel zijn. Dit betreft de vraag naar effectiviteit en evenredigheid. Als met de verwerking van de gegevens niet het gestelde doel bereikt kan worden, of als dat zeer onwaarschijnlijk is, dan is deze verwerking niet snel proportioneel. Het tweede element van de proportionaliteitstoets betreft de evenredigheid. Het legitieme doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt.

Subsidiariteit betreft de vraag of het genoemde doel niet op een andere, minder ingrijpende wijze (bijvoorbeeld door géén of minder persoonsgegevens te verwerken) kan worden bereikt.

4.3.1 Noodzaak en internetonderzoek

De wet en jurisprudentie geven geen exacte criteria om te bepalen of voldaan is aan de proportionaliteitstoets en subsidiariteitstoets met betrekking tot internetonderzoek door de overheid. Dit zal met name afhangen van de omstandigheden van het geval. In dit stuk zal de subsidiariteitstoets verder niet behandeld worden. Wel zal verkend worden hoe de Belastingdienst mogelijk de proportionaliteitstoets uit kan voeren met betrekking tot internetonderzoek⁵⁰.

In de literatuur zijn aanknopingspunten te vinden hoe de proportionaliteitstoets uitgevoerd kan worden. Het uitgangspunt is daarbij: Hoe meer ingrijpend het internetonderzoek is en hoe ernstiger de inmenging is in iemands privésfeer, hoe groter de kans dat de verwerking van persoonsgegevens niet meer proportioneel is. Hierna wordt een aantal criteria uit de literatuur behandeld die helpen een belangrijke vraag voor de praktijk te beantwoorden: Wanneer vindt een meer dan geringe inbreuk plaats?

4.3.2 Ernst van de inmenging

Op Europees niveau bestaat nog geen rechtspraak over het verzamelen van persoonsgegevens via *internet voor handhavingsdoeleinden*. Hoogleraren Oerlemans en Schuurmans verwachten dat bij openbronnenonderzoek op het internet het Europese Hof de privacy-inmenging *in beginsel* niet als bijzonder ernstig zal aanmerken. Mensen mogen een minder grote verwachting van privacy hebben als hun informatie in een open bron voor een ieder beschikbaar is.⁵¹

Echter geven zij ook aan dat bij een openbronnenonderzoek de ernst van privacy-inmenging van geval tot geval zal verschillen, vanwege de variërende intensiteit. Zij geven aan dat een eenmalige check van een Twitterbericht een andere intensiteit heeft dan het gebruik van een techniek zoals scraping, waarbij mogelijk grote hoeveelheden persoonsgegevens worden binnengehaald.

4.3.3 Voorafgaande schriftelijke beoordeling

Internetonderzoek verlangt dus een bepaalde mate van onderzoek vooraf, om de intensiteit zo goed mogelijk te kunnen inschatten. Van belang is dat een bestuursorgaan altijd van te voren, dus voorafgaand aan het onderzoek, een beoordeling maakt van de aan te treffen gegevens en deze beoordeling archiveert.⁵² Dit dient te gebeuren aan de hand van de op dat moment beschikbare informatie en de beoogde inzet van het middel, met inachtneming van de ervaringen met resultaten van de inzet van een dergelijk middel in eerdere gevallen. Bij twijfel zou de inspecteur ervoor kunnen kiezen om eerst een oppervlakkige zoekslag te maken, om een eerste beeld te krijgen van wat een

⁵⁰ Binnen de Belastingdienst is het reeds gebruikelijk om een privacytoets (o.a. WMK) uit te voeren voorafgaand aan een onderzoek waarin de proportionaliteit en subsidiariteit beoordeeld worden. Echter verlangt de proportionaliteitstoets bij internetonderzoek een diepere analyse, waarvoor deze paragraaf een eerste verkenning biedt.

⁵¹ Internetonderzoek door bestuursorganen, J. Oerlemans en Y. Schuurmans, 20 mei 2019.

⁵² Gebaseerd op de algemene beginselen van behoorlijk bestuur.

uitgebreide zoekslag op zou kunnen leveren, aldus Commissie Koops.⁵³

Maar hoe kan een bestuursorgaan nu zorgvuldig beoordelen hoe groot de mate van inmenging in iemands privésfeer is? De Belastingdienst zal dit vooraf moeten toetsen aan de hand van een aantal factoren, om willekeur en misbruik tegen te gaan.

4.3.4 Factoren

De Commissie Koops heeft onderzoek gedaan naar de 'regulering van opsporingsbevoegdheden in het digitale tijdperk'. Zij identificeren 17 factoren die de ernst van de inbreuk op de persoonlijke levenssfeer beïnvloeden bij openbronnenonderzoek. Zie *de bijlage* voor een compleet overzicht van deze factoren die kunnen helpen bij het bepalen van de ernst van de inmenging. De factoren kunnen geclusterd worden tot de volgende vier aspecten: (1) omvang en type van de (over te nemen) gegevens, (2) aard van de bron, (3) wijze van zoeken en (4) het gebruik van de gegevens en de mogelijke impact op de persoon. Deze factoren heeft deze commissie weliswaar opgesteld voor opsporing in het strafrecht, maar zijn ook zeer bruikbaar zijn voor het toezicht in het bestuursrecht, omdat de beoordeling 'mate van inmenging' gebaseerd is op het (Europese) grondrecht – kortweg recht op privacy - dat altijd geldt (zowel in het strafrecht als bestuursrecht).

4.3.4.1 GLIJDENDE SCHAAL ERNST INBREUK

Het uiteindelijke antwoord op de vraag wat de mate van inbreuk is, zal dus van geval tot geval verschillen én is niet eenvoudig vooraf te geven. Zie bijvoorbeeld de eerste factor: 'de hoeveelheid van gegevens' die gevonden zullen worden bij een internetonderzoek. Afhankelijk van de praktijksituatie biedt soms reeds enkele gegevens een min of meer volledig beeld van bepaalde aspecten van iemands privéleven, terwijl in een ander onderzoek een grote hoeveelheid aan gegevens geen volledig beeld van iemands privéleven zal schetsen. Dit verlangt een scherp vermogen van de inspecteur en wellicht ook het OSINT-team om op tijd, en bij voorkeur dus *vooraf*, maar ook tijdens het zoekproces, te bepalen met elkaar of de inbreuk nog steeds gerechtvaardigd is, gezien het belang van de Belastingdienst. Om deze onzekerheid zoveel mogelijk te mitigeren, is het aan te bevelen om met een multidisciplinair team de beoordeling voorafgaand aan een internetonderzoek te verrichten en deze beoordeling vast te leggen, mogelijk al voordat het verzoek tot onderzoek wordt gedaan bij het OSINT-team.⁵⁴

4.3.4.1 OMSLAGPUNT ONTBREEKT

Het beoordelen van de factoren en het beantwoorden van de vragen lost nog niet direct alles op. Want ook na het beantwoorden van de vragen uit de bijlage blijft de vraag in eerste instantie nog onbeantwoord of de Belastingdienst dit internetonderzoek nu mag doen. Er is immers geen omslagpunt waarop duidelijk wordt dat vanaf dát punt een (zeer) ernstige mate van privacy-inmenging plaatsvindt. Echter helpen de factoren om de belangenafweging die de Belastingdienst zelf dient te maken voorafgaand aan het zoekproces, te verfijnen.

De uiteindelijke toetsing is aan de rechter, echter zal de rechter bij afwezigheid van strikte normen vermoedelijk een grotere waarde hechten aan de zorgvuldigheid en uitlegbaarheid van het handelen van een bestuursorgaan dan aan het uiteindelijke resultaat.

4.4 Dataminimalisatie en doelbinding

Het beginsel van doelbinding houdt in dat de persoonsgegevens alleen mogen worden verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel (artikel 5 lid 1 sub b AVG). Tevens mogen de gegevens niet verder worden verwerkt als dat onverenigbaar is met het oorspronkelijke doel. Op grond van artikel 6 lid 4 AVG en artikel 23 lid 1 AVG kan hierop een

⁵³ Commissie Koops, p. 159.

⁵⁴ Zie hiervoor ook de aanbeveling in de DPIA.

uitzondering worden gemaakt, als de verdere verwerking noodzakelijk is in het belang van onderzoek naar strafbare feiten is of als er een lidstatelijk economisch of financieel belang is (fiscale aangelegenheden⁵⁵). Ook dient men altijd de hoeveel data zoveel mogelijk te beperken (artikel 5 lid 1 sub c AVG).

4.5 Informatieplicht/transparantie

In artikel 12, 13 en 14 van de AVG is een plicht opgenomen voor de verwerkingsverantwoordelijke om passende maatregelen te nemen zodat de betrokkene de informatie ontvangt over de verzameling van de hem betreffende persoonsgegevens. De verwerkingsverantwoordelijke dient onder meer aan te geven waarvoor de verwerking is bestemd, en op basis van welke grondslag hij deze gegevens verwerkt. De verwerkingsverantwoordelijke wordt door deze artikel verplicht de betrokkene te informeren over alle aspecten van de verwerking: hoe, wat, waarom worden de gegevens verwerkt? Hoe lang? Welke gegevens betreft het?

4.5.1 INFORMATIEPLICHT TEN BEHOEVE VAN INDIVIDUEN

Het beginsel van transparantie brengt mee dat het voor betrokkene duidelijk is welke gegevens voor welke doeleinden worden verwerkt en met wie deze gedeeld worden (art. 5 lid 1 onder a AVG). Wat betreft het moment dat betrokkene geïnformeerd moet worden, is het van belang of de gegevens door de verwerkingsverantwoordelijke via betrokkene of een derde zijn verkregen.

In het geval de gegevens bij betrokkene zijn verkregen, dient de verwerkingsverantwoordelijke betrokkene al bij het verkrijgen van de gegevens te informeren. Hij dient informatie te verstrekken over onder meer: de doeleinden van verwerking, de ontvangers van de gegevens, de periode dat ze bewaard worden en de rechten die betrokkene heeft ten aanzien van de gegevens (art. 13 AVG). Indien de verwerkingsverantwoordelijke voornemens is de gegevens verder te verwerken voor een ander doel dan waarvoor de gegevens zijn verzameld, dan verstrekt deze vóór de verdere verwerking informatie over dat andere doel (art.13 lid 3 AVG).

Indien de verwerkingsverantwoordelijke de gegevens via derden heeft verkregen, moet de gegevensverantwoordelijke binnen een redelijke termijn, maar uiterlijk binnen één maand aan betrokkene de informatie verstrekken (art. 14 lid 3 onder a AVG). De informatieverstrekking aan betrokkene kan bij gegevensverkrijging via derden echter achterwege blijven als de verwezenlijking van de doeleinden van de verwerking onmogelijk wordt (art. 14 lid 5 onder b AVG).

Hoe dient de Belastingdienst om te gaan met deze plicht tot informatieverstrekking bij internetonderzoek? Een enge interpretatie van de AVG zou een plicht inhouden voor de Belastingdienst om iedere individueel belastingplichtige te informeren. Wellicht kan de Belastingdienst een beroep doen op de uitzonderingsgrond van artikel 23 AVG j. 41 UAVG lid 1 onder e en h. In dit artikel staat dat onder andere de informatieplicht uit de artikelen 13 en 14 AVG buiten toepassing gelaten kan worden als dit noodzakelijk is om een doelstelling van algemeen belang te waarborgen (zoals fiscale aangelegenheden) of om een taak op het gebied van toezicht of inspectie te waarborgen. Internetonderzoek zou onder een van deze belangen kunnen vallen. Echter dient de Belastingdienst dan nog rekening te houden met de eisen uit artikel 41 lid 2 UAVG, zie meer hierover in onderstaande paragraaf.

4.5.2 SECTORSPECIEKE WETGEVING MOGELIJK NODIG

Indien de Belastingdienst gebruik wil maken van deze uitzonderingsmogelijkheid om burgers níet te informeren over internetonderzoek, zal zij als verwerkingsverantwoordelijke zelf moeten bepalen of

⁵⁵ Dit is in de zaak van de Museumjaarkaart expliciet goedgekeurd (Rb. Amsterdam, 15-11-2018, nr. C/13/655200 / KG ZA 18-1059). Zie ook: Gerechtshof Amsterdam, 5 november 2019, ECLI (verkort): 3967.

dit gerechtvaardigd is. Artikel 41 lid 2 UAVG dwingt tot een zorgvuldige afweging. In dit lid zijn alle elementen opgenomen waarmee de verwerkingsverantwoordelijke rekening dient te houden. De Memorie van Toelichting op de AVG geeft aan dat van geval tot geval bepaald moet worden op welke verplichting een uitzondering wordt gemaakt. De verwerkingsverantwoordelijke mag alleen afwijken als dit strikt noodzakelijk is en op proportionele wijze gebeurt, en alleen op *individuele* basis. Indien de verwerkingsverantwoordelijke categorisch wil afwijken, dient sectorspecifieke wetgeving opgenomen te worden, aldus de toelichting.⁵⁶

Echter dient volgens artikel 41 UAVG lid 2 onder g en h de Belastingdienst rekening te houden met de risico's voor de rechten en vrijheden van de betrokkenen en het recht van betrokkene om van de beperking op de hoogte te worden gesteld (tenzij dit afbreuk doet aan het onderzoek/de controle). Dit betekent dat zodra het onderzoek is afgerond, de belastingplichtige alsnog geïnformeerd wordt over de informatievergaring (ook als geen besluit wordt genomen).

Vermoedelijk is deze sectorspecifieke wetgeving wel wenselijk voor de Belastingdienst met betrekking tot internetonderzoek gericht op toezicht en handhaving, zodat categorische afwijking van de plicht tot informeren wettelijk gewaarborgd is.

Bovenstaande gaat om de plicht om de individu te informeren met betrekking tot de raadpleging van persoonsgegevens. Indien dit op individuele basis onmogelijk blijkt voor de Belastingdienst en de uitzonderingswet nog even op zich laat wachten, is het raadzaam om – indien gestart wordt met internetonderzoek via OSINT – de belastingplichtige wel al zo goed mogelijk te informeren, al dan niet online.⁵⁷

4.5.3 INFORMATIEPLICHT BIJ ALGORITMEN

Een ander onderwerp, in het verlengde van transparantie, is het belang van transparantie rondom de inzet van algoritmen (data-analyses). Transparantie kan bijdragen aan het vertrouwen dat burgers in deze analyses hebben en de burger zal beter in staat zijn de werkwijze van de overheid bij een data-analyse te controleren en zo bijdragen aan een zo evenwichtig mogelijke verhouding tussen burger en overheid⁵⁸. Volgens de Richtlijnen voor het toepassen van algoritmes door overheden⁵⁹ dient een overheidsorganisatie die data-analyses verricht, op haar website het publiek te informeren over zaken als dat en waarom zij data-analyses uitvoert, wat de eventuele consequenties van de analyse voor betrokken burgers zijn, wat de wettelijke grondslag voor het uitvoeren van deze analyses is, welke kwaliteitsborging er plaatsvindt etc. Ook uit de SyRi-uitspraak wordt duidelijk dat de overheid inzicht moet bieden in de risicomodellen. Of voor de Belastingdienst een uitzondering geldt, dient nader te worden uitgezocht.

4.6 Juistheid van gegevens

Artikel 5 lid 1 onder d geeft aan dat de verantwoordelijke moet zorgen voor juistheid van de persoonsgegevens en dat deze gegevens zonedig moeten worden geactualiseerd of verwijderd wanneer deze onjuist blijken.

⁵⁶ Intro op de AVG uit MvT, Kamerstuk 34851, nr. 3, p. 47-49

⁵⁷ De Handhavingsstrategie is over het gebruik van internet als bron zeer summier, zie p. 20. <https://over-ons.belastingdienst.nl/wp-content/uploads/2017/02/Handhavingsstrategie-Belastingdienst.pdf>

⁵⁸ Zie ook de SyRi-uitspraak waarin de rechter de Nederlandse Staat o.a. liet weten dat zij inzicht miste in de risicomodellen.

⁵⁹ <https://www.rijksoverheid.nl/documenten/rapporten/2019/10/08/tk-bijlage-over-waarborgen-tegen-risico-s-van-data-analyses-door-de-overheid>

⁶⁰ Zo claimde een politiek vluchteling dat zijn profiel op LinkedIn bewust niet klopte, zie uitspraak rechtbank

Persoonsgegevens die via internetonderzoek worden verzameld zijn niet altijd betrouwbaar⁶⁰ en verifieerbaar. Voor de inspecteur en de OSINT-medewerker is het vanuit privacyrechtelijk oogpunt van belang dat de gegevens kloppen. Echter is vanzelfsprekend de juistheid van gegevens ook van belang zodra deze gegevens worden gebruikt als bewijs in een dossier dat ten grondslag ligt aan een besluit. Controle aan de hand van objectieve gegevens is raadzaam, anders bestaat de kans dat het besluit strandt in verband met onzorgvuldige voorbereiding en onvoldoende motivering⁶¹. Voorafgaand, bij de opzet van het (internet)onderzoek en tijdens het onderzoek, dienen de inspecteur en de OSINT-medewerker zich bewust te zijn van dit risico.

4.7 Beveiliging en opslag

Het behoeft een aparte analyse (al dan niet in een DPIA) hoe de beveiliging is bewerkstelligd met betrekking tot de gegevens die via internetonderzoek worden verwerkt en valt buiten de reikwijdte van dit stuk. Het is volgens de AVG verplicht de beveiliging in kaart te brengen en passende en organisatorische maatregelen te nemen (o.a. artikel 32 AVG). De DPIA meldt hierover in dit stadium alvast het volgende:

“Team OSINT moet als onderdeel van de Belastingdienst (BD) voldoen aan de BIO, die door BD is vertaald in de Integrale Beveiliging Belastingdienst (IBB), die in 2020 is ingegaan. Huidige werkwijze OSINT (zij werkt buiten de reguliere omgeving BD) voldoet daar nu niet aan. BIO heeft 3 beveiligingsniveaus, gelet op risicoprofiel van activiteiten van OSINT moet BBN (Basis Beveiligings Niveau)niveau voor OSINT worden bepaald, zodat OSINT proces daarop kan/moet worden afgestemd. Op basis van de resultaten van deze DPIA zullen we in DPIA adviseren welk BBN niveau passend is.”

Overigens is in artikel 67 Awr min of meer een organisatorische beveiligingsmaatregel opgenomen. Dit artikel behelst een geheimhoudingsplicht voor de medewerker bij de Belastingdienst:

Het is een ieder verboden hetgeen hem uit of in verband met enige werkzaamheid bij de uitvoering van de belastingwet over de persoon of zaken van een ander blijkt of wordt meegedeeld, verder bekend te maken dan noodzakelijk is voor de uitvoering van de belastingwet of voor de invordering van enige rijksbelasting als bedoeld in de Invorderingswet 1990 (geheimhoudingsplicht).

In lagere regelgeving is een uitzondering opgenomen voor onder andere het delen van informatie met andere overheidsorganen.⁶²

4.8 DPIA

De AVG vereist niet dat een DPIA wordt uitgevoerd voor elke verwerking die risico's voor de rechten en vrijheden van natuurlijke personen kan inhouden. Een DPIA is alleen verplicht als de verwerking "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen" (artikel 35, lid 1, geïllustreerd door artikel 35, lid 3, en aangevuld door artikel 35, lid 4). Een DPIA is bijzonder relevant wanneer een nieuwe technologie voor gegevensverwerking wordt geïntroduceerd, aldus de Working Group 29.⁶³

In gevallen waarin het niet duidelijk is of een DPIA vereist is, raadt de WP29 aan om deze toch uit te voeren omdat een DPIA een nuttig instrument is dat verwerkingsverantwoordelijken helpt om aan de

Den Haag van 8 juni 2017 (ECLI:NL:RBDHA:2017:6180). In een andere zaak, van 19 juli 2016, werd één Facebook-bericht niet als voldoende bewijs beschouwd (ECLI:NL:RBDHA:2016:8215).

⁶¹ Zie bijvoorbeeld uitspraak Raad van State van 21-08-2013 ECLI:NL:RVS:2013:792

⁶² Zie artikel 43c Uitvoeringsregeling Awr.

⁶³ Groep Gegevensbescherming artikel 29, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, p. 9

wetgeving inzake gegevensbescherming te voldoen. 'Internetonderzoek' wordt niet als zodanig genoemd in de AVG, echter heeft de Working Group 29 een aantal voorbeelden verzameld van verwerkingen met 'waarschijnlijk een hoog risico'. In de bijlage is deze opsomming opgenomen (zie WP29- Overzicht Verwerkingen). Een grove inschatting leert dat de Belastingdienst met internetonderzoek waarschijnlijk een hoog-risico verwerking zal uitvoeren, waarschijnlijk is sprake van verwerking onder punt 1, 2, 3, 5, 6, 8 en 9. In de meeste gevallen kan een verwerkingsverantwoordelijke ervan uitgaan dat voor een verwerking die aan twee criteria voldoet een DPIA moet worden uitgevoerd.

Het is per definitie raadzaam om een DPIA uit te voeren. De positie van de Belastingdienst als bestuursorgaan verlangt een zorgvuldige opstelling tegenover de burger (immers is sprake van een bepaalde onevenwichtigheid), zeker indien ook vanwege internet als nieuw te ontsluiten bron en de onzekerheden die dit met zich meebrengt.

4.9 Conclusie

Over het algemeen kan geconcludeerd worden dat de grondslag voor internetonderzoek aanwezig is. Echter kunnen bepaalde, meer ingrijpende onderzoeken, een specifiekere grondslag verlangen. Hiervoor dient nieuwe wetgeving te komen, mocht de noodzaak en behoefte zijn tot meer ingrijpende onderzoeken bij de Belastingdienst. Verder is duidelijk dat stelselmatig verzamelen nu niet toegestaan is, maar dat de jurisprudentie geen duidelijk beeld geeft wat wél is toegestaan met betrekking tot de mate van inbreuk in iemands privéleven (proportioneel is). Het inschatten van de mate van inmenging zal helpen bij de interne afweging die de Belastingdienst zelf dient te maken omtrent de ernst van de inbreuk en de noodzakelijkheid. Hiervoor kunnen de 'factoren' gebruikt worden uit de bijlage. Tevens is het raadzaam om een DPIA uit te voeren.

De informatieplicht verlangt een bepaalde transparantie van de Belastingdienst richting de belastingplichtige. Indien de Belastingdienst structureel hier van wilt afwijken, dient sectorspecifieke wetgeving opgesteld te worden.

Hoofdstuk 5 Enkele juridische uitdagingen/risico's

Hierna volgen enkele onderwerpen, gerelateerd aan het doen van internetonderzoek, die in de praktijk vragen oproepen.

5.1 Geen specifieke wettelijke grondslag voor internetonderzoek

De Awb en de AWR bevatten geen specifieke grondslag voor het doen van *internetonderzoek*. Artikel 3:2 Awb betreft een algemeen artikel waarin het bestuur verplicht wordt zich een goed beeld te vormen van de bij een besluit betrokken belangen. Het artikel houdt een gedeeltelijke codificatie in van het zorgvuldigheidsbeginsel. Dit algemene beginsel van behoorlijk bestuur houdt in dat een bestuursorgaan een besluit zorgvuldig dient voor te bereiden en te nemen.

De Belastingdienst kan op basis van het algemene zorgvuldigheidsbeginsel de benodigde kennis achterhalen op het internet (artikel 3:2 Awb). Daarnaast heeft de inspecteur onderzoeksbevoegdheden toegekend gekregen teneinde de naleving van de verplichtingen van belastingplichtigen te waarborgen. Zonder deze 'controlebevoegdheden' zou een maatschappelijk verantwoorde belastingheffing niet mogelijk zijn. De wettelijke grondslagen voor deze bevoegdheden zijn in de AWR bijeengebracht in de afdeling 'Verplichtingen ten dienste van de belastingheffing'. In art. 47 t/m 56 AWR van deze afdeling zijn voor de belastingplichtige bijkomende verplichtingen neergelegd op grond waarvan de inspecteur bevoegd is om ten dienste van de belastingheffing informatieverplichtingen op te leggen. De inspecteur kan ingevolge art. 47 AWR

informatie vorderen van de belastingplichtige zelf, en ingevolge art. 53 AWR, respectievelijk 55 AWR, ook van administratieplichtigen en overheidslichamen. Ook kan de inspecteur ingevolge art. 50 AWR waarnemingen ter plaatse (WTP) verrichten.

De genoemde algemene grondslag lijkt vooralsnog voldoende in de praktijk. Er is nog geen rechtspraak beschikbaar over de reikwijdte van deze grondslag. Al kan dit in de toekomst veranderen zodra een belastingplichtige dit ter discussie stelt.

Internetonderzoek op kleine schaal is tot nu toe niet als onrechtmatige onderzoeksmethode aangemerkt. Zie bijvoorbeeld een uitspraak van Rechtbank Noord-Holland van 12 september 2018 waarin de belastinginspecteur de profielpagina op LinkedIn heeft gebruikt in zijn onderzoek. Dit vormde geen aanleiding voor discussie.⁶⁴ Echter blijft de vraag hoe de rechter zou oordelen als dit wél een onderwerp was dat de rechter moet beoordelen. Ook op grotere schaal lijkt internetonderzoek 'door de beugel' te kunnen, al is de kritiek in de literatuur dat de rechter onvoldoende gekeken heeft naar de manier van zoeken op het internet.⁶⁵

Echter is de vraag of het algemene artikel uit de Awb wel voldoende specifiek is. Is dat niet het geval, dan dient een grondslag in specifiekere (sectorale) wetgeving aanwezig te zijn. Interessant om na te gaan is of zo'n specifieke grondslag er altijd is voor internetonderzoek. Stel dat we uitgaan van de grondslag in artikel 47 Awr.

Artikel 47 lid 1 Awr luidt:

Ieder is gehouden desgevraagd aan de inspecteur:

a. de gegevens en inlichtingen te verstrekken welke voor de belastingheffing te zijnen aanzien van belang kunnen zijn;

b. de boeken, bescheiden en andere gegevensdragers of de inhoud daarvan - zulks ter keuze van de inspecteur - waarvan de raadpleging van belang kan zijn voor de vaststelling van de feiten welke invloed kunnen uitoefenen op de belastingheffing te zijnen aanzien, voor dit doel beschikbaar te stellen.

Artikel 47 Awr stelt kortweg dat als de inspecteur *erom vraagt* (desgevraagd), de belastingplichtige (of een derde) gegevens moet verstrekken. Bij internetonderzoek is er geen sprake van rechtstreeks vragen aan de belastingplichtige, maar van *halen/vinden/aantreffen*. De verplichting in artikel 47 Awr betreft bovendien vooral een verplichting voor de belastingplichtige, en lijkt minder geschreven als een bevoegdheid voor de inspecteur. Het artikel 47 Awr zal dus wellicht in de praktijk niet altijd afdoende zijn. Ter illustratie een specifiek artikel uit de Participatiewet, dat volgens de Centrale Raad van Beroep in ieder geval voldoende bevoegdheid creëerde voor het raadplegen van Facebook door een gemeente. Het betreft artikel 53a lid 6 Participatiewet, dat luidt: "Het college is bevoegd onderzoek in te stellen naar de juistheid en volledigheid van de verstrekte gegevens en zonodig naar andere gegevens die noodzakelijk zijn voor de verlening dan wel de voortzetting van bijstand. Indien het onderzoek daartoe aanleiding geeft kan het college besluiten tot herziening of intrekking van de bijstand." ⁶⁶

Vanuit het oogpunt van juridische zuiverheid is het raadzaam voor de Belastingdienst om artikelen zoals artikel 47 Awr te verrijken met een concretere onderzoeksbevoegdheid voor de inspecteur.

⁶⁴ Zie uitspraak van Rechtbank Noord-Holland van 12 september 2018 (ECLI:NL:RBNHO:2018:7806)

⁶⁵ Zie Rb. Amsterdam 5 april 2017, ECLI:NL:RBAMS:2017:2123; Rb. Amsterdam 15 februari 2018, ECLI:NL:RBAMS:2018:780; en Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442.

⁶⁶ Uitspraak Centrale Raad van Beroep, 4 juli 2017, ECLI:NL:CRVB:2017:2284

Tevens is het raadzaam om uit te zoeken of het nodig is om een wettelijke bevoegdheid te creëren voor de Belastingdienst ten behoeve van trendrapportages en marktonderzoeken. Zie bijvoorbeeld artikel 2 lid 4 Instellingswet van de Autoriteit Consument en Markt ter inspiratie: *“Tot de taken van de Autoriteit Consument en Markt behoort het uit eigen beweging doen van marktonderzoeken en maken van rapportages, indien dat naar haar oordeel nuttig is voor de uitvoering van de taken, bedoeld in het tweede lid.”* Met een soortgelijk artikel voor de Belastingdienst is dan meteen een grondslag aanwezig voor de internetonderzoeken die geen toezicht of handhaving betreffen, maar wel nuttig zijn voor het heffen en innen van belastingen.

TUSSENCONCLUSIE

De algemene grondslag van artikel 3:2 van de Awb lijkt vooralsnog afdoende. Afhankelijk van het type internetonderzoek kan het zijn dat een specifiekere grondslag vereist is. Dit zal echter moeten blijken na uitspraken van de rechter. Tot nu toe zijn niet veel burgers in staat om in hun verweer nauwgezet argumentatie aan te voeren met betrekking tot dit onderwerp en is het onderwerp niet nauwgezet beoordeeld door de rechter⁶⁷. Dit betekent echter niet dat de betreffende grondslag altijd juridisch zuiver is en levert dus een juridisch risico op voor de Belastingdienst. Mogelijk kunnen de huidige grondslagen iets specifieker gemaakt worden door een (techniekneutrale) onderzoeksbevoegdheid voor de inspecteur op te nemen.⁶⁸

5.2 Grote schaal: crawlen

Inherent aan bepaalde OSINT-middelen is dat binnen relatief korte duur een grote zoekactie kan worden gecreëerd. Crawlen is één van de processen of technieken die de Leidraad noemt die nu niet uitgevoerd mogen worden. Voorafgaand aan het bepalen van de ernst van de inbreuk dient allereerst te worden vastgesteld wat crawlen precies is en hoe dit werkt. Commissie Koops omschrijft een crawler als volgt:

“Een crawler is een geautomatiseerd proces dat binnen gestelde condities (zoals welke bronnen moeten worden doorzocht en op welke woorden of andere zoektermen moet worden doorzocht) al dan niet met gebruik van inloggegevens, als ware hij een gewone gebruiker, contact maakt met bronnen die via het internet toegankelijk zijn. De werking is afhankelijk van het type bron. Wanneer het gaat om webpagina's, zullen deze worden geladen en worden de daarop vastgelegde gegevens vergeleken met de zoekcriteria. De webpagina's die niet voldoen aan de criteria, worden niet opgeslagen. Wat wel voldoet aan de criteria wordt overgenomen.”

Over de inbreuk op de persoonlijke levenssfeer meldt de Commissie:

“De inzet van een crawler kan enerzijds, wanneer de crawler wordt voorzien van beperkingen, de inbreuk op de persoonlijke levenssfeer beperken, met name bij een korte looptijd. Anderzijds is de gecompliceerdheid of fijnmazigheid van de vooraf te maken inschatting over de te verwachten privacyinbreuk moeilijk te verwerken in een crawler. Ook is tussentijdse aanpassing naar bevind van zaken nauwelijks mogelijk. Bovendien is het mogelijk dat zelfs indien vooraf beperkingen aan een crawler worden meegegeven, bij langere looptijd de uiteindelijke datasets niet veel afwijken van onbeperkte crawlers; dit zal mede afhangen van het gebruikte type crawler.”

De crawler doorzoekt grote hoeveelheden gegevens op relevantie. Alleen relevante gegevens worden *overgenomen*. De andere gegevens worden alleen *doorzocht*. Commissie Koops meldt hierover: *“Een bijzonder aspect aan de inzet van een crawler is dus dat er ook een (kleine) inbreuk op*

⁶⁷ Art. 8:69 lid 1 Awb

⁶⁸ E.e.a. dient verder uitgewerkt te worden. Bovenstaande dient ter inspiratie voor het project Wetsvoorstel Gegevensverwerking.

de persoonlijke levenssfeer plaatsvindt ten aanzien van de personen wier gegevens door de crawler zijn onderzocht, maar niet zijn overgenomen. Het betreft gegevens die op een in beginsel onbeperkte hoeveelheid plaatsen op het internet kunnen worden aangetroffen.”

De Commissie Koops wijst erop dat hier dus geen sprake is van *kennismemen* of *overnemen*, maar van een zekere vorm van *geautomatiseerd onderzoek* zonder dat het desbetreffende gegeven ooit door de ogen van een mens wordt gezien of ooit wordt opgeslagen in een systeem.⁶⁹ De Commissie Koops geeft aan dat hier wel sprake is van een inbreuk, maar dat dit een ander type inbreuk is dan wanneer het gaat over een inbreuk op de persoonlijke levenssfeer van *specifieke personen*. De Commissie is van oordeel dat er geen sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer.

TUSSENCONCLUSIE

Het is goed mogelijk dat crawling in strijd is met het beginsel van dataminimalisatie uit de AVG. Immers wordt (mogelijk) een groot aantal persoonsgegevens doorzocht. Echter vindt de Commissie dat dit niet meer dan een geringe inbreuk betreft, daar het geen specifieke personen aangaat en de meeste data niet door een mens wordt gezien of wordt opgeslagen in een systeem. Ook speelt de feitelijke toegankelijkheid van de bron een rol.

Daarnaast geeft de Commissie als argument dat voor het automatisch scannen van kentekens voorafgaand aan het vastleggen (van enkel de hits) nu ook al kan onder het algemene artikel 3 Politiewet 2012. In tegenstelling tot het beweerde in de Leidraad lijkt crawling an sich geen reden om internetonderzoek niet te verrichten. Wel dient het gebruik omkleed te zijn met voldoende waarborgen.

5.2.1 CRAWLEN EN DE BELASTINGDIENST

Mogelijk kan de Belastingdienst beheersmaatregelen nemen door vooraf goed in kaart te brengen welke data benodigd is en aan te geven wat er gebeurt met de data die enkel wordt doorzocht (maar niet wordt overgenomen). Tevens zou de Belastingdienst beheersbare beperkingen vóór aan de crawler mee kunnen geven, een korte looptijd van de zoektocht kunnen meegeven en tussendoor controlemomenten kunnen inplannen. Ook is het raadzaam om een afgeschermd en beveiligde omgeving te creëren door de data afkomstig van het internetonderzoek, zonder koppeling met de bestaande Belastingdienst-systemen. Commissie Koops omschrijft het als ‘de kluis’: ‘en waarbij wel, omwille van toetsbaarheid, de vergaarde gegevens wel in de afgeschermd omgeving, de “kluis”, bewaard blijven tot na afloop van de zaak, zonder dat deze gegevens gebruikt kunnen worden voor andere doeleinden.’⁷⁰

5.3 Grote schaal: scraping

De Leidraad noemt ook ‘scraping’ als element waarvoor meer informatie benodigd is voordat aan internetonderzoek via OSINT begonnen kan worden. Scraping ligt echter in het verlengde van crawlen. Bijzonder hoogleraar Oerlemans vat het verschil tussen crawlen en scrapen als volgt samen: “Een crawler is kortgezegd een programma dat binnen ingestelde condities (zoals welke bronnen moeten worden doorzocht en op welke woorden of andere zoektermen moet worden doorzocht) gegevens van internet verzamelt, zoals webpagina’s die voldoen aan de criteria, en deze vervolgens

⁶⁹ Het OSINT-team binnen de Belastingdienst is zich bewust van dit verschil. Dit ((rechts)filosofische én technische) punt zal idealiter bij de voorbespreking van een internetonderzoek besproken moeten worden. Zie voor de filosofische inslag ook:

https://nl.wikipedia.org/wiki/Als_een_boom_in_een_bos_omvalt_...#:~:text=Het%20vallen%20van%20de%20boom,%2C%20is%20er%20geen%20geluid.%22

⁷⁰ Commissie Koops, p. 167

indexeert. Als daarbij ook gegevens worden vastgelegd, wordt gesproken van een ‘scraper’.⁷¹ Zowel crawling als scraping zijn technieken die het OSINT-team van de Belastingdienst ook kan inzetten.

Voor deze algemene juridische analyse is het niet relevant om een scraping-tool te analyseren. Of nu scraping, crawling of een ander proces wordt gebruikt, het gaat uiteindelijk om de vraag hoe ernstig de mate van inbreuk in iemands privéleven is wanneer zo’n proces wordt gebruikt. Omdat een scraper of crawler van te voren ingesteld kan worden en dus het zoekgedrag beïnvloed kan worden door de input van de inspecteur of OSINT-medewerker, staat niet van te voren vast dat het gebruik van deze processen/technieken per definitie een grote inbreuk in iemands privéleven oplevert. Dit zal van onderzoek tot onderzoek verschillen. De zorgvuldige beoordeling vooraf door een bestuursorgaan – dus het bepalen van de inzet van de middelen, de zoekwoorden etc. bij een internetonderzoek – is van groot belang. Naar aanleiding van bovenstaande zal dus niet apart een analyse volgen van scraping.

Wel is van belang om de uitspraak van de Rechtbank van Amsterdam⁷² aan te halen. In deze zaak werd scraping gebruikt op de website van Airbnb ter handhaving van het woonbeleid van de gemeente Amsterdam. De rechter is akkoord gegaan met het gebruik van de scraper. Echter merken hogleraren Oerlemans en Schuurmans op dat de rechtbank meer inzichtelijk had moeten maken hoe groot de privacy-inbreuk is en hoe verstrekkend de omvang van de gegevensverzameling is geweest.⁷³ De rechter heeft nagelaten om te kijken naar de instellingen van de scraper. Dit terwijl de omvang en het type gegevens en de zoekmethode zeer relevante factoren zijn bij de beoordeling in welke mate sprake is van een privacyinbreuk (zie de ‘Factoren’ van de Commissie Koops in Hoofdstuk 4).

TUSSENCONCLUSIE

Ook hier blijkt weer dat de jurisprudentie technieken zoals scraping nog niet afkeurt, maar dat vanuit de rechtswetenschap wel vragen bestaan over inzet van dit soort middelen. Dit vormt een juridisch risico voor de Belastingdienst, waarvoor diverse beheersmaatregelen genomen dienen te worden, zoals een zorgvuldige en aantoonbare beoordeling vóór af van de aanpak van het onderzoek.

5.4 Heimelijk waarnemen

Het waarnemen en eventueel verzamelen van persoonsgegevens via internet door de Belastingdienst, zal in de praktijk – in eerste instantie – heimelijk zijn. De betrokkene wordt dus niet op de hoogte gesteld van het feit dat informatie van hem wordt verzameld. Dit zal met name plaatsvinden bij het type internetonderzoek dat toezicht of handhaving betreft, waarbij vermoedens al dan niet bevestigd worden door informatie afkomstig van publiek toegankelijke bronnen. Indien de belastingplichtige vooraf wordt geïnformeerd, bestaat de kans dat het online bewijsmateriaal gewist of bewerkt wordt. De vraag is of heimelijk waarnemen online is toegestaan.

De wet verbiedt heimelijk waarnemen op zichzelf genomen niet. Maar indien een minder ingrijpend middel voorhanden is om hetzelfde doel te bereiken, dan dient dat middel gebruikt te worden (subsidiariteitsbeginsel). Ook zal een overheidsorgaan altijd rekening moeten houden met de algemene beginselen van behoorlijk bestuur en de informatieplicht die vanuit de AVG bestaat. Het heimelijk waarnemen kan mogelijk worden gerechtvaardigd indien het noodzakelijk is voor de uitoefening van een taak van algemeen belang: artikel 6 lid 1 onder e AVG. Dit betekent dat de Belastingdienst de noodzakelijkheid van de heimelijkheid goed moet kunnen onderbouwen. Indien

⁷¹ Zie artikel J.J. Oerlemans in Tijdschrift Modernisering Strafvordering, Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk. Afl. 2, 2018.

⁷² Rechtbank Amsterdam, 27 juni 2018 ECLI:NL:RBAMS:2018:4442

⁷³ Internetonderzoek door bestuursorganen, J. Oerlemans & Y. Schuurmans, 20 mei 2019.

het gaat om stelselmatige heimelijke waarneming, zullen overigens andere (strengere) eisen gelden. Zo is het in het strafrecht verplicht om dan eerst een bevel van de Officier van Justitie te verkrijgen.

De AVG verlangt daarnaast dat bij het verwerken van persoonsgegevens de betrokkene wordt geïnformeerd en de verwerkingsverantwoordelijke transparant is over de verwerking (zie hoofdstuk 4 onder Informatieplicht). Dit kan voor een organisatie die veelvuldig informatie van het internet afhaalt én dat heimelijk wil doen, in de praktijk onwerkbaar zijn. Mogelijk kan de Belastingdienst een beroep doen op de uitzondering die is opgenomen in artikel 23 AVG en 41 UAVG en volstaan met uitleg op haar website over internetonderzoek.⁷⁴ Een meer strikte benadering, uitgaande van de toelichting op de wet, verlangt echter dat bij categorisch afwijken van de informatieplicht een aparte, specifieke grondslag vereist is (zie Hoofdstuk 4, Informatieplicht/transparantie, Sectorspecifieke wetgeving mogelijk nodig).

In de Juridische Verkenning Internet onderzoek uit 2013⁷⁵ wordt nog de vraag gesteld of heimelijk onderzoek op het internet vergeleken kan worden met heimelijke waarneming ter plaatse. De conclusie daarin is: wat offline is toegestaan, mag online ook. Deze constatering is zeven jaar later enigszins achterhaald, omdat ondertussen uit jurisprudentie reeds blijkt dat internetonderzoek wordt toegestaan en wordt beschouwd als een onderzoeksmethode die valt onder de wetgeving voor 'niet-internetonderzoek'. Wel is ondertussen de vraag of de conclusie 'wat offline mag, mag online ook' soms niet te kort door de bocht is, daar (de anarchie van) het internet niet geheel te vergelijken is met de offline wereld. Commissie Koops merkt wat betreft stelselmatige observatie online hierover op: "De aanwezigheid, het gedrag of de bewegingen van de persoon worden in geval van stelselmatige observatie "realtime" gevolgd of waargenomen en daarmee feitelijk vastgesteld, al dan niet met behulp van een technisch hulpmiddel. Bij het onderzoek in open bronnen (red.: op het internet) gaat het daarentegen vooral om "historische" gegevens die reeds aanwezig en beschikbaar zijn."⁷⁶ Bij de beoordeling van het wetsvoorstel tot vernieuwing van het Wetboek van Strafvordering pleitte de Commissie daarom voor een aparte grondslag voor stelselmatige observatie in open bronnen.⁷⁷

5.4.1 GROTE SCHAAL ÉN HEIMELIJK = DPIA

De Autoriteit Persoonsgegevens heeft grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld met onderzoek, zonder de betrokkene daarvan vooraf op de hoogte te stellen, gekwalificeerd als gegevensverwerking dat een hoog privacyrisico oplevert⁷⁸. De Autoriteit Persoonsgegevens geeft als voorbeeld: "... heimelijk onderzoek door particuliere recherchebureaus, onderzoek voor fraudebestrijding en onderzoek op internet voor bijvoorbeeld online handhaving van auteursrechten."

Indien de Belastingdienst dus heimelijk internetonderzoek op grote schaal wil verrichten, dient zij apart een DPIA uit te voeren. Voor een internetonderzoek op grote schaal, met enkel als doel 'markt- of fenomeenonderzoek' dat geen rechtsgevolgen voor betrokkenen inhoudt zal de Belastingdienst een andere DPIA moeten uitvoeren dan voor internetonderzoek op grote schaal met als doel handhaving van normen uit het Belastingrecht.

⁷⁴ In het verleden dienden verwerkingsverantwoordelijken een voorafgaande raadpleging te verrichten bij het College Bescherming Persoonsgegevens. Zie hiervoor https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2004-1649_procesbeschrijving.pdf

⁷⁵ Juridische Verkenning Internet onderzoek, 2013, Landelijk Kenniscentrum.

⁷⁶ Commissie Koops, p. 168.

⁷⁷ Het wetsvoorstel is nog niet definitief ten tijde van het schrijven van deze analyse.

⁷⁸ Staatscourant 2019 nr. 64418 27 november 2019

Intern zal beraadslaging moeten plaatsvinden om na te gaan wat de Belastingdienst als ‘grootschalig’ beschouwt. Daar geeft de wet of de AP geen uitleg bij.⁷⁹ Het kan raadzaam zijn om, gezien de positie van de Belastingdienst als overheidsorgaan én de onzekerheden die internetonderzoek met zich meebrengen, in de beginfase per definitie een DPIA uit te voeren, zelfs als geen sprake is van ‘grootschaligheid’.

Verder geldt dat wanneer na implementatie van uit de DPIA voortkomende beheersmaatregelen de risico's daarmee onvoldoende kunnen worden gereduceerd en deze nog steeds hoog blijven, een organisatie verplicht is de verwerking eerst aan de AP voor te leggen (voorafgaande raadpleging) en toestemming van de AP moet verkrijgen om met de verwerking te mogen starten.

5.5 Gefingeerde accounts

De vraag die uit de Leidraad te abstraheren is, is of de Belastingdienst onder een andere identiteit mag interacteren met belastingplichtigen. Dit betreft een vraagstuk met betrekking tot *onderzoeksbevoegdheid* in de eerste plaats. Mag de Belastingdienst dit op basis van bestaande wetgeving ten aanzien van toezicht en handhaving en hoe dient de Belastingdienst als bestuursorgaan zich te gedragen ten opzichte van de burger/belastingplichtige? Deze vragen zullen in dit stuk niet aan de orde komen, omdat dit een onderwerp is wat een aparte analyse verlangt. Zie ook over dit onderwerp Hoofdstuk 2 – Inloggen met een account. Daarnaast betreft het interacteren met een belastingplichtige onder een andere identiteit ook een vraagstuk dat het privacyrecht raakt. Zodra de Belastingdienst rechtmatig een gefingeerd account heeft aangemaakt om bepaalde informatie bij belastingplichtige te achterhalen, luidt de vraag of de belastingplichtige ook *geïnformeerd* dient te worden over het feit dat – indien het persoonsgegevens betreft – data bij hem verkregen is, volgens de regelgeving van de AVG. Over de informatieplicht is meer uiteengezet in hoofdstuk 4. Tevens betreft het gebruik van een gefingeerd account (als dit al is toegestaan) een vorm van heimelijk internetonderzoek. Zie hierover meer onder het kopje ‘Heimelijk waarnemen’ van hoofdstuk 5.

5.6 ‘Bijvangst’

Wat te doen als het internetonderzoek (veel) meer persoonsgegevens opbrengt dan was voorzien? En de gegevens misschien wel bruikbaar zijn voor de Belastingdienst, maar niet voor het onderzoeksdoel? In het strafrecht wordt dit wel ‘bijvangst’⁸⁰ genoemd. Deze situatie is niet expliciet geregeld in het bestuursrecht. De algemene beginselen van behoorlijk bestuur bieden aanknopingspunten: de overheid dient haar onderzoeksproces zorgvuldig in te richten, niet willekeurig te handelen en mag geen misbruik maken van haar positie.

Indien meer gegevens dan beoogd wordt binnengehaald, bestaat de kans dat een bestuursorgaan verweten wordt aan ‘fishing expedition’ te doen. In een zaak waarbij een belastingplichtige de Belastingdienst verweet aan een ‘fishing expedition’ te doen meldt de Hoge Raad het volgende:

“De uitdrukking ‘fishing expedition’ wordt dikwijls in de mond genomen in dit verband, maar wat hieronder moet worden verstaan is nergens in de wet omschreven. Zij roept associaties op met een ‘sleepnet’ dat over de zeebodem wordt gehaald, waarmee niet alleen de beoogde vissoorten of fruits de mer boven water worden gehaald maar ook ‘bijvangst’. De uitdrukking ontbeert evenwel de juridische precisie die mag worden verwacht wanneer het gaat om de afbakening van overheidsbevoegdheden en grondrechten. In wezen betreft het hier een toepassing van de eisen van

⁷⁹ Wel is voor de zorgsector een uitleg beschikbaar:

<https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/uitleg-begrip-%E2%80%98grootschalig%E2%80%99-verduidelijkt-voor-alle-zorgaanbieders>

⁸⁰ Zie CBb 09-07-2015, ECLI:NL:CBb:2015:193 en hierover ook Commissie Koops, p. 160.

proportionaliteit. Indien sprake is van een inmenging door een overheidsorgaan in de uitoefening van het recht op privacy (want daar gaat het meestal om in dit type gevallen), vereist art. 8 lid 2 EVRM niet alleen dat de inmenging in de wet is geregeld, maar ook: dat de inmenging plaatsvindt ten behoeve van een legitiem doel; dat de inzet van het door de overheid gebezigde middel in een redelijke verhouding staat tot dat doel (proportionaliteit), in welk verband mede van belang is of een andere, minder belastende methode beschikbaar is om dat doel te bereiken (subsidiariteit). Ten slotte is een afweging vereist van de wederzijds bij het concrete geval betrokken belangen. Een zoekactie door de Belastingdienst zonder een concrete aanwijzing dát de persoon van wie de informatie wordt gevorderd in staat is de gevraagde informatie te verschaffen, of zonder concrete aanduiding van de te verschaffen informatie, zal niet snel aan deze verdragsrechtelijke vereisten voldoen.”⁸¹

De Hoge Raad verlangt dus samenvattend dat de inmenging bij wet geregeld is, dat het plaatsvindt ten behoeve van een legitiem doel, dat het middel redelijk is ten opzichte van het doel, dat er geen minder belastende methode is en de Hoge Raad verlangt een afweging van de wederzijdse belangen.

Het is niet altijd uit te sluiten dat bij internetonderzoek ‘bijvangst’ optreedt. Echter is er een nuanceverschil aan te brengen: enerzijds bestaat de situatie waarin bij internetonderzoek van te voren reeds een groot sleepnet wordt ingezet (om in de termen van de Hoge Raad te blijven) met veel ‘vangst’ als gevolg en anderzijds de situatie waarin een zo klein mogelijk net wordt ingezet en tóch meer wordt gevangen dan beoogd. In dat laatste geval zal het verwijt ‘fishing expedition’ minder waarschijnlijk zijn, aangezien het internetonderzoek al was gestart met een zo klein mogelijk net. Echter dient dan wel te zijn voldaan aan de eisen zoals de Hoge Raad stelt.

De Belastingdienst zal dit bij de inrichting van haar proces voorafgaand aan het internetonderzoek zoveel mogelijk bijvangst moeten voorkomen, maar de Belastingdienst zal óók rekening moeten houden met het scenario dat bijvangst optreedt en hiervoor een proces inrichten dat zo zorgvuldig mogelijk omgaat met de gegevens uit de bijvangst (ongezien ‘teruggooien in zee’), helder vooraf de belangenafweging uiteenzet en zich vergewist van een legitieme aanleiding, doel en grondslag. Ook relevant zal zijn in welke mate de persoonsgegevens verwerkt worden: betreft het slechts een doorzoeking door een software of worden de gegevens opgeslagen en ingezien door medewerkers? Zie hierover ook de paragraaf over crawling. Echter blijft dit terrein enigszins onontgonnen en verdient dit nader onderzoek.

Onderstaande procesbeschrijving bij stelselmatig overnemen van online gegevens, afkomstig van de Commissie Koops, is wellicht voor de Belastingdienst nog wel bruikbaar bij de inrichting van haar proces. Al moet opgemerkt worden dat het strafrecht een ander rechtsterrein is, waarbij ‘bijvangst’ dus ook al wettelijk geregeld is, in tegenstelling tot in het bestuursrecht:

“Op dat moment zou de zoekactie (op basis van het taakstellend artikel) moeten stoppen, waarbij de gevonden informatie naar huidig recht als bijvangst kan worden gebruikt. Daarbij moet wel worden aangetekend dat bij het stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen vaak minder tussenstappen in het onderzoeksproces mogelijk zijn. Dit kan betekenen dat pas op een later moment dan bij klassiek rechercheren het geval zou zijn duidelijk wordt dat de grens van stelselmatigheid nabij komt of mogelijk zelfs al is bereikt. De beoordeling zou in dat licht dus moeten plaatsvinden op het proces, niet het resultaat, waarbij dat proces zodanig ingericht zou moeten zijn dat naar redelijke verwachting voldoende herijkingpunten in het onderzoeksproces zitten om op tijd te kunnen constateren of stelselmatigheid is bereikt of bereikt zal gaan worden <.....> aan de rechter (achteraf) wettelijk het oordeel toe of de toepassing van de opsporingsmethode rechtmatig is geweest. Daarbij is niet alleen het daadwerkelijke resultaat van de inzet beslissend, maar vooral ook

⁸¹ Zie 2.30, Hoge Raad 09-06-2017, ECLI:NL:HR:2017:1039. Ook relevant in 2.30:

*het resultaat dat daarvan op voorhand redelijkerwijs mocht worden verwacht.*⁸²

TUSSENCONCLUSIE

Het kan dus voorkomen dat, ondanks de afbakening vooraf aan het internetonderzoek, gaandeweg het onderzoek blijkt dat toch een min of meer volledig beeld van bepaalde aspecten van iemands privéleven ontstaat en dat de ernst van de inmenging in privésfeer groter is dan in eerste instantie werd aangenomen. Het is raadzaam om als Belastingdienst een proces in te richten voor dit scenario (al dan niet ‘bijvangst’ genoemd), met voldoende waarborgen en herijkingspunten. Tevens dient een instructie bedacht te worden voor de situatie dat de bijvangst bestaat uit bijzondere persoonsgegevens waarvoor geen verwerkingsgrondslag bestaat.

5.7 Bijzondere persoonsgegevens

De AVG heeft als uitgangspunt dat de verwerking van bijzondere categorieën persoonsgegevens verboden is, tenzij een van de uitzonderingen zich voordoet. Het reikt te ver om alle categorieën persoonsgegevens in dit stuk te bespreken, evenals alle uitzonderingscategorieën, echter is het interessant om een eerste verkenning te doen omtrent ‘foto’s’, omdat de kans groot is dat via internetonderzoek foto’s worden aangetroffen. Hoe dient de Belastingdienst om te gaan met foto’s die zijn aangetroffen online?

Kenmerken over ras, geloof en gezondheid zijn vaak via foto’s waar te nemen. Foto’s van personen zijn daardoor bijna altijd als bijzondere persoonsgegevens te kwalificeren. De Hoge Raad hanteerde onder de Wbp een ‘strikte benadering’ en kwalificeerde foto’s en camerabeelden, met verwijzing naar de wetsgeschiedenis van de Wbp, als bijzondere persoonsgegevens⁸³. Deze benadering leidt tot een praktisch probleem: een foto kan op grond van deze benadering per definitie – behoudens uitdrukkelijke toestemming, kennelijke openbaarmaking van de betrokkene of een andere uitzonderingsgrond – niet worden verwerkt.

Voor profielfoto’s aangetroffen op profielen van sociale media kan met enige zekerheid vastgesteld worden dat deze kennelijk openbaar zijn gemaakt door de betrokkene zelf. Dit feit betreft een rechtmatige uitzondering voor de verwerking door de Belastingdienst.

Verder hanteert de Autoriteit Persoonsgegevens in 2006 al een pragmatische benadering: alleen wanneer een partij foto’s of ander beeldmateriaal publiceert met het doel om onderscheid te maken naar ras, het een ‘redelijke wetstoepassing’ is om beeldmateriaal aan te merken als een bijzonder persoonsgegeven. In 2016, ruime tijd na het arrest van de Hoge Raad uit 2010, herhaalde de AP deze pragmatische, ‘doelgerichte’ benadering in beleidsregels over cameratoezicht.⁸⁴ De AP week met dit standpunt uitdrukkelijk af van de Wbp, de Privacyrichtlijn en het genoemde arrest van de Hoge Raad. Of dit pragmatische standpunt van de AP ook stand houdt bij de rechter is nog onduidelijk. Als blijkt dat foto’s beschouwd kunnen worden als een ‘normaal’ persoonsgegeven, kan de Belastingdienst voor de verwerking van foto’s met persoonsgegevens – voor de foto’s die niet openbaar zijn gemaakt door de betrokkene - een beroep doen op artikel 6 lid 1 onder e.

⁸² Zie Commissie Koops, p. 160 en bijvoorbeeld HR 13 november 2012, ECLI:NL:HR:2012:BW9338, NJ 2013/413, m.nt. Borgers en ECLI: NL:PHR:2015:1029 (gevolgd door HR in ECLI:NL:HR:2015:1815) over observatie.

⁸³ HR 23 maart 2010, ECLI:NL:HR:2010:BK6331, r.o. 2.6.

⁸⁴ Autoriteit Persoonsgegevens, Cameratoezicht – Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens, 28 januari 2016 (hierna: Beleidsregels cameratoezicht), p. 26.

TUSSENCONCLUSIE

De wet geeft aan dat het verwerken van bijzondere persoonsgegevens verboden is. De rechter hanteert een strikte uitleg wat betreft foto's, de AP een meer pragmatische uitleg. Het is raadzaam om intern – Belastingdienst breed – een standpunt in te nemen over de verwerking van bijzondere persoonsgegevens en foto's in het bijzonder.

5.8 Bestandskoppeling

Hoe gaat de Belastingdienst om met persoonsgegevens, wellicht binnengehaald op grote schaal via OSINT-middelen. Mag en kan zij die koppelen aan data uit interne bronnen? Voorop gesteld dient de Belastingdienst zich te houden aan de beginselen van minimale gegevensverwerking en opslagbeperking. Zodra gegevens intern doorgestuurd én gekoppeld worden, wordt een inbreuk gemaakt op deze beginselen. Echter is bestandskoppeling op zich genomen niet verboden. Toch ligt dit onderwerp gevoelig doordat het bijeenbrengen van grote hoeveelheden data weer nieuwe privacyrisico's met zich meebrengt, denk hierbij aan verdere gegevensanalyse. Ook hier mag dit alleen plaatsvinden indien het *noodzakelijk* is voor het algemeen belang van een lidstaat, zoals een economisch of financieel belang (zie art. 6 lid 4 j. art 23 lid 1 AVG).

Binnen de sociale zekerheid maken de verschillende instanties ook gebruik van bestandskoppeling en geautomatiseerde gegevensanalyse om potentiële fraudeurs op te sporen. In de uitspraak over het Systeem Risico Indicatie (SyRI) toetste de rechtbank Den Haag aan art. 8 lid 2 EVRM en concludeerde echter dat SyRI hiermee strijdig was, met name omdat geen inzicht werd geboden in de gehanteerde risicomodellen.⁸⁵

Het behoeft een aparte analyse om uit te zoeken hoe ver de Belastingdienst met bestandskoppeling kan en mag gaan. Zie hiervoor een eerste uiteenzetting in de DPIA.

5.9 Verantwoordingsplicht en privacy by design and default

De Belastingdienst heeft met het verrichten van internetonderzoek te maken met een verantwoordings- en motiveringsplicht. Deze plicht komt voort uit diverse (ongeschreven) regelgeving in het bestuursrecht en het privacyrecht.

Bestuursrecht

Uit het zorgvuldigheidsbeginsel vloeit voort dat een bestuursorgaan altijd vooraf de inzet van bevoegdheden kiest: voorkomen moet worden dat halverwege het onderzoek blijkt dat het bestuursorgaan de onderzoeksbevoegdheid niet heeft (en er onrechtmatig jegens de burger is gehandeld). Tevens controleert het bestuursorgaan of voldaan is aan de voorwaarden van de bevoegdheid. Dit pleit dus voor een schriftelijke verantwoording vooraf.

Privacyrecht

De verwerkingsverantwoordelijke dient volgens artikel 5 lid 2 AVG de beginselen inzake verwerking (zie begin hoofdstuk 3 voor de beginselen) na te leven én te kunnen aantonen. Het gaat de AVG dus niet enkel om het voldoen aan de regelgeving, maar zij legt ook een nadruk op het kunnen *aantonen* dat men voldoet.

Artikel 24 van de AVG verlangt van de verantwoordelijke passende technische en organisatorische maatregelen te treffen om *aan te kunnen tonen* en te kunnen *waarborgen* dat voldaan is aan de eisen uit de AVG. Indien nodig dient ook een gegevensbeschermingsbeleid aanwezig te zijn (artikel

⁸⁵ Zie P&I, 'Bestandskoppeling voor fraudebestrijding in de sociale zekerheid' van I. van der Helm, afl. 5, oktober 2020.

24 lid 2 AVG). Tevens dient zoveel mogelijk vooraf, bij ontwerp en door instellingen vooraf, gegevensbescherming plaats te vinden (artikel 25 AVG, privacy by design and default). Zo dienen crawler-instellingen zoveel mogelijk beperkt te worden, bijvoorbeeld tot bepaalde type bronnen etc.

Ook is het van belang dat de verwerkingsverantwoordelijke kan onderbouwen waarom zijn belang (in casu van de Belastingdienst: financieel/economisch belang voor de staat) vóór gaat op het belang van de betrokkene (recht op eerbiediging privéleven). De belangenafweging dient helder uiteengezet te zijn om aan het noodzakelijkheidsvereiste te kunnen voldoen.

TUSSENCONCLUSIE

Om het verwerken van persoonsgegevens te verantwoorden en te motiveren, dient een toets plaats te vinden of er bij het internetonderzoek dat men voor ogen heeft, sprake is van een *meer dan geringe inbreuk*.⁸⁶ Tevens dient een toets plaats te vinden met betrekking tot de rechtmatigheid.

5.10 Conclusie

Voor de onderzoekspraktijk betekent bovenstaande dat voorafgaand aan een internetonderzoek een uitgebreide toetsing dient plaats te vinden, zodat conform het bestuursrecht en het privacyrecht wordt gehandeld. In dit stadium, waarin nog niet bekend is wélk type internetonderzoek zal worden uitgevoerd, is niet te voorspellen welke onderwerpen aan bod komen. Zoals in bovenstaand hoofdstuk duidelijk wordt, is een aantal vraagstukken niet eenvoudig op te lossen. Is bijvoorbeeld de wens om te werken met gefingeerde accounts? Op welk terrein? Hoe lang? Dan dient daar een nadere analyse op plaats te vinden. Een DPIA is een nuttig instrument voor een eerste inschatting van de privacyrisico's. Daarnaast dient dus sprake te zijn van vastlegging van de beoordeling vooraf en van de wijze van uitvoering van het onderzoek.

Hoofdstuk 6 Conclusie en samenvatting

6.1 De belangrijkste beheersmaatregel: focus op zorgvuldigheid, motivering en aantoonbaarheid

De inleiding van dit stuk bevatte de volgende kernvraag:

Aan welke juridische voorwaarden met betrekking tot privacywetgeving dient de Belastingdienst te voldoen om in lijn met wet-en regelgeving een internetonderzoek uit te mogen voeren?

Het gesimplificeerde antwoord op bovenstaande kernvraag luidt: de Belastingdienst dient te voldoen aan de eisen uit de AVG, Awr, Awb, EHRM, etc. en de betreffende jurisprudentie. Hierna zal echter een poging gedaan worden om de eerste bevindingen iets concreter samen te vatten.

6.1.1 NOODZAKELIJK VOOR ALGEMEEN BELANG

Naar alle waarschijnlijkheid zullen bij internetonderzoek bijna per definitie persoonsgegevens verwerkt worden. Het maakt hierbij niet uit of dit voor een individuele belastingplichtige plaatsvindt of voor meerdere belastingplichtigen. Het verwerken van persoonsgegevens mag niet zomaar volgens de AVG. De verwerking dient een grondslag te hebben (zowel in de Europese AVG als in nationale wetgeving) én dient te voldoen aan allerlei eisen met betrekking tot rechtmatigheid, proportionaliteit en veiligheid.

De Belastingdienst kan voor het verwerken van persoonsgegevens voor internetonderzoek een beroep doen op een van de zes rechtsgronden in de AVG, namelijk: de verwerking is *noodzakelijk* voor uitvoering van een taak van algemeen (economisch/financieel) belang. De taak van de Belastingdienst tot het heffen en innen van belasting is in nationale wet omschreven.

⁸⁶ Zie bijlage voor een mogelijke toets voor de praktijk: 17 factoren

Bovenstaande betekent niet dat de Belastingdienst zonder verdere maatregelen van start kan gaan met internetonderzoek. Het is ten eerste aan te bevelen om een DPIA te verrichten (zowel in deze fase als bij de daadwerkelijk start van een onderzoek), en om daarnaast een beoordeling te maken van de mate van inbreuk in privésfeer aan de hand van de 17 factoren van de Commissie Koops en om het afwegingskader vast te leggen, evenals de onderzoeksopzet en het proces, om zo te voldoen aan de verantwoordingsplicht en zorgvuldigheidsbeginsel uit het privacy- en bestuursrecht.

PROPORTIONALITEIT: MATE VAN INBREUK

De Belastingdienst maakt bij de verwerking van persoonsgegevens tijdens een internetonderzoek in meer of mindere mate een inbreuk op een of meerdere grondrechten van een belastingplichtige, zoals het recht op eerbiediging voor iemands privéleven of de bescherming van persoonsgegevens. De wet, jurisprudentie en de literatuur bieden nog geen eenduidig antwoord tot hoever deze inbreuk mag gaan. Zeker is nu dat het stelselmatig verzamelen niet mag (zie ANPR).

BEOORDELING VOORAF

Om met deze onzekerheid om te gaan, is het raadzaam dat voorafgaand aan het internetonderzoek bepaald wordt hoe groot de mate van inbreuk is in iemands privésfeer en hoe de belangenafweging heeft plaatsgevonden. Dit komt niet alleen de interne besluitvorming ten goede, maar wordt vanuit het zorgvuldigheidsbeginsel en motiveringsbeginsel ook verlangd van een bestuursorgaan. De vraag die dan ontstaat is hoe de Belastingdienst de mate van inbreuk in privésfeer dient te beoordelen. Het blijkt dat immers geen gedetailleerde wetgeving of jurisprudentie beschikbaar is met betrekking tot het gebruik van internetonderzoek of typische OSINT-middelen en inbreuk in iemands privésfeer.

FACTOREN

De factoren van de Commissie Koops kunnen bij de beoordeling behulpzaam zijn. De Commissie Koops heeft 17 factoren opgesteld die van invloed kunnen zijn op de beoordeling in welke mate sprake is van een privacy-inbreuk en raadt aan om deze factoren te benutten bij de beoordeling in welke mate sprake is van een privacy-inbreuk. Zoals uit de analyse en de factoren blijkt is het dus afhankelijk van het type internetonderzoek hoe groot de mate van privacy-inbreuk zal zijn en zal per onderzoek een afweging gemaakt moeten worden of deze doorgang vindt of niet.

6.1.2 KARAKTER VAN INTERNETONDERZOEK

Een extra uitdaging bij internetonderzoek wordt veroorzaakt door het feit dat de inhoud van de bron – in dit geval het World Wide Web – onbekend en soms ongelimiteerd is, in tegenstelling tot de reeds aanwezige bronnen. Het is daardoor lastiger te voorspellen welke data binnengehaald en dus verwerkt wordt. Echter is de aan te treffen data ook weer niet volledig onbeheersbaar. Integendeel. De zoektechnologieën van OSINT kunnen van te voren worden ingesteld wat betreft duur, locatie en zoekwoorden. Daarnaast is uiteraard een juiste mate van beveiliging en het hanteren van de juiste bewaartermijnen vereist voor de persoonsgegevens die daadwerkelijk verwerkt worden.

6.1.3 ZORGVULDIGHEID, MOTIVERING EN AANTOONBAARHEID

Bij internetonderzoek is het echter niet *uit te sluiten* dat *meer of andere* persoonsgegevens worden verwerkt dan was voorzien. Dit betekent dat van een bestuursorgaan dat internetonderzoek (op grote schaal) wil doen, een grote mate van zorgvuldigheid vooraf wordt gevraagd. De focus van de Belastingdienst dient te liggen op de *verwachting en zorgvuldigheid* in het proces vooraf.

Het is raadzaam om de context van internetonderzoek (het ontbreken van duidelijke normen, de gebruikte techniek etc.) expliciet te beschrijven in de onderzoeksvoorstellen. Het is tevens raadzaam om daarbij het afwegingskader (de ernst van de inbreuk versus de handhavingsactie) expliciet te maken. Wat bewoog de Belastingdienst om tóch internetonderzoek te doen, ondanks dat dit

onderzoek mogelijk een meer dan geringe mate van inbreuk in iemands privéleven kan hebben? Hierbij is de toets aan de hand van de factoren behulpzaam, evenals de vragenlijst en de lijst met mogelijke zoekhandelingen (zie de bijlage).

En het is ten slotte raadzaam om de onzekerheden van te voren zo goed mogelijk te beschrijven en procesmatig te beheersen: het vaststellen van zoekwoorden, het inbouwen van extra controlemomenten ten aanzien van de hoeveelheid data, type data etc. zodat tussendoor beoordeeld kan worden of de inbreuk nog steeds gering is of dat ondertussen een compleet beeld van bepaalde aspecten van iemands privéleven is ontstaan. Commissie Koops raadt aan om, als van te voren onvoldoende zicht is op wat men zal aantreffen aan persoonsgegevens, de medewerker eerst een oppervlakkig onderzoek te laten doen.⁸⁷ Dit is niet iets wat expliciet in wetgeving staat aangegeven. Hieruit blijkt dat ook enige mate van creativiteit wordt verlangd van het bestuursorgaan om zo zorgvuldig mogelijk te werk te gaan.

ENKELE BEHEERSMAATREGELEN

Het is gebruikelijk om de onzekerheden en risico's te beschrijven in de DPIA, evenals beheersmaatregelen. Vooruitlopend op de DPIA is een krachtige beheersmaatregel in dit kader de inrichting van een basisproces voor internetonderzoeken door team OSINT op grond van een DPIA op het beoogde proces, waarin de privacy risico's van het proces en benodigde beheersmaatregelen voor die risico's in beeld worden gebracht en geïmplementeerd.

En een ander belangrijk element is dat wordt vastgelegd, bijvoorbeeld in een uitgebreid (aanbod) formulier, dat alle door dat proces voorgeschreven stappen zijn doorlopen. Ook zou een beheersmaatregel kunnen zijn om – met name in de beginfase – als onderdeel van het basisproces nieuwe/afwijkende verzoeken te laten toetsen door een multidisciplinair team⁸⁸ waarin kennis wordt opgebouwd over de privacyaspecten van internetonderzoek. De inzichten die daar worden ontwikkeld kunnen desgewenst Belastingdienst breed worden ingezet.

6.2 Tot slot

Privacy en internetonderzoek met OSINT-middelen is – zo blijkt – zeker geen volledig ontgonnen terrein. Dit heeft te maken met onvoldoende specifieke wetgeving, onvoldoende jurisprudentie, met het karakter van de bron (de 'oneindige hoeveelheid persoonsgegevens'), de onbekendheid met de gebruikte zoektechnieken en enkele onzekerheden in het zoekproces. Om toch internetonderzoek te kunnen verrichten (en als Belastingdienst inzicht te krijgen in de economische werkelijkheid), luidt het advies om alle redelijke voorzorgsmaatregelen te nemen die van een bestuursorgaan verwacht mogen worden, zowel vanuit de wet bezien als vanuit de algemene beginselen van behoorlijk bestuur. Dit betekent dat voorafgaand aan elk nieuw internetonderzoek nog een nadere analyse zal moeten plaatsvinden, soms klein en soms groot, afhankelijk van het type internetonderzoek en de onderwerpen die geraakt zullen worden.

Wanneer de focus van de Belastingdienst ligt op het zorgvuldige proces voorafgaand aan het onderzoek, laat de Belastingdienst zien dat zij van te voren zo zorgvuldig mogelijk is omgegaan met de belangen van de betrokkenen. Mocht dan alsnog door een rechter geoordeeld worden dat de wet onvoldoende basis biedt voor dit type onderzoek, dan is dat een duidelijk signaal voor de politiek en wetgever om nieuwe wetgeving te faciliteren.

Wel is het raadzaam om op bepaalde punten proactief te handelen en als Belastingdienst zelf met een wetsvoorstel of beleid te komen met betrekking tot *transparantie, voorzienbaarheid* en de

⁸⁷ Commissie Koops, p. 159

⁸⁸ Bestaande uit in ieder geval vertegenwoordigers van de vaktechnische lijn (zowel lokaal als centraal), de DF&A en de technisch specialisten van team OSINT.

informatieplicht. Daarnaast zullen enkele onderwerpen, afhankelijk van de onderzoeksbehoefte, nader uitgediept moeten worden.

Bijlagen

17 factoren⁸⁹ voor de toets 'mate van inbreuk'

1) **Omvang en type** van de (over te nemen) gegevens:

- de hoeveelheid gegevens;
- de aard van de gegevens;
- de diversiteit van gegevens;
- deze factoren hangen mede samen met de mate waarin vooraf bekend is hoeveel en hoe de persoon zich manifesteert in publiek toegankelijke bronnen (in de praktijk: op het internet).

2) **Aard** van de bron:

- de aard van de locatie waarop de gegevens te vinden zijn; sommige bronnen zijn naar hun aard zeer openbaar (de krant), andere helemaal niet (de inhoud van privé-opslagruimte die toevallig niet beveiligd was);
- de menselijke bron van de gegevens (heeft de betrokkene deze zelf op internet geplaatst, of hebben anderen dat gedaan?);
- het doel waarmee de gegevens in eerste instantie zijn vergaard of gepubliceerd; is bijvoorbeeld expliciet of, gezien de context, impliciet duidelijk dat de gegevens op internet zijn geplaatst met het oog op brede verspreiding, of juist niet met het oog op kennisneming door een brede of onbepaalde kring;
- de plaats van de gegevens (welke privacyverwachting bestaat bij de locatie van de gegevens: staan ze direct zichtbaar op een platform met een breed publiek, of op een obscure webpagina?);
- de feitelijke bekendheid van de gegevens (zijn de gegevens in een brede groep verspreid? Als het gevoelige gegevens betreft, is dit de eerste openbaarmaking? Of zijn er (inmiddels) vele bronnen die er mededeling over hebben gedaan?)

3) **Wijze van zoeken:**

- de geavanceerdheid van het gebruikte technisch hulpmiddel (handmatig zoeken met een klassieke zoekmachine, of geautomatiseerd zoeken en combineren van gegevens, of geautomatiseerde veredeling van gegevens?);
- het doel van de zoekactie (gericht op het overnemen van enkele simpele gegevens, of breder);
- de manier van zoeken (persoonsgericht en beperkt, of niet gericht op specifieke personen en beperkt; tegenover: persoonsgericht en diep; niet gericht op specifieke personen maar diep);

⁸⁹ Bron: Commissie Koops, p. 16

- de specificiteit van de zoekvraag (wordt een algemene of heel specifieke vraag gesteld, wordt de zoekvraag op voorhand toegespitst aan de hand van reeds in een onderzoek bekende gegevens, en gaat het om “gesloten vragen” of om “open vragen”? Dit hangt samen met de manier van zoeken, maar is niet hetzelfde);
- de samenhang tussen de zoekvraag en de onderhavige norm (is de zoekvraag direct en specifiek gericht op deze norm, of breder?).

4) Het **gebruik** van gegevens en de mogelijke **impact** op de persoon:

- de mate waarin (door een crawler of inspecteur onderzochte) gegevens worden overgenomen en de selectiviteit die daarbij wordt gehanteerd (worden gegevens alleen beperkt en gericht overgenomen in systemen, of is er juist sprake van een brede en weinig selectieve overneming van wat is aangetroffen?);
- de in het onderzoek reeds bekende informatie (hoeveel steentjes zal de zoekactie toevoegen aan het reeds bestaande beeld?);
- de combinatie van gegevens uit verschillende bronnen (bijvoorbeeld het combineren van internetzoekresultaten met op de markt ingekochte bestanden met persoonsgegevens of bestaande bestanden).

Vragenlijst protocol

1. Ben je als medewerker bevoegd om dit type internetonderzoek te doen?
2. Wat voor type internetonderzoek is het?
3. Wat is het onderzoeksdoel?
4. Wat is de aanleiding van het onderzoek?
5. Welke gegevens ga je vermoedelijk aantreffen?

Betreft het informatie over een persoon? (kans is 99% : zodra je wat intypt in Google is er bijna altijd sprake van 'verwerking van persoonsgegevens' volgens de wet.)

6. Wat wil je aantonen/bewijzen? Is het noodzakelijk voor het doel wat je wil bereiken om deze zoekactie te verrichten? Of kan het ook op een andere manier (bijvoorbeeld via de belastingplichtige(n) zelf)

NB. Let op, het doel moet altijd te koppelen zijn aan de wettelijke taak van de Belastingdienst, zoals omschreven in de wet ...

7. Wat voor type gegevens betreft het?

NB. Let op. Gegevens over ras, etnische afkomst, politieke opvattingen, religieuze overtuiging, gezondheid, geaardheid etc zijn verboden⁹⁰ om te verwerken. Dus ook foto's. Maar art 25 UAVG (a) geeft ruimte om een betrokkene te identificeren, voor zover dat onvermijdelijk en noodzakelijk is.

8. Waar ga je de gegevens aantreffen? Zijn de gegevens bedoeld om openbaar te zijn?
9. Hoe vindt de wijze van vergaren van informatie plaats?
10. Betreft het software van de belastingdienst zelf? Of van een externe partij?

NB. Let op. De aanbieder van de zoektechniek slaat mogelijk de data ook extern op. Zoek dit eerst uit.

11. Hoe lang ga je gegevens verzamelen?
12. Wat ga je doen met de gegevens? Hoe en waar worden de gegevens vastgelegd?
13. Hoe lang vindt de opslag van de gegevens plaats?
14. Ga je de gevonden gegevens nog combineren met andere datasets?
15. Ben je van plan om een compleet beeld van iemand in kaart te brengen?

⁹⁰ Uitzonderingen zijn mogelijk.

NB. Zodra je 'profielen' gaat opstellen, dan is er mogelijk sprake van 'stelselmatigheid' en dient een strengere toets plaats te vinden.

16. Ben je van plan om met enige regelmaat gegevens te zoeken?

NB. Let op, het kan zijn dat dit onder 'stelselmatige observatie' valt.

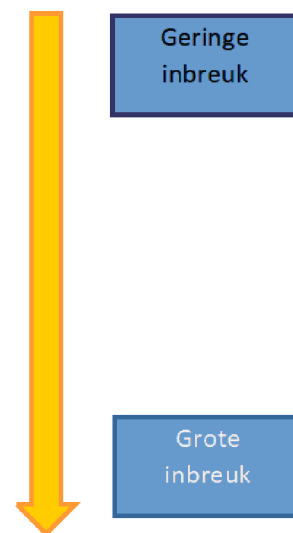
17. Wat is de hoeveelheid van de persoonsgegevens die je gaat aantreffen?

18. Ben je wel/niet van plan om te laten weten aan de belastingplichtigen dat je persoonsgegevens van hen hebt geraadpleegd? Zo nee, dan dien je uit te leggen waarom niet. Deze uitleg dient te voldoen aan de eisen van artikel 41 UAVG!

Mogelijke zoekhandelingen

Onderstaande handelingen⁹¹ zijn mogelijke handelingen die kunnen plaatsvinden in een zoekactie via OSINT. Deze handelingen zijn zo gecategoriseerd dat ze oplopen van kans op een kleine inbreuk naar kans op mogelijk een grote inbreuk. Het betreft een glijdende schaal, waarbij ook de vragen uit de vragenlijst hierboven van belang kunnen zijn voor de beoordeling hoe groot het privacyrisico uiteindelijk is.

- Klikken op één URL n.a.v. een vermoeden
- Aanwezig zijn, rondkijken, je oriënteren
- Profielen lezen en vastleggen, links openen en vastleggen
- Berichten lezen en vastleggen, links openen en vastleggen
- In kaart brengen woonomgeving, vastleggen woonomgeving
- In kaart brengen netwerk, familie, vrienden, volgers, contacten
- Actief deelnemen aan gesprekken
- Ongericht en onbeperkt zoeken op diverse zoekwoorden op WWW of TOR



⁹¹ Idealiter wordt dit in een later stadium in een matrix gegoten. Want wellicht klikt de inspecteur op één URL (=geringe inbreuk), maar ziet zij (in theorie) daarna een berg aan bijzondere persoonsgegevens. Dan is alsnog sprake van een grote inbreuk, maar wellicht toegestaan gezien het 'vergrijp'.

WP29 – Overzicht Verwerkingen met ‘waarschijnlijk een hoog risico’⁹²

1) Evaluatie of scoretoekenning, met inbegrip van profielbepaling en voorspelling, met name van "kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene" (overwegingen 71 en 91). Voorbeelden hiervan zijn een financiële instelling die haar klanten screent op basis van een kredietreferentiedatabank, een databank die wordt ingezet in de strijd tegen witwaspraktijken en terrorismefinanciering, of een fraudedatabank, of een biotechnologiebedrijf dat rechtstreeks aan consumenten genetische tests aanbiedt om ziekte-/gezondheidsrisico's te beoordelen en te voorspellen, of een bedrijf dat gedrags- of marketingprofielen opstelt op basis van het gebruik van of de navigatie op zijn website.

2) Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg: verwerking die gericht is op het nemen van beslissingen met betrekking tot betrokkenen "waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden" of die "de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen" (artikel 35, lid 3, onder a)). De verwerking kan bijvoorbeeld leiden tot uitsluiting of discriminatie van natuurlijke personen. Verwerking met weinig of geen gevolg voor natuurlijke personen voldoet niet aan dit specifieke criterium. Verdere uitleg over deze begrippen wordt verstrekt in de komende WP29-richtsnoeren inzake profielbepaling.

3) Stelselmatige monitoring: verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of "stelselmatige [...] monitoring van openbaar toegankelijke ruimten" (artikel 35, lid 3, onder c)). Dit type monitoring is een criterium omdat de persoonsgegevens kunnen worden verzameld in omstandigheden waarin de betrokkenen mogelijk niet weten wie hun gegevens verzamelt en hoe die gegevens zullen worden gebruikt. Bovendien kan het voor natuurlijke personen onmogelijk zijn om te voorkomen dat ze aan een dergelijke verwerking in een openbare (of openbaar toegankelijke) ruimte worden onderworpen.

4) Gevoelige gegevens of gegevens van zeer persoonlijke aard: dit omvat speciale categorieën persoonsgegevens zoals omschreven in artikel 9 (bijvoorbeeld informatie over de politieke opvattingen van personen), evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten zoals omschreven in artikel 10. Een voorbeeld hiervan is een algemeen ziekenhuis dat medische dossiers van patiënten bewaart of een privédetective die gegevens van overtreeders bewaart. Naast deze bepalingen van de AVG kunnen sommige gegevenscategorieën worden beschouwd als categorieën die het mogelijke risico voor de rechten en vrijheden van natuurlijke personen verhogen. Deze persoonsgegevens worden als gevoelig (zoals deze term algemeen wordt begrepen) beschouwd omdat ze verband houden met huishoudelijke en privéactiviteiten (zoals elektronische communicatie waarvan de vertrouwelijkheid moet worden beschermd) of omdat ze de uitoefening van een grondrecht beïnvloeden (zoals locatiegegevens waarvan de verzameling de vrijheid van verkeer in vraag stelt) of omdat de schending ervan duidelijk gevolgen heeft voor het dagelijkse leven van de betrokkene (zoals financiële gegevens die kunnen worden gebruikt voor betalingsfraude). In dit opzicht kan het relevant zijn of de gegevens al openbaar zijn gemaakt door de betrokkene of door derden. Het feit dat persoonsgegevens openbaar zijn, kan als een factor worden beschouwd bij de beoordeling of de gegevens naar verwachting

⁹² Bron: GROEP GEGEVENSBESCHERMING ARTIKEL 29, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, p.10 e.v.

verder zullen worden gebruikt voor bepaalde doeleinden. Dit criterium kan ook betrekking hebben op gegevens zoals persoonlijke documenten, e-mails, dagboeken, notities uit e-readers met notitiefuncties, en zeer persoonlijke informatie in "life-logging"-applicaties.

5) Op grote schaal verwerkte gegevens: in de AVG wordt niet gedefinieerd wat grootschalig is, al worden in overweging 91 enkele richtsnoeren gegeven. In ieder geval raadt de WP29 aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd:

- a. het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
- b. het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
- c. de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit;
- d. de geografische omvang van de verwerkingsactiviteit.

6) Matching of samenvoeging van datasets, bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zou overschrijden.

7) Gegevens met betrekking tot kwetsbare betrokkenen (overweging 75): de verwerking van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Kwetsbare betrokkenen kunnen kinderen omvatten (kinderen kunnen worden geacht niet in staat te zijn om bewust en bedachtzaam in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens), werknemers, kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven (geesteszieken, asielzoekers, bejaarden, patiënten enz.), en in elk geval waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.

8) Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen, zoals het combineren van het gebruik van vingerafdrukken en gezichtsherkenning voor een betere fysieke toegangscontrole enz. In de AVG wordt duidelijk gesteld (artikel 35, lid 1, en de overwegingen 89 en 91) dat het gebruik van een nieuwe technologie, gedefinieerd "conform het bereikte niveau van technologische kennis" (overweging 91), aanleiding kan geven tot de noodzaak om een gegevensbeschermingseffectbeoordeling uit te voeren. Dit komt omdat het gebruik van dergelijke technologie nieuwe vormen van gegevensverzameling en -gebruik kan inhouden, mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen. De persoonlijke en sociale gevolgen van het gebruik van een nieuwe technologie kunnen immers onbekend zijn. Een gegevensbeschermingseffectbeoordeling zal de verwerkingsverantwoordelijke helpen om dergelijke risico's te begrijpen en aan te pakken. Bijvoorbeeld bepaalde toepassingen van het "internet der dingen" kunnen een aanzienlijk effect hebben op het dagelijkse leven en de privacy van natuurlijke personen; en bijgevolg een gegevensbeschermingseffectbeoordeling vereisen.

9) Wanneer als gevolg van de verwerking zelf "betrokkenen [...]" een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst" (artikel 22 en overweging 91). Dit omvat verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan, te wijzigen of te

weigeren. Een voorbeeld hiervan is een bank die zijn klanten screent op basis van een databank met kredietreferenties om te beslissen of ze al dan niet een lening aangeboden krijgen.