Mr. G.P. Roth & mr. L.B.G. Hillen[1]

Digitaal onderzoek door de AFM

Hoe gaat dat in zijn werk, mag dat zomaar en hoe adequaat is de rechtsbescherming?

Ondernemingsrecht 2020/141

De financiële sector digitaliseert en zo ook de AFM bij de uitoefening van haar onderzoeksbevoegdheden. Uit het oogpunt van rechtsbescherming levert dat allerlei interessante vragen op. In deze bijdrage gaat het om één specifieke en veelgebruikte onderzoeksbevoegdheid: de inzagevordering. Onderzocht wordt hoe de AFM deze bevoegdheid in de praktijk inzet tijdens een al dan niet aangekondigd bezoek aan een financiële instelling. Daarbij wordt specifiek ingegaan op het vorderen van inzage in digitale gegevens waarover de financiële instelling en/of haar beleidsbepalers beschikken. Vastgesteld wordt dat waar de AFM zich voorheen vooral op e-mailonderzoek richtte, zij inmiddels ook steeds vaker andere digitale gegevensbronnen in het vizier heeft, waaronder mobiele telefoons.

Bij afwezigheid van een specifieke wettelijke regeling voor digitaal onderzoek hanteert de AFM sinds een aantal jaren een eigen Werkwijze. Die Werkwijze houdt een beschrijving in van de procedure die zij bij digitaal onderzoek ter plaatse volgt en voorziet in enige waarborgen voor financiële instellingen die met een inzagevordering worden geconfronteerd. Indachtig de wettelijke grenzen waar de AFM bij de inzet van een inzagevordering aan is gebonden, wordt een aantal in de praktijk opkomende rechtsvragen besproken en wordt op kritische wijze stilgestaan bij de aan financiële instellingen en hun beleidsbepalers toekomende rechtsbescherming.

1. Inleiding

Onder toezicht staande financiële instellingen en hun beleidsbepalers worden in toenemende mate geconfronteerd met onderzoeken ter plaatse waarbij medewerkers van de Autoriteit Financiële Markten (AFM) de op gegevensdragers – zoals laptops, usb-sticks en mobiele telefoons – opgeslagen digitale informatie kopiëren en inzien.[2] Deze praktijk heeft vaak ingrijpende gevolgen. De vraag of de AFM dit zomaar mag en welke mate van rechtsbescherming er bestaat wordt dan ook steeds relevanter.

In deze bijdrage wordt eerst de praktijk van digitale onderzoeken door de AFM[3] bij financiële instellingen ter plaatse[4] toegelicht. Vervolgens worden de grenzen verkend die de AFM bij de uitoefening van haar bevoegdheden in dit kader in acht moet nemen en worden een aantal rechtsvragen besproken die daarbij, met name vanuit het perspectief van rechtsbescherming, opkomen. Tot slot wordt ingegaan op de mogelijkheden voor instellingen om de rechtmatigheid van digitale onderzoeken ter discussie te stellen. Bijzondere aandacht wordt besteed aan onderzoek naar op mobiele telefoons vastgelegde gegevens, nu dit type gegevensdrager steeds vaker in het vizier van de toezichthouder lijkt te komen.

2. Digitaal onderzoek AFM in de praktijk

2.1 *Algemeen*

In een steeds verder digitaliserende financiële sector is het niet verwonderlijk dat de AFM steeds vaker onderzoek doet naar digitale gegevens. Daarvoor moet ze ui-

1 Guido Roth en Laurens Hillen zijn beiden advocaat te Amsterdam. Omwille van de transparantie: eerstgenoemde auteur trad in een aantal van de in deze bijdrage besproken beroeps- en voorlopige voorzieningenprocedures op als gemachtigde van eiser respectievelijk verzoeker. Guido Roth is tevens redacteur van dit tijdschrift.

2 In het kader van de coronacrisis meldde de AFM op 22 mei 2020 op haar website per 1 juni 2020 weer te zullen starten met onderzoeken ter plaatse, mits redelijkerwijs noodzakelijk en er geen minder belastende mogelijkheden zijn om het onderzoek te verrichten.

3 De Nederlandsche Bank (DNB) lijkt minder vaak digitaal onderzoek te verrichten, hoewel ze te dezer zake in het verleden wel samen met de AFM is opgetrokken en sinds 22 juni 2020 net als de AFM over een 'Werkwijze inzien en kopiëren van digitale gegevens' beschikt. Deze werkwijze is overigens vrijwel identiek aan die van de AFM. De in deze bijdrage vervatte analyse over digitaal onderzoek door de AFM is dan ook grotendeels van overeenkomstige toepassing op digitaal onderzoek door DNB.

4 Er wordt dus niet ingegaan op digitaal onderzoek door de AFM 'op afstand' waarbij ze per brief of e-mail digitale stukken bij de financiële instelling opvraagt. Evenmin wordt ingegaan op digitaal onderzoek door de AFM ter plaatse van aan de financiële instelling gelieerde derden, zoals de accountant of beleidsbepalers. Wel zij hier opgemerkt dat de AFM op grond van art. 5:15 lid 1 Awb niet een woning van (bijvoorbeeld) een beleidsbepaler mag betreden zonder toestemming van de beleidsbepaler, hetgeen overigens weer niet betekent dat digitale gegevens in een woning ook daadwerkelijk veilig zijn, zie Rb. Rotterdam 5 september 2012, ECLI:NL:RBROT:2012:BX6988, r.o. 6.2.

teraard wel eerst de hand op digitale gegevens weten te leggen. Daartoe kan de AFM de financiële instelling fysiek bezoeken. Dergelijke bezoeken kan ze aankondigen, maar vinden in toenemende mate onaangekondigd plaats.

Voorheen bestonden de toezichthouders[5] van de AFM die dergelijke bezoeken afleggen vooral uit juristen en hoogstens een enkele IT-medewerker. Tegenwoordig zijn juist vooral IT-specialisten aanwezig om digitale gegevens veilig te stellen. Alle toezichthouders dienen ter plaatse desgevraagd hun legitimatiebewijs te tonen.[6] Zij zullen de instelling doorgaans een onderzoeksbrief uitreiken met daarin een toelichting op het onderzoek. Wordt die toelichting niet verstrekt, dan doet de instelling er, gelet op de hierna te bespreken vraag of het onderzoek de evenredigheidstoets doorstaat, goed aan te verlangen dat dit alsnog gebeurt.

Toezichthouders van de AFM zijn over het algemeen desgevraagd bereid te wachten met het onderzoek totdat ook de advocaat/gemachtigde van de instelling ter plaatse is, mits dit binnen een redelijke termijn valt te realiseren.

2.2 *De Werkwijze van de AFM*

Het digitale onderzoek van de AFM zag tot kortgeleden vooral op e-mails. Inmiddels worden de pijlen ook gericht op andere digitale bronnen, waaronder gegevens op mobiele telefoons. Op een telefoon zullen weer andere gegevens opgeslagen zijn dan in een e-mailbox, zoals een contactenlijst, *WhatsApp*-berichten, sms-berichten, foto's, video's en locatiegegevens. We hebben in de praktijk kunnen vaststellen dat niet alleen zakelijke toestellen worden onderworpen aan onderzoek, maar ook privételefoons van de beleidsbepalers.

De Algemene wet bestuursrecht (Awb) voorziet niet in een specifieke regeling voor digitaal onderzoek. Wel hanteert de AFM sinds een aantal jaar een eigen 'Werkwijze AFM inzien en kopiëren van digitale gegevens' (de Werkwijze). De Werkwijze beschrijft de procedure die de AFM bij digitaal onderzoek ter plaatse volgt en beoogt te voorzien in enige waarborgen voor het onderzoekssubject. De Werkwijze is laatstelijk gewijzigd op 9 maart 2020.[7] Volgens de AFM was dit nodig omdat eerdere versies vooral zagen op het doen van e-mailonderzoek. De nieuwe Werkwijze zou toezien op integraal digitaal onderzoek.[8]

De Werkwijze beschrijft grofweg vijf stappen. De eerste[9] bestaat eruit dat de toezichthouder die het toezichtonderzoek uitvoert (in de Werkwijze gedefinieerd als Onderzoeker) aan de hand van het doel van het onderzoek vaststelt welke digitale gegevens worden gevorderd van de financiële instelling. Ten aanzien van mobiele telefoons is onze ervaring dat reeds tijdens het bezoek, dus ten kantore van de instelling, per mobiele telefoon wordt geselecteerd welke informatie wordt gekopieerd en meegenomen. Van e-mailboxen wordt doorgaans wel een integrale kopie gemaakt en meegenomen. De door een IT-medewerker van de AFM (in de Werkwijze gedefinieerd als IT-Specialist)[10] gekopieerde gegevens worden ten kantore van de AFM opgeslagen op een van het toezicht afgescheiden IT-omgeving, waartoe de Onderzoeker volgens de Werkwijze geen toegang heeft.

De tweede stap[11] houdt in dat de IT-Specialist de instelling een overzicht van gekopieerde gegevens verstrekt, en 10 werkdagen geeft om onderbouwd toe te lichten welke gekopieerde gegevens als geprivilegieerd[12] en/of privé kwalificeren en daarom moeten worden uitgesloten.[13]

De derde stap[14] ziet op de beoordeling van de in stap twee bedoelde schoningsverzoeken (in de Werkwijze ook aangeduid als claims). In eerste instantie is het de IT-Specialist die beoordeelt of ingediende claims terecht zijn, en wel door het "*vluchtig inzien*" van de litigieuze gegevens. Deze schoning vindt volgens de Werkwijze in beginsel plaats ten kantore van de AFM. Alsdan moet de instelling in de gelegenheid worden gesteld daarbij aanwezig te zijn. Echter, als de instelling "*ondubbelzinnig en met precisie*" geprivilegieerde- of privégegevens kan duiden, zal de schoning reeds ten kantore van de instelling (moeten) plaatsvinden, tenzij daartegen zwaarwegende praktische bezwaren bestaan.[15]

Wordt een claim met betrekking tot geprivilegieerde gegevens afgewezen door de IT-Specialist, dan kan de instelling verzoeken dat deze claim (nogmaals) wordt beoordeeld door de zogeheten Functionaris Verschoningsrecht van de AFM. Indien (ook) de Functionaris Verschoningsrecht van

5 Met toezichthouder wordt niet bedoeld de AFM zelf maar een natuurlijk persoon "*bij of krachtens wettelijk voorschrift belast met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift*", zie art. 5:11 Awb. Art. 1:72 lid 1 Wft bepaalt in dit kader dat met toezicht op de Wft en daarop gebaseerde regelgeving zijn belast de bij besluit van AFM of DNB aangewezen (natuurlijke) personen. Zie *Stcrt.* 2020, 40669 voor het aanwijzingsbesluit van de AFM per 1 augustus 2020.

6 Art. 5:12 lid 2 Awb.

7 *Stcrt.* 2020, 13499.

8 Zie https://www.afm.nl/nl-nl/over-afm/werkzaamheden/toezichtaanpak.

9 Art. 2 Werkwijze.

10 Ook een toezichthouder in de zin van art. 5:11 Awb, maar volgens art. 1 Werkwijze niet betrokken bij de inhoudelijke uitvoering van het toezichtonderzoek.

11 Art. 2 Werkwijze.

12 Zoals gedefinieerd in art. 1 Werkwijze, kort gezegd advocaat-cliëntcorrespondentie.

13 Wat nog weleens lijkt te worden vergeten is dat betoogd kan worden dat een schoningsverzoek ook op eigen titel kan worden gedaan door de betrokken advocaat. Zie hierover Rb. Rotterdam 20 april 2010, ECLI:NL:RBROT:2010:BM4487, r.o. 2.9.

14 Art. 3-4 Werkwijze.

15 Art. 3 lid 2 Werkwijze.

oordeel is dat de claim onterecht is, moet hij de instelling daarvan schriftelijk en gemotiveerd in kennis stellen en erop wijzen dat hij de gegevens niet eerder dan na 10 werkdagen beschikbaar maakt voor de Onderzoeker. Deze wachttermijn biedt de instelling de mogelijkheid tegen de afwijzing op te komen via een kort geding bij de civiele rechter.

De vierde stap[16] houdt in dat de IT-Specialist, na afronding van de schoning, de Onderzoeker toegang geeft tot de geschoonde verzameling digitale gegevens. De Onderzoeker mag vervolgens uitsluitend in die verzameling gerichte zoekacties uitvoeren. De zoekstrategie moet zijn gebaseerd op zoektermen, die hun oorsprong vinden in het doel van het onderzoek, waarbij gebruik mag worden gemaakt van technische hulpmiddelen om het zoeken efficienter te laten verlopen. Desgevraagd dient de Onderzoeker de gehanteerde zoekstrategie toe te lichten. Nieuw in de Werkwijze is dat het gebruik van zoektermen niet verplicht is indien de gegevens, gezien het doel van het onderzoek, "*in hun totaliteit relevant kunnen zijn*".[17] De relevante gegevens worden vervolgens door de IT-Specialist overgedragen aan de Onderzoeker en opgeslagen in het onderzoeksdossier.

De vijfde en laatste stap[18] houdt verband met de bewaring en vernietiging van digitale gegevens. De IT-Specialist moet alle gekopieerde gegevens, met uitzondering van de gegevens die conform stap vier zijn opgeslagen in het onderzoeksdossier, vernietigen zo spoedig mogelijk nadat (i) het toezichtonderzoek is gesloten of (ii) de naar aanleiding van het onderzoek genomen besluiten onherroepelijk zijn geworden.

3. Grenzen en rechtsvragen bij digitaal onderzoek AFM

3.1 *De inzagevordering en medewerkingsplicht*

Op grond van art. 5:17 Awb is een toezichthouder bevoegd inzage te vorderen van zakelijke gegevens en bescheiden. Uit de wetsgeschiedenis volgt dat onder 'gegevens' ook digitale gegevens moeten worden begrepen.[19] Een toezichthouder is voorts bevoegd om van zakelijke gegevens en bescheiden ter plaatse kopieën te maken of, indien het ter plaatse maken van kopieën niet mogelijk is, de gegevens en bescheiden voor dat doel "*voor korte tijd mee te nemen*".

Art. 5:20 lid 1 Awb luidt:

> "Een ieder is verplicht aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden."

Overtreding van deze medewerkingsplicht kan door de AFM worden gesanctioneerd met een last onder dwangsom[20] en/of een boete[21] en kan zelfs leiden tot strafrechtelijke vervolging wegens het niet opvolgen van een ambtsedig gegeven bevel.[22]

3.2 *Grenzen aan de inzagevordering en medewerkingsplicht*

De hiervoor bedoelde inzagevordering en medewerkingsplicht zijn ruim geformuleerd. Tegelijkertijd heeft de wetgever wel degelijk grenzen getrokken die een toezichthouder in acht moet nemen. Een aantal grenzen sommen we hierna op.

3.2.1 *Alleen zakelijke gegevens en bescheiden*

De inzagevordering mag alleen betrekking hebben op zakelijke gegevens en bescheiden.[23] Digitale gegevens, waaronder gegevens op een mobiele telefoon, die geen zakelijk karakter hebben mogen in beginsel dus niet worden ingezien door een toezichthouder.

3.2.2 *Originele gegevens(drager) niet meenemen indien kopiëren ter plaatse mogelijk is*

Alleen indien de toezichthouder van zakelijke gegevens kopieën wenst te maken en dit ter plaatse niet mogelijk is, is de toezichthouder bevoegd de gegevens voor korte tijd mee te nemen. In de context van mobiele telefoons betekent dit dus dat een toezichthouder een mobiele telefoon in beginsel niet mag meenemen, omdat het maken van kopieën in de regel ter plaatse zal kunnen geschieden.

3.2.3 *Evenredigheids- en motiveringsbeginsel, voldoende specifiek*

Het proportionaliteits- en subsidiariteitsvereiste[24] brengen met zich dat een toezichthouder slechts gebruik mag maken van zijn bevoegdheden voor zover dat redelijkerwijs nodig is voor de vervulling van zijn taak. Dit betekent dat een inzagevordering moet vallen binnen de reikwijdte van het door de toezichthouder ingestelde onderzoek naar de naleving van het bepaalde bij of krachtens wettelijke voorschriften. De inzagevordering moet verder voldoende specifiek zijn en een toezichthouder moet in concrete gevallen toelichten waarom de inzagevordering met het oog op het doel en onderwerp van het onderzoek redelijker-

16 Art. 5 Werkwijze.
17 Waarbij volgens voetnoot 4 van de Werkwijze kan worden gedacht aan onderzoek op basis van controledossiers (Wta) en cliëntdossiers (Wwft).
18 Art. 6 Werkwijze.
19 *Kamerstukken II* 1993/94, 23700, nr. 3 (MvT), p. 144.
20 Art. 1:79 lid 1 onderdeel d Wft.
21 Art. 1:80 onderdeel d Wft.
22 Art. 184 Sr.
23 Volgens de MvT en NnavV bij art. 5:17 Awb moet onder zakelijke bescheiden en gegevens worden verstaan "*gegevens die worden gebruikt ten dienste van het maatschappelijk verkeer*", zie *Kamerstukken II* 1993/94, 23700, nr. 3, p. 144 en *Kamerstukken II* 1994/95, 23700, nr. 5, p. 85.
24 Zoals bepaald in art. 5:13 Awb. Deze bepaling is een nadere invulling van het in art. 3:4 lid 2 Awb neergelegde evenredigheidsbeginsel, zie ook *Kamerstukken II* 1993/94, 23700, nr. 3 (MvT), p. 142.

wijs nodig is.[25] Ongerichte en/of ongemotiveerde zoekacties (*fishing expeditions*) zijn niet toelaatbaar.[26]

3.2.4 *Overige beginselen behoorlijk bestuur*

Bij de inzet van de inzagevordering zal een toezichthouder zich in beginsel ook rekenschap moeten geven van de overige beginselen van behoorlijk bestuur, zoals het zorgvuldigheidsbeginsel,[27] het verbod van misbruik van bevoegdheden (*détournement de pouvoir*)[28] en het beginsel van onpartijdigheid (*fair play*).[29, 30]

3.2.5 *Uitzondering medewerkingsplicht*

Geheimhouders – bijvoorbeeld advocaten en notarissen – zijn niet gehouden om medewerking te verlenen aan een inzagevordering.[31] Dit houdt onder meer in dat correspondentie tussen een geheimhouder[32] en de instelling in beginsel niet door een toezichthouder mag worden ingezien. Aangenomen wordt dat ook de instelling zelf zich met betrekking tot deze geprivilegieerde correspondentie tegenover een toezichthouder kan beroepen op de uitzondering op de medewerkingsplicht.[33]

3.2.6 *Grondwettelijke bescherming communicatie*

Art. 13 lid 1 Grondwet (Gw) bepaalt dat het briefgeheim onschendbaar is, behalve, in de gevallen bij de wet bepaald, op last van de rechter. Voor telefoonverkeer bevat art. 13 lid 2 Gw een vergelijkbare bepaling. In een ruime interpretatie van art. 13 Gw geniet ook digitaal verkeer, zoals e-mail-, sms- en app-verkeer, grondwettelijke bescherming. In de rechtspraak is het briefgeheim in het kader van de digitale inzagevordering tot op zekere hoogte ook wel als relevante omstandigheid aangenomen.[34] De Eerste en Tweede Kamer hebben inmiddels een wetsvoorstel aangenomen om de grondwettelijke bescherming op dit punt expliciet uit te breiden naar alle huidige en toekomstige communicatiemiddelen.[35] Op het punt van de digitale inzagevordering lijkt het er echter op dat van deze uitbreiding niet te veel moet worden verwacht. In de toelichting bij het wetsvoorstel wordt namelijk gesteld dat het vorderen van inzage in communicatie die aanwezig is bij de verzender of de geadresseerde, *niet* onder de bescherming van art. 13 Gw valt.[36] Dit betekent dat het vorderen van inzage in mobiele telefoons rechtstreeks bij de gebruiker van de telefoon (en niet bij de telecom, app- of *cloudstorage*-provider) – hetgeen bij digitale onderzoeken door toezichthouders van de AFM in de regel het geval is – in beginsel buiten de reikwijdte van de grondwettelijke bescherming blijft.[37]

3.2.7 *Art. 8 EVRM*

Ingevolge art. 8 lid 1 van het Europees Verdrag voor de rechten van de mens (EVRM) heeft een ieder recht op eerbiediging van zijn of haar privéleven, familie- en gezinsleven, woning en correspondentie. Op grond van art. 8 lid 2 EVRM is een beperking van dit recht alleen mogelijk indien dit bij de wet is voorzien en in een democratische samenleving noodzakelijk is. Op art. 8 EVRM zal in paragraaf 4 nader worden ingegaan.

3.2.8 *Bescherming persoonsgegevens op grond van de AVG*

Hiervoor is al opgemerkt dat een inzagevordering alleen betrekking mag hebben op zakelijke gegevens en bescheiden. Ook dan is de kans echter groot dat deze gegevens persoonsgegevens bevatten in de zin van art. 4 onderdeel 1) Algemene verordening gegevensbescherming (AVG).[38] De toezichthouder zal bij het onderzoeken van de met behulp van de inzagevordering in handen gekregen persoonsgegevens rekening moeten houden met de AVG.[39]

25 In gelijke zin de toelichting bij de in art. 1:74 Wft opgenomen inlichtingenvordering van de AFM (als bestuursorgaan), *Kamerstukken II* 2003/04, 29708, nr. 3 (MvT), p. 45.

26 Zie hierover Roth, 'De toezichtsbevoegdheden van de AFM en DNB. Op zoek naar de grenzen van het schier teugelloze', *Ondernemingsrecht* 2009/115 (Roth 2009), par. 4.2.

27 Art. 3:2 Awb.

28 Art. 3:3 Awb.

29 Art. 2:4 Awb.

30 Art. 3:2-3:3 Awb zijn ingevolge art. 3:1 lid 1 Awb niet alleen van toepassing op besluiten, maar ook op andere handelingen van bestuursorganen voor zover de aard van de handelingen zich daartegen niet verzet. Zie ook Roth 2009, par. 4.1.

31 Art. 5:20, lid 2 Awb.

32 Of een derde die door de geheimhouder is ingeschakeld, bijvoorbeeld een accountant ten behoeve van de advisering door een advocaat.

33 Aldus ook de Minister van Financiën in *Kamerstukken II* 2005/06, 29708, nr. 32 (NnavV), p. 42.

34 Zie Rb. Rotterdam 5 september 2012, ECLI:NL:RBROT:2012:BX6988, r.o. 7.1.

35 Wet van 19 augustus 2017, houdende verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim. Omdat het gaat om een wijziging van de grondwet is voor de daadwerkelijke grondwetswijziging vereist dat na nieuwe Tweede Kamerverkiezingen in beide Kamers een twee derde meerderheid voor het voorstel bestaat.

36 *Kamerstukken II* 2013/14, 33989, nr. 3 (MvT), p. 39. Communicatie die zich bevindt bij een derde die de communicatie beheert, komt volgens de toelichting wel onder de grondwettelijke bescherming te vallen en kan dus in beginsel niet door de AFM worden ingezien.

37 Overigens pleit de AFM in het kader van de Verordening marktmisbruik al sinds 2015 voor een verruiming van haar onderzoeksbevoegdheden teneinde snel en effectief telefoon- en dataverkeer bij telecomproviders op te kunnen vragen. De wetgever is in die wens van de AFM vooralsnog niet meegegaan (zie *Kamerstukken II* 2015/16, 34455, nr. 3 (MvT), p. 19), maar mocht dat in de toekomst wijzigen dan zal wellicht ook de uitbreiding van art. 13 Gw aan belang toenemen.

38 Art. 4 onderdeel 1) AVG definieert persoonsgegevens als "*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*".

39 Zie ook Dielemans-Goossens & Baneke, 'De Digitale Werkwijze van ACM langs de lat van de Algemene Verordening Gegevensbescherming (AVG)', *MP* 2018/2 (Dielemans-Goossens 2018) en Beumer, 'De digitale werkwijzen van de ACM en de AFM bekeken met een AVG-bril', *TvT* 2019/1.

Dit houdt onder meer in dat de toezichthouder de beginselen inzake verwerking van persoonsgegevens[40] in acht neemt, waaronder het beginsel van minimale gegevensverwerking,[41] alsook de rechten van de betrokkenen eerbiedigt,[42] waaronder hun inzagerecht.[43] Daarnaast kan worden betoogd dat de toezichthouder ook gehouden is om voorafgaand aan de verwerking te beoordelen wat het effect van de beoogde verwerking is op de bescherming van persoonsgegevens, de zogeheten *data protection impact analysis*.[44] Juist in de context van onderzoek naar digitale op mobiele telefoons opgeslagen gegevens, waarbij de AFM meer en meer gebruikmaakt van nieuwe analysemethoden en er tegelijkertijd al snel persoonsgegevens in het spel zullen zijn, zijn deze verplichtingen zeer relevant.

3.3 *Een selectie van rechtsvragen*

3.3.1 *Maken en doorzoeken van digitale kopieën in strijd met doorzoekverbod en evenredigheidsbeginsel?*

Zoals toegelicht, dient een inzagevordering binnen de reikwijdte te blijven van het desbetreffende onderzoek naar overtreding van het bepaalde bij of krachtens wettelijke voorschriften. Als een toezichthouder in de 'analoge' wereld op zoek gaat naar informatie, dan mag hij een bedrijfsbezoek afleggen en ingevolge art. 5:15 Awb 'zoekend rondkijken', maar niet 'doorzoeken'. Wat een toezichthouder dus niet mag is willekeurig lades openen, dossiers uit kasten trekken en papier- en prullenbakken omkeren,[45] al wordt in de rechtspraak overigens niet snel aangenomen dat van doorzoeken sprake is.[46]

Indien dit uitgangspunt wordt doorgetrokken naar digitale onderzoeken, dan is verdedigbaar dat wanneer een AFM-toezichthouder veel of zelfs alle op een gegevensdrager opgeslagen digitale gegevens kopieert, en daarin vervolgens op zoek gaat naar mogelijk relevante informatie, in feite een digitaal bedrijfsbezoek wordt afgelegd waarbij alle digitale lades, kasten, dossiers, papier- en prullenbakken worden opengetrokken en doorzocht. Daarbij komt dat een toezichthouder juist in dat geval de beschikking krijgt over allerlei soorten gegevens, waarvan een aanzienlijk deel hoogstwaarschijnlijk buiten de reikwijdte van het onderzoek zal vallen. De vraag is dan ook of het integraal kopiëren en doorzoeken van de inhoud van een gegevensdrager, zoals een mobiele telefoon, niet (veel) verder gaat dan wat de wetgever oorspronkelijk heeft willen toelaten.[47]

Daar kan tegen in worden gebracht dat de toezichthouder op grond van de Werkwijze zoektermen hanteert bij het onderzoeken van de digitale kopie en daarom voldoende gericht en binnen de reikwijdte van het onderzoek gegevens inziet. Dat gaat er echter aan voorbij dat de Werkwijze aan de inhoud van de zoektermen geen concrete eisen stelt, anders dan dat de zoektermen "*hun oorsprong vinden in het doel van het onderzoek*".[48] Het is maar zeer de vraag of de zoektermen dermate specifiek en onderzoek-gebonden zijn dat daarmee steeds bewerkstelligd wordt dat uitsluitend binnen-de-reikwijdte-informatie komt bovendrijven en zogeheten 'bijvangst' wordt uitgesloten. Voorts is de Werkwijze in maart 2020 zoals opgemerkt zo aangepast dat een toezichthouder het gebruik van zoektermen geheel achterwege kan laten indien de gekopieerde gegevens "*gezien het doel van het onderzoek, in hun totaliteit relevant kunnen zijn*".[49]

Zolang de wet op dit punt niet de benodigde duidelijkheid biedt, zullen aangezochte rechters hierover per individueel geval een oordeel moeten vellen. Daarbij valt op dat civiele kortgedingrechters tot nu toe (in mededingingszaken) bij de beantwoording van de vraag of een digitale inzagevordering rechtmatig door een toezichthouder is ingezet, veel belang lijken toe te kennen aan het onderzoeksbelang.[50]

3.3.2 *Leidt de Werkwijze tot uitholling van de waarborgen inzake geprivilegieerde informatie en tot strijdigheid met de AVG?*

Een tweede interessante rechtsvraag is of de in art. 5:20 lid 2 Awb opgenomen uitzondering op de medewerkingsplicht voor advocaat-cliëntcommunicatie, niet wordt uitgehold als een IT-Specialist respectievelijk een Functionaris Verschoningsrecht claims van de instelling beoordeelt.[51]

De IT-Specialist is volgens de Werkwijze "*een toezichthouder in de zin van artikel 5:11 Awb die tevens belast is met het proces van identificeren, veiligstellen, kopiëren en verwerken van Digitale gegevens en die niet betrokken is bij de inhoudelijke uitvoering van het toezichtonderzoek*". Een Functionaris Verschoningsrecht wordt in de Werkwijze

40 Art. 5 AVG.
41 Art. 5 lid 1 onderdeel c AVG.
42 Art. 12-22 AVG.
43 Art. 15 AVG.
44 Art. 35 AVG.
45 *Kamerstukken II* 1993/94, 23700, nr. 3 (MvT), p. 143 en CBb 12 oktober 2017, ECLI:NL:CBB:2017:326, r.o. 4.6.
46 Zie ook Roth 2009, par. 3.1.
47 Zie ook Nuijten & Stijnen, *Rechterlijke toetsing van besluiten en handelingen van de AFM en DNB* (VDHI nr. 155) (Nuijten 2018), p. 62.
48 Art. 5 lid 2 onderdeel a Werkwijze.
49 Art. 5 lid 2 onderdeel b Werkwijze.
50 Zie Rb. Den Haag 22 november 2017, ECLI:NL:RBDHA:2017:14150, dat gaat over digitaal onderzoek door de Autoriteit Consument & Markt (ACM) naar de inhoud op mobiele telefoons. Zie verder bijvoorbeeld Rb. 's-Gravenhage 13 oktober 2008, ECLI:NL:RBSGR:2008:BH2647, r.o. 4.5-4.6. De rechtbank oordeelt dat de (voorloper van de) ACM bij het inzetten van de inzagevordering om digitale kopieën van volledige e-mailboxen te maken, in strijd heeft gehandeld met het evenredigheidsbeginsel van art. 5:13 Awb. De rechtbank verbindt daaraan echter niet de conclusie dat de gekopieerde gegevens moeten worden vernietigd, maar dat het onderzoek van de digitale kopieën moet plaatsvinden in aanwezigheid van de gemachtigden van de betrokken ondernemingen, zodat die erop toe kunnen zien dat gekopieerde gegevens die buiten doel en onderwerp van het onderzoek vallen niet worden doorzocht.
51 Zie art. 3-4 Werkwijze.

omschreven als "*een door het bestuur van de AFM aangewezen persoon die, niet als IT-Specialist of als Onderzoeker bij onderzoeken betrokken is of zal zijn, onafhankelijk van het toezicht het geprivilegieerde karakter van de door het Onderzoekssubject geclaimde gegevens toetst*".

Beide functionarissen zijn dus *volgens de Werkwijze* niet inhoudelijk betrokken bij het onderzoek, maar wel gewoon werkzaam bij de AFM. De Werkwijze stelt bovendien geen enkele kwaliteits- of andere eis aan de persoon die als Functionaris Verschoningsrecht optreedt. Het aanwijzingsbesluit van de AFM[52] zegt hier wel iets over. Daarin wordt de 'General Counsel' van de AFM als Functionaris Verschoningsrecht aangewezen. Uit het aanwijzingsbesluit blijkt voorts dat de General Counsel besluitvorming vervolgens heeft gemandateerd[53] aan een "*manager die niet betrokken is bij onderzoek en handhaving*". Een General Counsel en een AFM-manager kunnen allerlei rollen binnen de AFM vervullen. Het kan dan ook niet worden uitgesloten dat zij bij andere onderzoeken en/of procedures – mogelijk zelfs met betrekking tot dezelfde instelling – wél inhoudelijk betrokken zijn. Het is daarom naar onze mening onwenselijk dat de General Counsel dan wel een manager kennis heeft van geprivilegieerde advocaat-cliëntcommunicatie. Toch is die situatie bepaald niet ondenkbeeldig. Denk bijvoorbeeld aan advocaatadviezen die door instellingen intern worden gedeeld, besproken en nader uitgewerkt, bijvoorbeeld in interne memo's. In dat geval kunnen discussies met de AFM ontstaan of ook die interne informatie/communicatie als geprivilegieerde informatie kwalificeert. Het is dan goed mogelijk dat de IT-Specialist op die informatie gerichte claims van de instelling afwijst en vervolgens de Functionaris Verschoningsrecht zich over die kwalificatievraag moet buigen, en dus kennisneemt van geprivilegieerde informatie.

We wijzen er verder op dat (i) door de IT-Specialist of Functionaris Verschoningsrecht als geprivilegieerd erkende gegevens en (ii) voor het onderzoek niet-relevante informatie, op basis van de Werkwijze niet meteen worden vernietigd. De AFM wacht conform de eigen Werkwijze doorgaans namelijk met vernietiging totdat het onderzoek is gesloten[54] of zelfs tot het einde van de bezwaar- en beroepsprocedure tegen besluiten die naar aanleiding van het onderzoek door de AFM zijn genomen.[55] Daarmee kunnen die gegevens tot in lengte van jaren bij de AFM blijven liggen, terwijl de Awb voor (het kopiëren en) het bewaren van die gegevens geen enkele grondslag lijkt te bieden. Betreft het daarbij persoonsgegevens dan roept deze praktijk bovendien sterk de vraag op of de AFM daarmee niet in strijd handelt met de AVG. Persoonsgegevens worden dan immers langer bewaard dan noodzakelijk.[56]

3.3.3 *Awb nog wel voldoende bij de tijd?*

Al het vorengaande werpt de vraag op of het bestaande wettelijk kader inzake de inzagevordering überhaupt nog wel voldoende is toegesneden op geavanceerd digitaal onderzoek door de AFM. De regeling zoals opgenomen in de Awb stamt uit de jaren '90 en is duidelijk gericht op het houden van toezicht en het doen van onderzoek in de niet-digitale wereld. Het lijkt niet te veel gezegd dat er een gat gaapt tussen de wet en de praktijk op dit punt, waardoor steeds onduidelijker wordt of de wet nog wel voldoende basis biedt.[57] Consequentie daarvan is ook dat de rechter er steeds vaker aan te pas moet komen om verouderde bepalingen toe te passen op nieuwe situaties.

3.3.4 *Voldoende mogelijkheden om inzagevordering ter discussie te stellen?*

Een vierde, belangrijke, rechtsvraag is of aan een instelling en haar beleidsbepalers op dit moment voldoende mogelijkheden toekomen om de rechtmatigheid van een digitale inzagevordering aan de orde te stellen. Op die vraag wordt hierna ingegaan.

4. Mogelijkheden om rechtmatigheid digitale inzagevorderingen ter discussie te stellen

4.1 *Jegens de AFM zijn de mogelijkheden relatief beperkt*

Als een toezichthouder van de AFM voornemens is via de inzagevordering op een gegevensdrager opgeslagen gegevens te kopiëren en in te zien, is het de vraag hoe een instelling en/of betrokken beleidsbepaler ervoor kan zorgen dat de toezichthouder daarbij de hiervoor besproken wettelijke grenzen in acht neemt, zonder direct naar de rechter te moeten stappen.

De betrokken instelling en beleidsbepaler zullen uiteraard het liefst zien dat überhaupt geen privégegevens, geprivilegieerde correspondentie en buiten-de-reikwijdte-informatie bij de AFM terechtkomen. Om dat ook daadwerkelijk te voorkomen is vereist dat de toezichthouder ter plekke een (geschoonde) selectie maakt van de te kopiëren en mee te nemen data, in overleg met onder meer de beleidsbepaler en diens advocaat. De AFM zal daar echter niet steeds mee instemmen, mede omdat dit praktische bezwaren oplevert indien op de gegevensdrager grote hoeveelheden data (zoals e-mails) staan. Een weigering om de gegevensdrager in dat geval aan de toezichthouder ter beschikking te stellen levert voor de instelling en de beleidsbepaler ook een aanzienlijk risico op, omdat de

52 *Stcrt.* 2020, 40669.
53 Ingevolge art. 10:7 Awb blijft de General Counsel bevoegd als Functionaris Verschoningsrecht op te treden.
54 Art. 6 lid 1 onderdeel a Werkwijze.
55 Art. 6 lid 1 onderdeel b Werkwijze.
56 Zo ook Dielemans-Goossens 2018, p. 34.
57 Zie ook Jansen, 'Koudwatervrees in een bananenkoninkrijk? Over de toekomstbestendigheid van titel 5.2 Awb', *JBplus* 2017/10.

AFM kan stellen dat daarmee de medewerkingsplicht wordt geschonden met alle risico's op sancties van dien.[58]

Het zal er daarom regelmatig op neerkomen dat, eventueel onder protest, wordt toegestaan dat de IT-Specialist ter plaatse een digitale kopie van de bewuste gegevens maakt. Vervolgens zal de AFM betrokkenen de gelegenheid bieden om de hiervoor besproken schoningsverzoeken in te dienen.[59] Positief is dat de Werkwijze in een aanwezigheidsrecht voorziet indien de daaropvolgende schoning ten kantore van de AFM plaatsvindt. Problematisch is echter dat die informatie, ook wanneer de schoningsverzoeken zijn gehonoreerd, dan wel al bij de AFM ligt, mogelijk voor een lange periode.

De Werkwijze voorziet er bovendien nog altijd niet in dat inzicht wordt geboden aan de instelling welke gekopieerde gegevens door de Onderzoeker als "*relevant*"[60] voor het onderzoek zijn aangemerkt. De Werkwijze voorziet dus ook niet in een procedure voor het indienen van bezwaren/schoningsverzoeken tegen de door de Onderzoeker gemaakte selectie. Dit kan als een materiële tekortkoming in de rechtsbescherming worden beschouwd en staat onzes inziens op gespannen voet met jurisprudentie van de Rechtbank Den Haag.[61] Deze jurisprudentie ziet op digitaal onderzoek verricht door de ACM en zou naar onze mening in dit verband, gelet op de gelijkenissen met digitaal onderzoek door de AFM, ook richtinggevend moeten zijn voor het handelen door de AFM.

Tot slot is van belang dat een schriftelijke inzagevordering op grond van jurisprudentie van het College van Beroep voor het bedrijfsleven niet wordt beschouwd als een besluit in de zin van art. 1:3 lid 1 Awb.[62] Daardoor is het niet mogelijk voor een instelling of beleidsbepaler om bezwaar te maken tegen een dergelijke vordering. Zij kunnen eventueel wel een besluit uitlokken door middel van een zogenoemd op zichzelf betrekking hebbend handhavingsverzoek. Dit zal inhouden een verzoek aan de AFM tot het opleggen van een last onder dwangsom strekkende tot naleving van de medewerkingsplicht ex art. 5:20 Awb inzake een (te geven) inzagevordering.[63] Daarbij moet wel worden bedacht dat het vervolgens maken van bezwaar de werking van bedoeld dwangsombesluit niet opschort.[64] Er zal dus alsnog binnen de begunstigingstermijn[65] aan de inzagevordering voldaan moeten worden, tenzij in de tussentijd de hierna te bespreken voorzieningenrechter uitkomst biedt.

4.2 *Gang naar de rechter?*

Als de betrokken instelling en/of beleidsbepaler er over de inzet van de digitale inzagevordering met de AFM zelf niet uit komt, rest een gang naar de rechter om de rechtmatigheid te laten toetsen. Daarbij kan onderscheid worden gemaakt in een gang naar de rechter in de voorfase (de IT-Specialist heeft nog geen gegevens gekopieerd), tussenfase (de IT-Specialist heeft gegevens wel gekopieerd maar deze zijn door de Onderzoeker nog niet ingezien) en nafase (de Onderzoeker heeft de geschoonde gegevens ingezien en aan het onderzoeksdossier toe laten voegen).

4.2.1 *Voorfase*

In de voorfase laat zich een gang naar de bestuursrechter niet gemakkelijk voorstellen, vooral waar het een onaangekondigd bedrijfsbezoek van de AFM betreft. De instelling wordt dan immers ter plekke met de inzagevordering geconfronteerd. Zoals hiervoor opgemerkt, wordt de inzagevordering conform vaste jurisprudentie niet aangemerkt als een besluit in de zin van art. 1:3 lid 1 Awb. Daardoor ontbreekt niet alleen de mogelijkheid van bezwaar en beroep, maar ook de mogelijkheid om een voorlopige voorziening te vragen. Een, als toegelicht, niet aantrekkelijke uitweg is dan de enkele weigering om aan de inzagevordering mee te werken, waarna de instelling tegen een eventuele door de AFM opgelegde last onder dwangsom – die wel als besluit kwalificeert – alsnog een voorlopige voorziening inclusief voorlopig rechtmatigheidsoordeel kan vragen bij de voorzieningenrechter. Een andere mogelijke uitweg is het hiervoor genoemde op zichzelf betrekking hebbende handhavingsverzoek.[66] Dat verzoek kan ter plaatse aan de AFM worden gericht of, in geval van een aangekondigd bedrijfsbezoek, van tevoren.

58 Voor een praktijkvoorbeeld, zie Rb. Rotterdam 20 april 2010, ECLI:NL:RBROT:2010:BM4487.

59 In het licht van art. 5:13 Awb is overigens onduidelijk waarom de Werkwijze op dit punt niet in een voor de instelling minder belastende procedure voorziet. Indien eerst met zoektermen wordt vastgesteld welke gegevens voor het onderzoek relevant zijn, en daarna ten aanzien van die (overgebleven) gegevens de instelling in de gelegenheid worden gesteld schoningsverzoeken in te dienen, zou dat bij grote hoeveelheden gekopieerde gegevens qua belasting aanmerkelijk kunnen schelen.

60 Art. 5 lid 4 Werkwijze.

61 Rb. Den Haag 12 juli 2017, ECLI:NL:RBDHA:2017:7968, r.o. 4.12. In deze zaak stond de digitale werkwijze van de ACM centraal, die overigens op het punt van 'binnen/buiten-de-reikwijdte-van-het-onderzoekinformatie' meer waarborgen biedt dan de AFM-Werkwijze. Niettemin toonde de rechter zich ook over de ACM-Werkwijze kritisch en oordeelde dat de betrokken instelling de mogelijkheid moet hebben om bij de ACM bezwaar te maken tegen het gebruik van bepaalde, concrete documenten die volgens de instelling buiten de reikwijdte van het onderzoek vallen. Indien een dergelijk bezwaar wordt gemaakt, kan de ACM volgens de rechter dat niet afwijzen uitsluitend met verwijzing naar de nadere selectie met behulp van de door de ACM gehanteerde zoektermen.

62 Zie hierover ook Roth, 'Rechtsbescherming tegen handelingen van DNB en de AFM. Observaties uit dogmatisch én praktisch oogpunt', *Ondernemingsrecht* 2016/48 (Roth 2016), p. 225 en Nuijten 2018, p. 7-9 en de aldaar genoemde jurisprudentie.

63 Uiteraard zal de instelling om een voor zichzelf minst belastende maatregel willen verzoeken. In het kader van de Wft zal dat de aanwijzing ex art. 1:75 Wft zijn. Echter, een aanwijzing lijkt niet mogelijk nu een aanwijzing (anders dan een last onder dwangsom) ingevolge art. 1:75 Wft niet kan worden gegeven voor een (dreigende) schending van art. 5:20 Awb.

64 Art. 6:16 Awb.

65 De termijn gedurende welke de instelling de last kan uitvoeren zonder dat een dwangsom wordt verbeurd.

66 Zie voor een praktijkvoorbeeld Rb. Rotterdam 5 september 2012, ECLI:NL:RBROT:2012:BX6988. Hoewel dit niet als zodanig in de uitspraak tot uitdrukking is gebracht, kwam de hierin behandelde last voort uit een handhavingsverzoek van verzoekers zelf.

Indien de AFM een dergelijk verzoek honoreert en de instelling ook daadwerkelijk een last onder dwangsom oplegt, staat eveneens de gang naar de voorzieningenrechter open. In beide situaties hangt het wel af van de in het dwangsombesluit opgenomen begunstigingstermijn of dit praktisch gezien ook haalbaar is.[67]

In de voorfase kan steeds een gang naar de civiele (kortgeding)rechter worden overwogen op grond van een dreigende onrechtmatige daad door de AFM. Het zal echter telkens de vraag zijn of dat ook praktisch haalbaar is als de AFM vrijwel onmiddellijk inzage vordert.

4.2.2 *Tussenfase*

Op grond van art. 8 EVRM-jurisprudentie (*Delta Pekárny*)[68] moet rechterlijke controle achteraf (in ieder geval) effectief zijn wanneer een voorafgaande rechterlijke machtiging voor een tijdens een bedrijfsbezoek uit te voeren inspectie door de toezichthouder, ontbreekt. Het *Vinci*-arrest[69] gaat over rechterlijke controle achteraf in de situatie dat de betrokken instelling tijdens het onderzoek door de autoriteiten naar een veelheid aan documenten niet in staat wordt gesteld de inhoud van de in beslag genomen documenten te inspecteren en de inbeslagname ter discussie te stellen. Het EHRM oordeelde in het licht van art. 8 EVRM dat in casu van een dergelijke effectieve controle achteraf geen sprake was omdat de Franse rechter slechts terughoudend de rechtmatigheid toetste in plaats van (i) concreet te onderzoeken of de documenten wel binnen het onderzoek vielen en niet geprivilegieerd waren en (ii) zo nodig tot restitutie van de documenten te verplichten.

In het bestuursrecht geldt – zo nemen rechters aan – niet het vereiste van een (rechterlijke) machtiging voorafgaand aan de inzet van de inzagevordering.[70] Daarnaast zijn, zoals hiervoor geconstateerd, de mogelijkheden voor een instelling relatief beperkt om jegens de AFM tijdens het onderzoek de rechtmatigheid van het inzien van digitale gegevens aan de orde te stellen, bijvoorbeeld waar het de selectie van voor het onderzoek relevante gegevens betreft. Gelet hierop is de in de EHRM-jurisprudentie ontwikkelde effectiviteitstoets voor het rechterlijke oordeel achteraf naar onze mening zowel in de tussen- als nafase relevant en is het de vraag of een gang naar de Nederlandse rechter die toets doorstaat.

De rechter die het best geëquipeerd lijkt te zijn om te oordelen over de rechtmatigheid van een digitale inzagevordering is de bestuursrechter. De inzagevordering betreft immers een bevoegdheid uit de Awb die in belangrijke mate wordt begrensd door geschreven en ongeschreven bestuursrechtelijke beginselen. In de tussenfase zal een instelling daar niet snel terecht kunnen, omdat dan reeds (al dan niet onder protest) voldaan is aan de inzagevordering en de hiervoor in de voorfase genoemde uitwegen niet langer beschikbaar zijn.[71]

Een instelling kan zich in de tussenfase wel steeds wenden tot de civiele rechter. Die is namelijk als restrechter bevoegd om over de rechtmatigheid van toezichthandelingen – zoals de inzagevordering – een oordeel te geven. De civiele kortgedingrechter kan dat zo nodig op (heel) korte termijn doen.[72] Zoals hiervoor opgemerkt, biedt de Werkwijze voor afgewezen schoningsverzoeken inzake geprivilegieerde informatie de instelling ook expliciet de mogelijkheid om binnen 10 werkdagen een dergelijk kort geding tegen de AFM aanhangig te maken.

De kortgedingrechter toetste de rechtmatigheid van de inzet van digitale inzagevorderingen (in mededingingszaken) voorheen zeer terughoudend,[73] maar daar is nog niet zo heel lang geleden verandering in gekomen. In 2017 heeft de kortgedingrechter van de Rechtbank Den Haag, onder verwijzing naar de hiervoor genoemde EHRM-arresten *Vinci* en *Delta Pekárny*, geoordeeld dat een dergelijke terughoudende toetsing zich niet verdraagt met het recht van de betrokken instelling op effectieve rechterlijke controle achteraf. Hoe het volgens de kortgedingrechter wel moet? Bij onderbouwde stellingen dat specifiek geïdentificeerde documenten door de toezichthouder zijn meegenomen hoewel deze onvoldoende verband houden met het onderzoek of geprivilegieerd zijn, dient de kortgedingrechter de betreffende documenten te onderzoeken en indien nodig de teruggave daarvan te gelasten.[74] In 2018 heeft de kortgedingrechter van de Rechtbank Den Haag onder verwijzing naar *Delta Pekárny* benadrukt dat bij een rechterlijke toetsing van een bedrijfsbezoek achteraf niet uitsluitend de rechtmatigheid van dat bedrijfsbezoek, maar ook de noodzakelijkheid daarvan – in-

67 Als de begunstigingstermijn zo kort is dat deze verstrijkt voordat om een voorlopige voorziening kan worden verzocht, is het namelijk de vraag of nog wel sprake is van een spoedeisend belang zoals vereist door art. 8:81 Awb.

68 EHRM 2 oktober 2014, ECLI:CE:ECHR:2014:1002JUD000009711, *AB* 2015/29.

69 EHRM 2 april 2015, ECLI:CE:ECHR:2015:0402JUD006362910, *AB* 2016/45.

70 Zie bijvoorbeeld Rb. Den Haag 10 oktober 2018, ECLI:NL:RBDHA:2018:12722, r.o. 4.6, in hoger beroep bevestigd door Hof Den Haag 12 februari 2019, ECLI:NL:GHDHA:2019:470, r.o. 4.4 en 4.8.

71 Een voorbeeld waarin dit wel lukte biedt ECLI:NL:RBROT:2010:BM4487. In deze zaak hadden toezichthouders van de AFM tijdens een onderzoek ter plaatse e-mailboxen op DVD laten kopiëren. Vervolgens had de instelling de DVD in haar kluis geplaatst en de AFM verzocht om een op zichzelf betrekking hebbend handhavingsverzoek. De AFM legde de instelling een last onder dwangsom op, waarna (onder andere) de instelling zich met betrekking tot het dwangsombesluit tot de voorzieningenrechter wendde.

72 Voor een beroep op de kortgedingrechter moet gelet op art. 254 Rv wel sprake zijn van een spoedeisend belang aan de zijde van eiser (de betrokken instelling en/of de beleidsbepaler(s)). Daar zal echter al snel aan voldaan zijn bij de hier bedoelde inzagevorderingen.

73 Zie bijvoorbeeld Rb. 's-Gravenhage 9 april 2003, ECLI:NL:RBSGR:2003:AF7087, r.o. 4.3-4 en Rb. 's-Gravenhage 13 oktober 2008, ECLI:NL:RBSGR:2008:BH2647, r.o. 4.4.

74 Rb. Den Haag 12 juli 2017, ECLI:NL:RBDHA:2017:7968, r.o. 4.4-4.5.

clusief van het verzamelen van bewijsstukken (de gekopieerde documenten) – moet worden getoetst.[75]

Bedoelde uitspraken uit 2017 en 2018 hebben betrekking op digitaal onderzoek ter plaatse door de ACM en zouden, nu de ACM net als de AFM een bestuursorgaan is waarvan de medewerkers bij het doen van digitaal onderzoek gebruikmaken van dezelfde inzagevordering uit de Awb, naar onze mening ook richtinggevend moeten zijn in kortgedingprocedures waarin digitaal onderzoek door de AFM ter discussie wordt gesteld.

Hoewel deze nieuwe invulling van de rechterlijke controle vanuit het perspectief van rechtsbescherming een stap in de goede richting is, is hier ook de nodige kritiek op geuit[76] en blijft het de vraag of het civiele kort geding een voldoende effectief middel is om tegen een digitale inzagevordering op te komen. Allereerst blijft het immers een procedure bij een niet-bestuursrechter terwijl moet worden geoordeeld over de rechtmatigheid van de inzet van een bevoegdheid uit de Awb. Daarnaast is er in de literatuur op gewezen dat (i) het snelle en informele kort geding niet is bedoeld voor een proces waarin grote hoeveelheden bestanden één voor één moeten worden beoordeeld op hun relevantie voor het onderzoek van de toezichthouder;[77] (ii) de mogelijkheden van een civiele procedure achter gesloten deuren beperkter zijn dan bij een bestuursrechtelijke procedure en het risico van openbaarheid derhalve groter is;[78] (iii) het civiele griffierecht (aanzienlijk) hoger is dan in het bestuursrecht;[79] en (iv) het bestuursorgaan zich als gedaagde in een civiele procedure moet kunnen uitlaten over de omstreden stukken waarvan moet worden beoordeeld of zij wel of niet binnen de reikwijdte van het onderzoek vallen, terwijl de betrokken instelling juist wil voorkomen dat het bestuursorgaan daarvan kennis neemt.[80]

Onze indruk is dat een gang naar de civiele rechter door financiële instellingen, mede gelet op het voorgaande, als een (veel) hogere drempel wordt ervaren dan een gang naar de bestuursrechter. Dit lijkt ook te volgen uit het feit dat er maar een zeer beperkt aantal uitspraken beschikbaar is inzake civiele procedures tegen de AFM.

4.2.3 *Nafase*

Ook in de nafase – de Onderzoeker heeft dan inmiddels inzage genomen – staat een instelling een beroep op de civiele rechter ter beschikking, en voor wat betreft een kort geding zolang de instelling daarbij een spoedeisend belang heeft. Over een gang naar de bestuursrechter in de nafase het volgende. Indien het onderzoek waarvan de inzagevordering deel uitmaakte uiteindelijk leidt tot een besluit, zoals bijvoorbeeld een aanwijzing of een boete, dan staat tegen dat besluit bezwaar bij de AFM en vervolgens beroep bij de bestuursrechter open. Indien dat besluit (mede) is gestoeld op met de inzagevordering verkregen informatie, kan ook die inzagevordering als onderdeel van het bezwaar of beroep ter discussie worden gesteld. Echter, om verschillende redenen laat de effectiviteit van die rechterlijke controle achteraf te wensen over. Zo is het allereerst niet zeker dat het onderzoek ook daadwerkelijk in een besluit resulteert. En als de AFM wel een besluit neemt, is het goed mogelijk dat dit besluit slechts voor een (beperkt) deel is gebaseerd op de met de inzagevordering verkregen informatie, waardoor de rechter zich daarover slechts een beperkt oordeel kan vormen.[81] Daarnaast duurt het doorgaans geruime tijd voordat de bestuursrechter uitspraak heeft gedaan, terwijl eventuele onrechtmatig verkregen gegevens in de tussentijd wel tot andere onderzoeken van de AFM kunnen leiden.

4.3 *Roep om toezichthandelingen onder het besluitbegrip te brengen en een blik op het strafrecht*

Om de rechtsbescherming tegen toezichthandelingen te vergroten, wordt ervoor gepleit[82] om het wettelijke besluitbegrip uit te breiden met (onder andere) de schriftelijke inzagevordering. Dat zou ertoe leiden dat de instelling en andere belanghebbenden tegen het besluit van de AFM om de bijvoorbeeld op een mobiele telefoon opgeslagen gegevens in te zien en te kopiëren, steeds kunnen opkomen bij de AFM en vervolgens een beroep kunnen doen op de bestuursrechter van de Rechtbank Rotterdam. De bezwaar- en beroepsprocedure zorgt er als toegelicht in beginsel echter niet voor dat de werking van een dergelijk besluit wordt geschorst, maar daartoe zou dan – in het beste geval al in de voorfase – de voorzieningenrechter om een voorlopige voorziening inclusief voorlopig rechtmatigheidsoordeel kunnen worden gevraagd. Ook wij zouden bedoelde uitbreiding van het besluitbegrip toejuichen, waarbij wij ons realiseren dat ook dan nog steeds een enigszins bereidwillige opstelling van de AFM is vereist. De AFM zal ook dan immers bij een onaangekondigd bezoek het inzagebesluit ter plekke aan de instelling uitreiken en onmiddellijke medewerking kunnen eisen, zodat een gang naar de voorzieningenrechter op praktische problemen zal stuiten.

75 Rb. Den Haag 10 oktober 2018, ECLI:NL:RBDHA:2018:12722, r.o. 4.4. Zie ook de uitspraak in hoger beroep van Hof Den Haag 12 februari 2019, ECLI:NL:GHDHA:2019:470, r.o. 4.1-4.6 en 4.12.

76 Speyart, 'Vzr Rb Den Haag 12 juli 2017: binnen/buiten de reikwijdte discussie en effectieve rechtsbescherming na Vinci', *MP* 2017/5 (Speyart 2017).

77 Speyart 2017, par. 4.2.

78 Roth 2016, p. 225.

79 Idem.

80 Speyart 2017, par. 4.2.

81 Nuijten 2018, p. 12. Nuijten voegt daar nog aan toe dat zelfs als de rechter oordeelt dat materiaal onrechtmatig is verkregen, dit er niet toe zal leiden dat het materiaal moet worden teruggegeven en dat het zelfs in beginsel mag worden gebruikt door de toezichthouder.

82 Nuijten 2018 p. 14-16. Zie ook Barkhuysen, Van Emmerik e.a., *Adequate rechtsbescherming bij grondrechtenbeperkend overheidsingrijpen. Studie naar aanleiding van de agenda voor de rechtspraak*, Deventer: Kluwer 2014, p. 123 en 181 (eerste bullet).

In dit verband kan niet voorbij worden gegaan aan de ontwikkeling die in het strafrecht momenteel gaande is met betrekking tot digitale opsporing. De Hoge Raad heeft zich in 2017 in de zogeheten smartphone-arresten uitgesproken over het in beslag nemen en onderzoeken van mobiele telefoons in de strafrechtelijke sfeer.[83] In deze arresten heeft de Hoge Raad overwogen dat indien alle op een smartphone en/of de bijbehorende sim-kaart opgeslagen of beschikbare gegevens zijn door- en uitgelezen – waardoor (volledig) inzicht is verkregen in contacten, oproepgeschiedenis, berichten en foto's – het vermoeden ontstaat dat een "*meer dan beperkte inbreuk*" op de persoonlijke levenssfeer van de gebruiker is gemaakt.[84] Die inbreuk kan volgens de Hoge Raad onrechtmatig zijn, maar niet indien de officier van justitie (OvJ) of rechter-commissaris (R-C) – in plaats van de politie zelf – de onderzoeksbevoegdheden uitoefent. Daarbij valt volgens de Hoge Raad in het licht van art. 8 EVRM aan onderzoek door de R-C in het bijzonder te denken aan gevallen waarin op voorhand is te voorzien dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn.[85]

De mede naar aanleiding van de smartphone-arresten in het leven geroepen commissie-Koops[86] heeft de Minister van Justitie en Veiligheid aanbevolen de OvJ aan te wijzen als bevoegde autoriteit indien op voorhand redelijkerwijs voorzienbaar is dat door inzet van de onderzoeksbevoegdheden een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan. Indien een *ingrijpend* beeld van iemands privéleven kan ontstaan, stelt de commissie voor de R-C als beslissende autoriteit aan te wijzen.[87] De aanbevelingen van de commissie zijn volgens de minister zoveel mogelijk verwerkt in een nieuwe regeling met betrekking tot het onderzoek van gegevens.[88] Die exercitie maakt onderdeel uit van een bredere modernisering van het Wetboek van Strafvordering, waarvoor het wetsvoorstel momenteel in de maak is.

De hiervoor beschreven ontwikkeling die voorziet in meer waarborgen – inclusief expliciete machtiging door de OvJ of R-C vooraf – naarmate de te verwachten inbreuk op de privacy van de betrokkene groter is, heeft naar onze mening ook relevantie voor het bestuursrecht. Een analyse van de overeenkomsten en verschillen tussen het bestuursrecht en het strafrecht gaat het bestek van deze bijdrage te buiten, maar wij werpen hier wel alvast de vraag op of het te rechtvaardigen valt dat de waarborgen in het strafrecht en de waarborgen in het bestuursrecht op dit punt uit elkaar lopen. Ook in het bestuursrecht heeft het kopiëren van op een mobiele telefoon opgeslagen gegevens immers implicaties voor de privacy van de betrokken beleidsbepaler, met name wanneer de door de toezichthouder in beslag genomen gegevens afkomstig zijn van een telefoon die door de beleidsbepaler ook privé wordt gebruikt. Daarbij komt dat ook in het financiële bestuursrecht (heel forse) bestraffende sancties kunnen worden opgelegd. Toch hebben toezichthouders van de AFM geen machtiging nodig om die gegevens integraal te kopiëren en in te zien.

5. Uitleiding

Bij digitaal onderzoek door de AFM komen in optima forma allerlei rechtsvragen op waar de Awb geen duidelijk antwoord op geeft. Dat de AFM een Werkwijze hanteert is op zich positief, maar het is de vraag of de Werkwijze aan financiële instellingen en hun beleidsbepalers daadwerkelijk alle vereiste waarborgen biedt.

We menen dat in ieder geval verbeteringen mogelijk zijn ten aanzien van de beoordeling van geprivilegieerde informatie, de beoordeling of gegevens voor het onderzoek relevant zijn en de bewaring van gegevens die uiteindelijk niet in het onderzoeksdossier terechtkomen. Daarnaast is meer algemeen de vraag gewettigd of betrokkenen op dit moment wel over voldoende (effectieve) wettelijke mogelijkheden beschikken om de rechtmatigheid van toezichthandelingen van de AFM ter discussie te stellen. Een belangrijke stap voorwaarts zou hoe dan ook zijn dat wordt verzekerd dat inzagevorderingen steeds kwalificeren als besluiten, waardoor de bestuursrechter een prominentere rol kan spelen.

Financiële instellingen en hun beleidsbepalers doen er vanwege al het vorengaande goed aan zich terdege voor te bereiden op een (onaangekondigd) bezoek van de AFM. Als de AFM eenmaal op de stoep staat en inzage vordert in digitale gegevens zal er immers weinig tijd zijn om beslissingen te nemen, terwijl de consequenties van die beslissingen aanzienlijk kunnen zijn.

83 HR 4 april 2017, ECLI:NL:HR:2017:584, ECLI:NL:HR:2017:588 en ECLI:NL:HR:2017:592.
84 R.o. 2.7.2.
85 R.o. 2.8.
86 Volledig: Commissie modernisering opsporingsonderzoek in het digitale tijdperk.
87 Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 194.
88 *Kamerstukken II* 2018/19, 29279, nr. 501, p. 11.