Dit artikel wordt u aangeboden door Juridisch up to Date

Juridisch up to Date is hét vakblad voor juristen. Hierin vindt u een breed aanbod van korte maar diepgaande artikelen, voorzien van deskundig en praktijkgericht commentaar. In Juridisch up to Date worden alle rechtsgebieden belicht, maar de focus ligt op ondernemingsrecht in nationaal maar ook zeker Europees en internationaal verband. Juridisch up to Date is daarmee een onmisbare nieuwsbron voor juristen die in korte tijd volledig op de hoogte willen zijn van wat zich afspeelt in het brede juridische vakgebied.

Dit kunt u verwachten van Juridisch up to Date:

- tweewekelijks vakblad - digitaal en/of op papier
- toegang tot online database
- laatste vier vakbladen offline beschikbaar op tablet.

Kijk voor meer informatie of een (proef)abonnement op
https://www.futd.nl/vakblad/juridisch-up-to-date/abonneren/

JURIDISCH UP TO DATE FUTD
Vakblad voor de juridische praktijk

ID JutD 2018-0151
Datum 20181214
Rubriek Eu, mededinging en marktordening

De nieuwe 'Werkwijze AFM inzien en kopiëren van digitale gegevens' en de praktijk van digitaal onderzoek door toezichthouders

Auteur(s)
Karen Berg & Piet-Hein Eijssen, advocaten bij Bird & Bird LLP, Den Haag. *De auteurs danken Lianne Sieben voor de voorbereiding bij de totstandkoming van dit artikel.*

Inleiding

Met de toenemende digitalisering is de bewijsgaring door toezichthouders als de Autoriteit Consument & Markt ("**ACM**") en de Autoriteit Financiële Markten ("**AFM**") in het kader van hun toezicht op de naleving steeds meer gericht op de verzameling van digitale gegevens. Een bedrijfsbezoek door toezichthouders (of inval) is daarmee veelomvattender en ingrijpender geworden voor ondernemingen: digitale gegevensdragers bevatten immers veel meer informatie dan analoge gegevensdragers, digitale gegevens zijn meestal relatief eenvoudig toegankelijk en doorzoekbaar en digitale gegevens zijn makkelijk te kopiëren en dus mee te nemen door een toezichthouder. Mede in het licht van het toenemende belang en de impact van digitaal onderzoek, is het cruciaal dat er voldoende waarborgen bestaan rond digitaal onderzoek door toezichthouders.

Verschillende toezichthouders hebben beleidsregels opgesteld met richtlijnen voor digitaal onderzoek. De ACM hanteert, in navolging van haar rechtsvoorganger Nederlandse Mededingingsautoriteit ("**NMa**"), ook een digitale werkwijze, namelijk de 'ACM Werkwijze voor onderzoek in digitale gegevens 2014' ("**ACM Werkwijze**").[1] Recent heeft de AFM haar 'Werkwijze AFM inzien en kopiëren van digitale gegevens' ("**AFM Werkwijze**") herzien.[2]

In dit artikel gaan we in op de praktijk rond bedrijfsbezoeken en enkele verschillen tussen de ACM en de AFM Werkwijze en staan we stil bij de vraag of beide werkwijzen de grenzen van de reikwijdte van het onderzoek door deze toezichthouders voldoende waarborgen.

De praktijk van een bedrijfsbezoek

Op grond van artikelen 5:15 en 5:17 Algemene wet bestuursrecht ("**Awb**") zijn toezichthouders bevoegd bij ondernemingen binnen te treden en daarbij zakelijke gegevens te vorderen en te kopiëren. Iedereen is in beginsel verplicht mee te werken aan evenredige vorderingen door een bevoegde toezichthouder (vergelijk artikel 5:20 Awb). Komt de toezichthouder langs voor een bedrijfsbezoek, dan mag een onderneming dat dus niet weigeren. Toezichthouders zijn bij de uitoefening van hun

toezichtbevoegdheden uiteraard wel onder meer gebonden aan de algemene beginselen van behoorlijk bestuur en het Europees Verdrag van de Rechten van de Mens ("**EVRM**").

Een bedrijfsbezoek betekent in de praktijk dat een team toezichtambtenaren zich meldt bij het kantoor van een onderneming. Soms gebeurt dit met vooraankondiging, maar vaker zonder. De toezichtambtenaren informeren de onderneming over de doelomschrijving van het onderzoek en overhandigen daarbij meestal een document waarin de materiële en temporele afbakening en de juridische grondslag van het bedrijfsbezoek wordt beschreven en - indien van toepassing - van welke personen of functionarissen betrokkenheid wordt vermoed bij het doel/voorwerp van onderzoek. De doelomschrijving biedt daarmee het kader waarbinnen de toezichtambtenaren bij de uitoefening van hun (ingrijpende) bevoegdheden tijdens het bedrijfsbezoek moeten blijven. En voor de onderneming is het een leidraad die houvast biedt hoever haar medewerkingsplicht reikt.

Naast het verhoren van leidinggevenden en/of werknemers van de onderneming en het onderzoeken van werkplekken tijdens een bedrijfsbezoek, vormt het al genoemde digitaal onderzoek een steeds belangrijker onderdeel. De toezichthouder kan ter plekke een selectie maken van de (digitale) data die binnen de reikwijdte van het onderzoek vallen en deze vorderen in het belang van het onderzoek. In de praktijk worden soms ook grote delen van alle data op de server van een onderneming veiliggesteld (dus zonder selectie), waarbij niet zelden de digitale dossiers, e-mailboxen, laptops en smartphones van mogelijk betrokken personen integraal worden gekopieerd.

Tot zover de meer praktische kant van het bedrijfsbezoek zelf.

De ACM en de AFM Werkwijze en digitaal onderzoek

De ACM en de AFM Werkwijze beschrijven (onder andere) hoe de ACM, respectievelijk AFM vanaf dat moment te werk gaan. We bespreken hierna enkele verschillen tussen beide werkwijzen.[3] Daarbij is van belang om drie selecties te onderscheiden om van de door de toezichthouder veiliggestelde digitale dataset te komen tot een zogenoemde onderzoeksdataset die de basis vormt voor het verdere onderzoek. Data die - al dan niet op verzoek van de onderzochte onderneming - door toezichthouders uit de veiliggestelde dataset moeten worden gefilterd zijn: (a) geprivilegieerde data (gegevens die vallen onder het verschoningsrecht van een advocaat), (b) niet-zakelijke (lees: privé) data en (c) data die op grond van de doelomschrijving van het onderzoek buiten de reikwijdte van het onderzoek vallen. Deze laatste selectie maken toezichthouders doorgaans door het (elektronisch) filteren van de veiliggestelde data aan de hand van zoektermen die op basis van de doelomschrijving zijn geformuleerd.

Een opmerkelijk algemeen verschil tussen de beide werkwijzen is dat de AFM Werkwijze de onderneming eerst in de gelegenheid stelt de digitale data te schonen van geprivilegieerde en niet-zakelijke gegevens en dat daarna pas de digitale data worden geselecteerd die binnen de reikwijdte van het onderzoek valt.[4] De ACM Werkwijze gaat juist van een omgekeerde volgorde uit, waarbij eerst zoektermen op de tijdens het bedrijfsbezoek veiliggestelde dataset worden toegepast en daarna wordt de onderzochte onderneming in de gelegenheid gesteld om uit deze (kleinere) dataset geprivilegieerde en niet-zakelijke gegevens te (laten) verwijderen.[5] Het is de vraag of de AFM Werkwijze hiermee niet een te grote (en wellicht onnodige) last voor onderzochte onderneming (en voor de AFM zelf) met zich meebrengt. Immers, de door de AFM onderzochte onderneming zal in de praktijk een veel grotere dataset moeten doorzoeken op geprivilegieerde en niet-zakelijke data dan een onderneming die de ACM op bezoek heeft gehad. Dit verschil kan potentieel zeer omvangrijk zijn. Vooral wanneer wordt bedacht dat een door toezichthouders veiliggestelde dataset niet zelden bestaat uit honderdduizenden individuele documenten en de AFM Werkwijze vereist dat voor

uitsluiting van de onderzoeksdataset per document moet worden onderbouwd waarom een document een geprivilegieerd of niet-zakelijk karakter draagt.[6]

Gerelateerd aan dit praktische bezwaar is er een tweede opvallend verschil tussen de werkwijzen. De AFM Werkwijze bepaalt dat de onderneming uiterlijk binnen 10 werkdagen na ontvangst van een overzicht van de bij het bedrijfsbezoek veiliggestelde dataset een verzoek tot opschoning op geprivilegieerde en niet-zakelijke gegevens moet indienen.[7] De huidige ACM Werkwijze bevat op dit punt geen termijnen, in tegenstelling tot de (oude) daarvoor gehanteerde digitale werkwijze waarin ook een termijn van 10 werkdagen gold [8]. De ACM heeft juist besloten deze termijn los te laten, omdat die in de praktijk niet werkbaar bleek te zijn vanwege de (meestal) grote omvang van datasets. Het is waarschijnlijk dat de AFM Werkwijze op dit punt tot dezelfde praktische bezwaren leidt en dat ondernemingen (of hun advocaten) standaard om uitstel van deze termijn zullen (moeten) verzoeken.

Als derde verschil bevat de AFM Werkwijze wel de waarborg dat alleen toezichtsambtenaren die niet betrokken zijn bij de inhoudelijke uitvoering van het onderzoek de opschoning van de veiliggestelde dataset van zowel geprivilegieerde als niet-zakelijke documenten verrichten. Dat waarborgt de ACM Werkwijze ook voor de opschoning van de dataset van geprivilegieerde documenten. Echter, ACM toezichtsambtenaren die inhoudelijk betrokken zijn bij het onderzoek beoordelen de door de onderneming aangedragen claims ten aanzien van documenten die vanwege hun niet-zakelijke karakter van de onderzoeksdataset zouden moeten worden uitgesloten.[9]

Wat bij beide werkwijzen hetzelfde is, is dat de selectie van de (van geprivilegieerde en niet zakelijke documenten) geschoonde dataset naar de onderzoeksdataset wordt gemaakt op basis van zoektermen die worden aangedragen door een toezichthoudend ambtenaar die betrokken is bij het onderzoek. Juist dit selectieproces en dan vooral de vraag in hoeverre digitale data die volgens de onderzochte onderneming inhoudelijk buiten de reikwijdte van het onderzoek moeten vallen, maar die toch een treffer opleveren op een geformuleerde zoekterm en daardoor onderdeel zijn van de uiteindelijke onderzoeksdataset, waren de afgelopen twee jaar onderwerp van discussie in een drietal kortgedingprocedures.[10] Dit is een zeer relevante vraag voor ondernemingen die voorwerp zijn (of kunnen worden) van digitaal onderzoek door toezichthouders, omdat gegevens die toezichthouders in het kader van hun onderzoek hebben verkregen voor zover noodzakelijk ook mogen gebruiken bij de uitvoering van andere (onderzoeks)taken, en deze gegevens tevens mogen delen met andere - binnenlandse en buitenlandse - toezichthouders.[11] Wat betreft het mogelijke interne gebruik door AFM en ACM van verkregen gegevens bij de uitvoering van andere (onderzoeks)taken, dient te worden bedacht dat de onderneming naast het lopende digitale onderzoek mogelijk ook voorwerp van (parallel) toezicht kan zijn door dezelfde toezichthouder. Naast bijvoorbeeld een onderzoek door de ACM naar aanleiding van vermoedens van een overtreding van de Mededingingswet, houdt de ACM ook toezicht op ondernemingen op grond van sectorspecifieke marktregulering en/of regelgeving op het gebied van consumentenbescherming. Ook in verhouding tot de AFM kan de onderneming in een parallelle toezichtrelatie staan en is een zeer relevante vraag welke informatie de toezichthouder in welk toezichttraject kan gebruiken.

Een volledige analyse van de drie met deze materie samenhangende kort gedinguitspraken gaat het bestek van dit artikel te buiten, maar wij belichten hieronder de kern van de discussies.

Waarborgen van de grenzen van de reikwijdte van het onderzoek

Een belangrijke conclusie van de rechter in deze uitspraken is dat de ACM Werkwijze, in het licht van de *Vinci*-uitspraak van het Europees Hof voor de Rechten van de Mens,[12] op

in ieder geval één aspect niet voldoet aan de eisen die voortvloeien uit de rechten van de verdediging. Volgens de rechter dient een toezichthouder open te staan voor argumenten van een onderneming waarom bepaalde concrete documenten buiten de reikwijdte van de doelomschrijving van een onderzoek zouden vallen (ook wanneer deze beantwoorden aan de op zichzelf onbetwiste zoektermen) en dient de onderneming de mogelijkheid te hebben om deze bezwaren ter toetsing aan de rechter voor te leggen.[13] De toezichthouder kan dergelijke argumenten niet enkel afwijzen met als argument dat deze documenten een treffer hebben op een zoekterm, die is geformuleerd op basis van de doelomschrijving van het onderzoek. Volgens de rechter is een toezichthouder dus verplicht om inhoudelijk in te gaan op door de onderneming aangedragen argumenten waarom een specifiek document niet binnen de reikwijdte van een onderzoek valt, ook al was er een treffer op de gedefinieerde zoektermen. In de consultatie die voorafging aan de inwerkingtreding van de ACM Werkwijze werd al gewezen op het ontbreken van een procedure om 'bijvangst' die buiten de reikwijdte van het onderzoek valt, uit te sluiten van het onderzoek, terwijl een dergelijke procedure wel bestond onder de eerdere digitale werkwijze van de toenmalige Nederlandse Mededingingsautoriteit uit 2010.[14]

In de literatuur is wel beargumenteerd dat de ACM Werkwijze naar aanleiding van deze nationale en de Europeesrechtelijke rechtspraak zou moeten worden aangepast.[15] Het valt te betwijfelen of ook de herziene AFM Werkwijze op dit punt wel aan de rechtspraak voldoet. Daarin wordt namelijk slechts opgemerkt dat bij het samenstellen van de onderzoekdataset zoektermen worden gebruikt die zijn gebaseerd op het doel van het onderzoek en dat namens de onderzochte onderneming een verzoek kan worden gedaan om een toelichting op de door de AFM gehanteerde zoekstrategie.[16] In de praktijk zijn toezichthouders vaak wel bereid om met de (advocaat van de) onderneming in gesprek te gaan over de formulering van zoektermen en documenten die buiten de reikwijdte van de doelomschrijving van een onderzoek vallen en daarom moeten worden uitgesloten van het onderzoek,[17] maar een procedure en transparantie op dit punt ontbreken in beide werkwijzen. Bovendien heeft de toezichthouder in alle gevallen dan al kennis genomen van de betreffende documenten, ook als die evident buiten de doelomschrijving vallen en dus nooit in de onderzoeksdataset hadden mogen worden opgenomen.

In de literatuur is als praktische oplossing voorgesteld hiervoor de procedure te gebruiken die is geregeld voor het al dan niet moeten uitsluiten van documenten die onder het verschoningsrecht van een advocaat vallen.[18] Maar vooralsnog wijst ACM dit af en ook de AFM heeft deze suggestie in ieder geval niet ter harte genomen, want deze ontbreekt in de (herziene) AFM Werkwijze.

In een andere belangrijke uitspraak van 10 oktober 2018 oordeelde de kort gedingrechter onder meer dat het niet (volledig) volgen van de ACM Werkwijze door de ACM tot gevolg had dat daardoor verkregen veiliggestelde digitale data gedeeltelijk buiten het ACM onderzoek moesten blijven. Anders, aldus de kort gedingrechter: *"zou dat immers betekenen dat de in de Digitale Werkwijze neergelegde waarborgen tegen de ingrijpende bevoegdheden van gedaagde [ACM] een lege huls zouden zijn"*.[19] Naast de hierboven al eerder genoemde conclusie dat de ACM en de AFM Werkwijze als gevolg van recente rechtspraak mogelijk moeten worden aangepast waar het gaat om de wijze waarop de ACM en AFM omgaan met gegevens die al dan niet buiten de reikwijdte van een onderzoek vallen, blijkt uit deze laatste uitspraak bovendien dat het niet volgen van een digitale werkwijze tot resultaat heeft dat tijdens een bedrijfsbezoek door toezichthouders veiliggestelde data buiten het onderzoek moeten blijven.

Conclusie

Het is positief dat toezichthouders zoals de ACM en AFM met het hanteren van werkwijzen streven naar enige mate van transparantie over de wijze waarop zij digitaal onderzoek bij ondernemingen verrichten, al zou de transparantie op diverse punten verbeterd kunnen worden. Zo lijken de recente kortgedingprocedures in ieder geval met zich mee te brengen dat zowel de ACM als de AFM in hun digitale werkwijzen nadere richtlijnen en procedures moeten opnemen ten aanzien van het uitsluiten van documenten die niet binnen de reikwijdte van een onderzoek vallen. Voldoende waarborgen bij bedrijfsbezoeken zijn van groot belang, aangezien deze onderzoeksbevoegdheden zeer ingrijpend zijn voor de onderzochte ondernemingen. Bovendien kunnen toezichthouders digitale data waarvan is vastgesteld dat deze binnen de reikwijdte van een onderzoek vallen, gebruiken bij de uitvoering van andere (onderzoeks)taken en delen met andere binnenlandse en buitenlandse toezichthouders. Dat maakt meteen de noodzaak duidelijk om te voorkomen dat inzage wordt verkregen door de toezichthouder in documenten die buiten de reikwijdte van het onderzoek vallen.

Het opvolgen en updaten van werkwijzen voor digitaal onderzoek is dan ook cruciaal en het is bemoedigend dat een kort gedingrechter ook onlangs consequenties heeft verbonden aan het niet opvolgen door een toezichthouder van een digitale werkwijze. Hoe dan ook blijkt uit de reeks recente kortgedingprocedures, mede gebaseerd op EHRM-jurisprudentie, dat toezichthouders zich aan bepaalde minimale procedurele vereisten moeten houden bij de vaststelling of een document wel of niet aan een onderzoeksdataset kan worden toegevoegd. Het verdient dan ook aanbeveling dat de ACM en de AFM Werkwijze hiermee in overeenstemming worden gebracht.

Noten

1. ACM Werkwijze voor onderzoek in digitale gegevens 2014, Stcr. 11 februari 2014, 3993.
2. Werkwijze AFM inzien en kopiëren van digitale gegevens, Stcr. 2 november 2018, 62207.
3. Er valt een veel uitgebreidere analyse te maken dan we in dit artikel doen; we beperken ons tot enkele - in onze ogen - belangrijke verschillen.
4. Artikelen 2-5 AFM Werkwijze.
5. Zie de schematische weergave van de ACM werkwijze op pagina 6 van de ACM Werkwijze.
6. Zie artikel 2 leden 4 en 6 AFM Werkwijze.
7. Artikel 2 lid 7 AFM Werkwijze.
8. Zie artikel 6 en 7 van de Werkwijze NMa analoog en digitaal rechercheren 2010.
9. Zie artikel 2.3 lid 2 ACM Werkwijze.
10. Voorzieningenrechter rechtbank Den Haag 12 juli 2017, ECLI:NL:RBDHA:2017:7968; Voorzieningenrechter rechtbank Den Haag 22 november 2017, ECLI:NL:RBDHA:2017:14150; Voorzieningenrechter rechtbank Den Haag 10 oktober 2018, ECLI:NL:RBDHA:2018:12722.
11. Zie in geval van de ACM artikel 7 van de Instellingswet Autoriteit Consument & Markt en in geval van de AFM artikel 1:90 Wet op het financieel toezicht.
12. EHRM 2 april 2015, 63629/10 en 60567/10 (Affaire Vinci Construction et GTM Génie Civil et Services/Frankrijk).
13. Voorzieningenrechter rechtbank Den Haag 12 juli 2017, ECLI:NL:RBDHA:2017:7968, r.o. 4.12.
14. Zie de opmerkingen namens de Nederlandse Vereniging voor Mededingingsrecht in Reacties Consultatie Werkwijzen ACM, zie www.acm.nl/nl/download/bijlage/?id=11745, p. 27.
15. Zie bijvoorbeeld H.M.H. Speyart, 'Vzr Rb Den Haag 12 juli 2017: binnen/buiten de reikwijdte discussie en effectieve rechtsbescherming na Vinci', Mededingingsrecht in de Praktijk, 2017 nummer 5.
16. Zie artikel 5 lid 2 en 3 AFM Werkwijze.

17. Zie bijvoorbeeld Voorzieningenrechter rechtbank Den Haag 12 juli 2017, ECLI:NL:RBDHA:2017:7968, r.o. 2.13.
18. F. ten Have, 'Digitale bewijsvergaring door de ACM: herleving van het 'buiten de reikwijdte'-argument', Markt & Mededinging, 2017 nummer 4.
19. Voorzieningenrechter rechtbank Den Haag 10 oktober 2018, ECLI:NL:RBDHA:2018:12722, r.o. 4.14.