



HOOGHIEMSTRA
&
PARTNERS
strategisch en juridisch advies

Controle van digitale gegevensdragers

Colofon

Hooghiemstra & Partners
Bezuidenhoutseweg 161
2594 AG Den Haag
www.hooghiemstra-en-partners.nl
info@hooghiemstra-en-partners.nl



Auteurs: Thijs Drouen, Christian Boxum, Lisanne Kramer, Ester Post, Anna Keuning
Opdrachtgever: WODC
Datum: 11 november 2024

Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum – uitgevoerd door Hooghiemstra & Partners, strategisch en juridisch adviesbureau op het raakvlak van data en recht, Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, en de Rijksuniversiteit Groningen.

Begeleidingscommissie:

Prof. mr. J.M ten Voorde (UL)
Prof. dr. ir. J. van den Berg (TU Delft & UL)
Dr. R. Henskens (Hogeschool Utrecht)
Dr. D.A.G. van Toor (UU)
Dr. ing. S. Zebregs (WODC)
Drs. R. Zuidema (JenV)

Voor de inhoud van het rapport zijn de onderzoekers verantwoordelijk. Het leveren van een bijdrage (als medewerker van een organisatie of als lid van de begeleidingscommissie) betekent niet automatisch dat de betrokkene instemt met de gehele inhoud van het rapport. Dat geldt eveneens voor het ministerie van Justitie en Veiligheid en zijn minister.

Inhoudsopgave

1. Aanleiding	5
1.1 Deelonderzoeken en onderzoeksvragen	6
1.2 Onderzoeksmethoden	7
1.3 Deelonderzoeken I en II	7
1.4 Deelonderzoek III	9
1.5 Leeswijzer	11
2. Introductie begrippen uit het onderzoek	12
2.1 Inleiding	12
2.2 De definitie van digitale gegevensdragers	12
2.3 Het delict dat centraal staat bij de oplegging van de controle	13
2.4 Algemene en bijzondere voorwaarden	15
3. Ontwikkelingen jurisprudentie Hoge Raad	18
3.1 Inleiding	18
3.2 Betekenis 'gedrag van de veroordeelde betreffende'	18
3.3 Inkadering van de bijzondere voorwaarde door de Hoge Raad	19
3.3.1 Welk kader kan uit de uitspraken van de Hoge Raad worden afgeleid?	28
3.4 Conclusie	30
4. Cijfermatige analyse jurisprudentie lagere rechtspraak	32
4.1 Inleiding	32
4.2 Algemene en specifieke formuleringen	33
4.3 Kenmerken van de algemeen geformuleerde bijzondere voorwaarden	35
4.3.1 Aanduiding voorwerp van controle	36
4.3.2 Een of twee specificerende elementen	37
4.3.3 Instanties belast met controle	37
4.3.4 Proeftijd	38
4.4 Kenmerken van specifiek geformuleerde bijzondere voorwaarden	39
4.4.1 Elementen die zien op de wijze van controle	39
4.4.2 Overkoepelende bevindingen wijze controle	41
4.4.3 Elementen die zien op de wijze van medewerking	42
4.4.4 Overkoepelende bevindingen wijze medewerking	44
4.4.5 Frequentie van de controle	45
4.4.6 Aanduiding voorwerp van controle	45
4.4.7 Instanties belast met de controle	46
4.4.8 Proeftijd	47
4.5 Conclusie	47
5. Controle van digitale gegevensdragers in de praktijk	49
5.1 Inleiding	49
5.2 Betrokken actoren	50
5.3 Ontstaan van de controle: INDIGO-afdoening van zedenzaken	54
5.4 Uitbreiding naar andere strafrechtelijke titels	55
5.5 Afspraken over de uitvoering van de controle	55
5.6 Nieuwe afspraken over de uitvoering van de controle	55

5.7	Controle van digitale gegevensdragers als bijzondere voorwaarde	56
5.8	De praktijk	57
5.9	Opvolging uitkomsten controle	59
5.10	Effectiviteit van de controle	60
5.11	Knelpunten in de praktijk	62
5.12	Stopzetting controle	64
5.13	Tijdelijke voorziening	64
5.14	Conclusie	65
6.	Grondrechten	66
6.1	Inleiding	66
6.2	Artikel 6 EVRM: het nemo tenetur-beginsel	66
6.2.1	Definitie nemo tenetur-beginsel	67
6.2.2	Ratio nemo tenetur-beginsel	67
6.2.3	Toetsing aan het nemo tenetur-beginsel	68
6.2.4	Nemo tenetur-beginsel en de controle van digitale gegevensdragers	74
6.3	Artikel 8 EVRM	76
6.3.1	Verhouding EVRM, EU-Handvest en de Grondwet	76
6.3.2	Toetsing aan artikel 8 EVRM	77
6.3.3	Reflectie	80
6.4	Toepasselijkheid AVG en Wjsg	81
6.4.1	Toepasselijkheid AVG en Wet politiegegevens bij inzet van de politie	82
6.5	Conclusie	83
7.	Verkenning uitbreiding controle naar andere delicten	86
7.1	Inleiding	86
7.2	Online terrorisme, extremisme en radicalisering	87
7.2.1	Aard van de delicten	87
7.2.2	Dadereigenschappen	88
7.2.3	De techniek	89
7.3	Cybercrime	90
7.3.1	Aard van de delicten	90
7.3.2	Dadereigenschappen	90
7.3.3	De techniek	91
7.4	Andere online seksuele delicten	92
7.4.1	Aard delicten	92
7.4.2	Eigenschappen daders	92
7.4.3	De techniek	93
7.5	Andere randvoorwaarden	93
7.6	Conclusie	93
8.	Bevindingen en aanbevelingen	95
8.1	Inleiding	95
8.2	Evaluatie oude werkwijze controle	95
8.3	Aanpassing/doorontwikkeling van de controle	99
8.3.1	Aanbevelingen procedurele en organisatorische randvoorwaarden	100
8.3.2	Aanbevelingen inhoud controle	101
8.4	Uitbreiding naar andere online delicten	103

Literatuurlijst	106
Bijlage I: De geschiedenis van de bijzondere voorwaarden	108
De geschiedenis van de voorwaardelijke straffen en bijzondere voorwaarden	108
Van de vrije hand naar meer rechtszekerheid	109
Verruiming van de proeftijd c.q. duur	110
Bijlage II: Respondentenlijst	112

1. Aanleiding

In ongeveer 300 gevallen per jaar legt de rechter aan een veroordeelde van online seksueel misbruik een voorwaardelijke straf op met als bijzondere voorwaarde een controle van zijn digitale gegevensdragers.¹ De Reclassering is op grond van artikel 14c, zesde lid, van het Wetboek van Strafrecht (Sr) belast met het toezicht op de bijzondere voorwaarden en dient veroordeelden daarbij te ondersteunen en te begeleiden, indien de rechter reclasseringstoezicht oplegt. Aangezien de controle van digitale gegevensdragers technische expertise vereist, en de politie de benodigde kennis hiervoor heeft opgebouwd ten tijde van het INDIGO-project, voerde de politie tot medio 2023 de controle uit ten behoeve van de Reclassering door met een reclasseringsmedewerker mee te gaan tijdens een huisbezoek.²

Bij zowel de politie als de Reclassering bestaat al enige jaren de wens om de controle anders vorm te geven, omdat hierbij verschillende knelpunten worden ervaren. De politie heeft zelfs de wens geuit om te stoppen met de controle omdat door capaciteitstekort en het oplopende aantal opgelegde controles, geen toereikende invulling aan de controles kan worden gegeven. Daarnaast ziet de politie het ook niet als haar taak de controle uit te voeren. Bovendien kunnen hierbij opsporings- en toezichtstaken door elkaar heen gaan lopen. Ten slotte is in de Veiligheidsagenda 2023-2026 bepaald dat de politie zich op het gebied van online misbruik moet inzetten op een zo groot mogelijk maatschappelijk effect, waarbij interventies met name gericht zijn op vervaardigers, misbruikers en *keyplayers* in netwerken rond seksuele uitbuiting. De controle past niet goed bij deze prioritering, omdat hier meestal sprake is van *low level offenders*.³

De Reclassering adviseerde in een brief aan het Ministerie van Justitie en Veiligheid (JenV) een wetswijziging te verkennen, omdat – gelet op verschillende arresten van de Hoge Raad – zorgen bestonden of de controle juridisch gezien toelaatbaar was. Daarnaast liep de Reclassering tegen uitvoeringsproblemen aan.

De Minister voor Rechtsbescherming informeerde de Tweede Kamer bij brief van februari 2024 dat de politie vanaf de zomer van 2023 weinig tot geen ruimte in capaciteit zag om bijstand te verlenen aan de Reclassering en sindsdien geen controles meer uitvoert.⁴ Aangegeven is dat gewerkt wordt aan een tijdelijke voorziening door de Reclassering. Het idee van de tijdelijke voorziening is dat de Reclassering de controle doorontwikkelt en dat de politie de Reclassering op technisch vlak opleidt om de controle zelfstandig uit te kunnen voeren. Het is de bedoeling dat de Reclassering vanaf 2025 de doorontwikkelde controle gaat uitvoeren, waarbij de politie niet langer betrokken is.

Naar aanleiding van de gesignaleerde knelpunten en wensen tot verandering, is besloten om in opdracht van het WODC een onderzoek te laten uitvoeren om de (oude) werkwijze te evalueren en te bekijken hoe de controle kan worden doorontwikkeld. Daarnaast bestaat in de praktijk een groeiende behoefte om in het Reclasseringstoezicht beter zicht te krijgen op online gedrag bij andere delicten. Daarom is besloten een verkenning uit te voeren naar mogelijke toepassing van de doorontwikkelde controle bij andere online delicten.

¹ Startnotitie WODC-onderzoek controle van digitale gegevensdragers, oktober 2022.

² INDIGO is het project waar de controle is ontstaan. A. van Wijk e.a. Niet meer doen. Een onderzoek naar de INDIGO-afdoening, Den Haag, 2019.

³ Veiligheidsagenda politie 2023-2026.

⁴ Kamerstukken II, 2023/2024, 29270, nr. 156.

1.1 Deelonderzoeken en onderzoeksvragen

Het onderzoek bestaat uit drie deelonderzoeken.

I: Een evaluatie van de oude controle

II: Een onderzoek naar de doorontwikkeling van de controle

III: Een verkenning naar de uitbreiding van een doorontwikkelde controle naar andere online delicten.

Hiervoor zijn de volgende onderzoeksvragen geformuleerd.

I: Evaluatie oude controle

1. Wat zijn, mede gelet op de recente jurisprudentie, de juridische kaders waaraan controles van online gedrag betreffende seksueel kindermisbruik moeten voldoen?
2. Wat houden de controles van digitale gegevensdragers in de praktijk in en welke actoren zijn daarbij betrokken?
3. Zijn de controles in de huidige vorm in overeenstemming met de geldende juridische kaders?
4. Hoe verhouden de controles in de huidige vorm zich tot het werk van de Reclassering?
5. In hoeverre kan met de huidige controlemethodes inzicht worden gekregen in online gedrag betreffende seksueel kindermisbruik en hoe effectief zijn de controles?
6. Welke waarborgen worden getroffen om de inbreuk op de persoonlijke levenssfeer van de onder toezicht gestelde zoveel mogelijk te beperken?

II: Aanpassen/doorontwikkeling controle

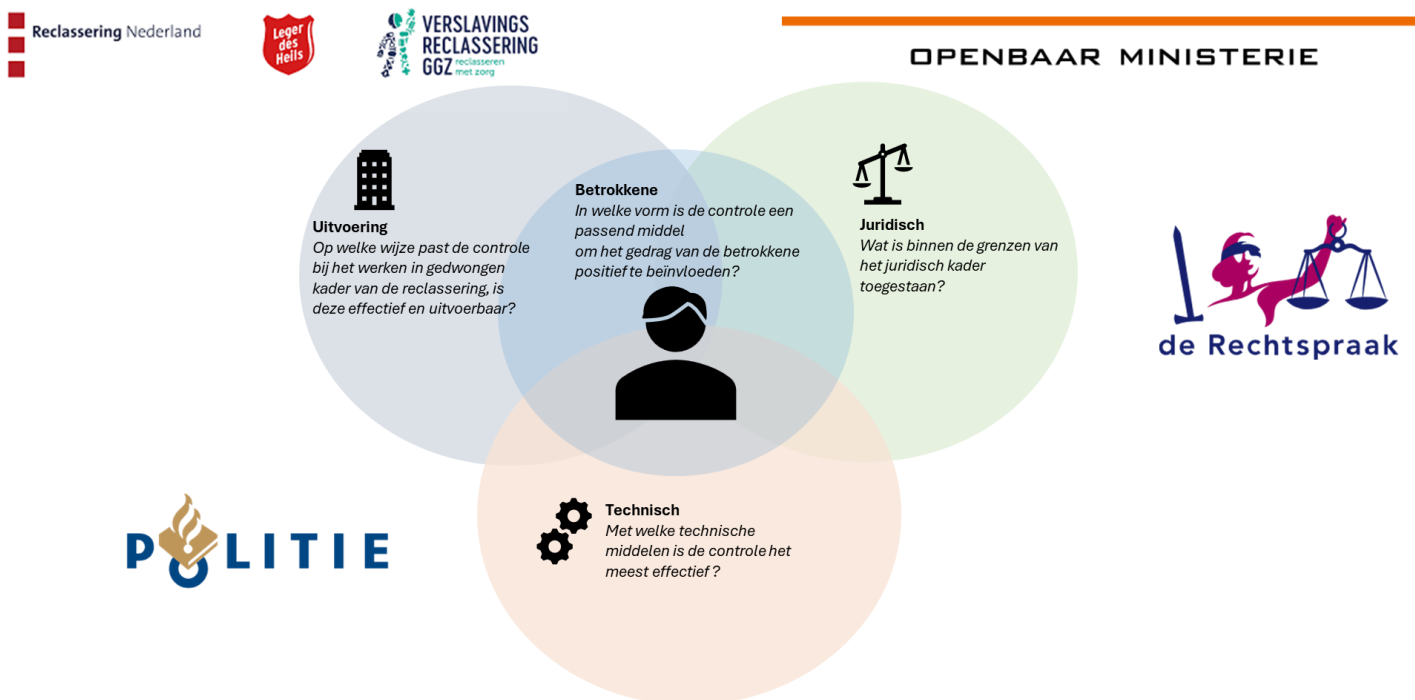
7. Indien de controles van digitale gegevensdragers in hun huidige vorm niet voldoen aan de juridische kaders, wat is nodig om deze wel in overeenstemming te brengen met de geldende juridische kaders?
8. Wat is er nodig om de controle van digitale gegevensdragers zo vorm te geven dat adequaat inzicht wordt verkregen in online gedrag betreffende seksueel kindermisbruik?
9. Hoe kunnen de controles van digitale gegevensdragers beter aansluiten bij het werk van de Reclassering?
10. Op welke wijze kunnen de controles van digitale gegevensdragers worden ingericht dat wordt voldaan aan (belangrijkste) vereisten die naar voren komen bij de beantwoording van de vragen 7, 8 en 9?

III: Uitbreiding naar andere online delicten

11. Kan de nieuw voorgestelde controle-methodiek in aangepaste vorm worden toegepast bij andere soorten online delicten, zoals andere seksuele delicten, cybercrime en delicten op het terrein van terrorisme, extremisme en radicalisering?
12. In hoeverre zijn er verschillen tussen deze soorten delicten waarmee rekening moet worden gehouden?

1.2 Onderzoeksmethoden

Het onderzoek is uitgevoerd door met verschillende, met elkaar samenhangende 'lenzen' te werken en steeds te reflecteren op de inzichten die deze lenzen bieden. Het gaat daarbij om de juridische lens, de lens van de uitvoering (in bijzonder die van de Reclassering) en de technische lens. In het midden van deze verschillende lenzen staat de betrokkene die de controle ondergaat, waarbij het gedragsperspectief van belang is. Elke betrokken actor heeft vanuit zijn organisatie expertise om invulling te geven aan een of meerdere van deze lenzen. In de plaat zijn deze betrokken actoren zoveel mogelijk bij deze betreffende lenzen neergezet. Deze kennis is gecombineerd om zo tot een evaluatie van de controle en advies over doorontwikkeling en uitbreiding te kunnen komen, die recht doet aan al deze perspectieven.



Figuur 1. De lenzen en betrokken actoren

1.3 Deelonderzoeken I en II

Bureauonderzoek

Er is gestart met een bureauonderzoek naar de relevante juridische kaders, om te bekijken aan welke wet- en regelgeving en jurisprudentie de uitvoering van de controle is gebonden, waar de grenzen liggen van wat wel en niet is toegestaan, welke bevoegdheden de betrokken partijen hebben in de uitvoering van de controle en wat de taak en werking van de Reclassering is. De volgende wet- en regelgeving is hiervoor bestudeerd:

- het algemene kader voor het opleggen van een bijzondere voorwaarden en het toezicht daarop (Sr en Wetboek van Strafvordering);
- de mensenrechten die in het kader van de controle een rol spelen, te weten het nemo tenetur-beginsel (artikel 6 Europees Verdrag voor de Rechten van de Mens (EVRM));
- het recht op de persoonlijke levenssfeer (artikel 8 EVRM);

- de bescherming van persoonsgegevens (de Algemene Verordening Gegevensbescherming (de AVG), de Wet politie politiegegevens (Wpg), en de Wet justitiële en strafvorderlijke gegevens (Wjsg);
- de taken en bevoegdheden van de Reclassering (de Reclasseringsregeling 1995), het beleidskader van de Reclassering, en de werkafspraken tussen openbaar ministerie, politie en Reclassering.

Cijfermatige analyse jurisprudentie lagere rechtspraak

Om te onderzoeken hoe lagere rechters de bijzondere voorwaarde formuleren en hoe de bijzondere voorwaarde zich door de jaren heen heeft ontwikkeld, is een jurisprudentieanalyse uitgevoerd, waarbij door middel van een zoekopdracht op rechtspraak.nl alle zoekresultaten op relevantie zijn beoordeeld en per jaar zijn geïnventariseerd, waarna de kenmerken van elke bijzondere voorwaarde zijn gescoord. Ten slotte wordt een link gelegd met de jurisprudentie van de Hoge Raad, door te analyseren op welke wijze deze jurisprudentie invloed heeft gehad op de ontwikkelingen in de lagere rechtspraak. Meer over de aanpak is te lezen in Hoofdstuk 4.

Oriënterende gesprekken

Om een eerste beeld te krijgen van de problematiek en om zicht te krijgen op de te houden interviews, zijn oriënterende gesprekken gevoerd met medewerkers van zowel de Reclassering, het openbaar ministerie als de Nationale Politie (hierna: politie). Deze gesprekken bleken daarnaast bruikbaar om al de nodige inhoudelijke input te verkrijgen over de praktijk.

Interviews

In totaal zijn er 15 interviews gehouden. In eerste instantie is met alle betrokken partijen bij de controle gesproken (Reclassering, politie, openbaar ministerie, rechtspraak, advocatuur). Tijdens die interviews is met de uitvoerende partijen van de controle (politie en Reclassering) aan bod gekomen hoe de controle verliep, tegen welke knelpunten werd aangelopen en hoe de organisatie tegen doorontwikkeling van de controle aankijkt. Met de Reclassering is stilgestaan bij het doel en werkwijze van deze organisatie en op welke wijze een doorontwikkelde controle bij de organisatie zou kunnen passen.

Hoewel het openbaar ministerie op meer afstand staat van de uitvoering van de controle, is de organisatie bevraagd op het verloop van het proces in de praktijk vanuit het oogpunt van deze organisatie, de gesignaleerde knelpunten, hun eigen rol, en hoe de organisatie aankijkt tegen doorontwikkeling. Met de advocatuur is gesproken over de verdediging met betrekking tot de oplegging van de controle, hoe wordt aangekeken tegen de controle gelet op de rechten van de betrokkene en het type daders dat het delict begaat. Ten slotte is met de rechtspraak gesproken over de rol van de rechter bij de oplegging van de bijzondere voorwaarde, over de arresten van de Hoge Raad en hun betekenis voor de lagere rechtspraak en de praktijk, hoe het formuleren van een bijzondere voorwaarde in zijn werk gaat, en over de mogelijke redenen voor de grote variatie in de formulering van de bijzondere voorwaarde.

Omdat in de praktijk weinig controles werden uitgevoerd was het niet mogelijk om binnen de onderzoeksperiode met een of meerdere zedendelinquent te spreken. Bovendien zou het voor de representativiteit van die interviews noodzakelijk zijn een andere onderzoeksmethode, zoals een enquête, te gebruiken. Gelet op de aard en de omvang van de doelgroep werd dit niet passend geacht. Ook zouden zij weinig input kunnen geven op de onderzoeksvragen die centraal staan in het onderzoek.

Daarnaast is met experts gesproken om een verdiepingsslag te kunnen maken op een bepaalde lens. Op het gebied van gedragsverandering van de betrokkene en de vraag hoe effectief een dergelijke interventie kan zijn, hebben we de opgehaalde inzichten vanuit de praktijk verrijkt door te spreken

met een GZ-psycholoog en een onderzoeker werkzaam bij de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen.

Ten slotte is met een universitair hoofddocent strafrecht en een hoogleraar staats- en bestuursrecht gesproken met als doel uit de juridische analyse opgehaalde inzichten op het gebied van de artikelen 6 en 8 EVRM te toetsen en aan te scherpen.

De bij de experts opgehaalde inzichten zijn gebruikt om de opbrengst van de interviews met betrokken partijen nader te duiden en om bepaalde zaken die uit het bureauonderzoek te toetsen. Voorafgaand aan elk interview ontving de desbetreffende gesprekspartner een gespreksagenda met de interviewvragen zodat deze zich goed kon voorbereiden op het interview. De interviews zijn afgenomen aan de hand van een semigestructureerde vragenlijst. Van alle interviews zijn schriftelijke verslagen gemaakt. Deze zijn voorgelegd aan de gesprekspartners en door hen geaccordeerd.

Demonstratie politie

De politie heeft de software die wordt gebruikt om de controle uit te voeren aan ons gedemonstreerd, om op die manier inzicht te krijgen in de technische uitvoering van de controle, de precieze inhoud van de controle, welke gegevens daarbij worden verwerkt en wat de software wel en niet kan. Getoond is hoe deze software in technische zin werkt, op welke wijze(n) de software inzicht kan geven in de digitale gegevensdragers en waar de beperkingen liggen. Ook zijn vragen van de onderzoekers over de software door de politie beantwoord.

Focusgroep

Enkele van de opgehaalde inzichten vanuit het bureauonderzoek en de interviews en de hoofdlijnen van het juridisch kader zijn besproken in een focusgroep waar het openbaar ministerie, de politie en de Reclassering aan hebben deelgenomen. Zo zijn de hoofdlijnen van de arresten van de Hoge Raad besproken en wat dit betekent voor de praktijk. Daarnaast is een discussie gevoerd over de oude werkwijze bij de controle in relatie tot het doel van de bijzondere voorwaarde en de taak van de Reclassering. Op die manier zijn inzichten getoetst en waar nodig bijgesteld. Hierbij waren twee deelnemers van de politie aanwezig, een van het openbaar ministerie en vijf van de Reclassering.

1.4 Deelonderzoek III

Selectie categorieën delicten en dadereigenschappen

In het laatste deelonderzoek is een verkenning gedaan naar de mogelijkheden van een aangepaste controle voor andere soorten delicten die online worden gepleegd of een online component hebben. Hiervoor is een aantal categorieën online delicten geselecteerd om te bekijken in hoeverre deze categorieën delicten verschillen van het delict dat centraal staat in dit onderzoek, met het oog op de vraag of er potentie zit in uitbreiding van de controle van digitale gegevensdragers. Om deze potentie te verkennen zijn de eerder beschreven lenzen gehanteerd. Voor de selectie van de categorieën delicten is aangesloten bij de categorieën die in de uitvraag van het WODC zijn benoemd.

Allereerst is verkend wat de aard van het type delict is en van het online gedrag dat daarmee verband houdt. Daarbij is ingeschat of het haalbaar is het verboden online gedrag voldoende nauwkeurig te omschrijven in een bijzondere voorwaarde. Dat is mede van belang voor de vraag in hoeverre het online gedrag te controleren is, en daarmee of de controle van de digitale gegevensdrager technisch haalbaar en uitvoerbaar is.

Daarnaast zijn twee dadereigenschappen van deze categorieën delicten verkend, en is beoordeeld hoe deze verschillen van de plegers van online seksueel misbruik. De geselecteerde eigenschappen zijn van belang zijn voor beantwoording van de vraag of en in hoeverre de controle effectief, uitvoerbaar en technisch haalbaar kan zijn. Het gaat om de bereidwilligheid om het gedrag te veranderen en de kennis/expertise om de online gedragingen af te schermen.

Bij deze verkenning zijn tevens inzichten uit de deelonderzoeken I en II meegenomen.

Interviews

Inzichten zijn opgehaald aan de hand van de eerder beschreven interviews met de betrokken partijen uit de strafrechtketen (het openbaar ministerie, de rechtspraak en de Reclassering). Aan deze partijen is gevraagd hoe zij aankijken tegen een doorontwikkeling op de geselecteerde categorieën delicten, of zij daar een toekomst voor zien en met welke aandachtspunten wat betreft de aard van de delicten en de eigenschappen van de daders rekening gehouden moet worden. Daarnaast is een aantal aparte interviews gevoerd. Zo is met een analist van de AIVD, gespecialiseerd in online terrorisme en extremisme, gesproken om meer inzicht te krijgen in de eigenschappen van deze dadergroepen. Ten slotte is gesproken met twee medewerkers van de Reclassering die ervaring hebben met de controle bij online terrorisme, extremisme en radicalisering. Deze inzichten zijn verwerkt in Hoofdstuk 7.

1.5 Leeswijzer

In hoofdstukken 2 tot en met 7 werken we toe naar de uitkomsten van de drie deelonderzoeken die centraal staan in dit rapport: de evaluatie van de oude werkwijze bij de controle, een advies over de doorontwikkeling van de controle en een verkenning naar een mogelijke uitbreiding van de controle voor andere online delicten. Dat doen we als volgt.

Het zwaartepunt van het onderzoek ligt bij de evaluatie en het advies over de doorontwikkeling. De relevante informatie die nodig is voor de evaluatie van de oude werkwijze en voor een advies over de doorontwikkeling betreft het juridisch kader, de betrokken actoren (in het bijzonder de taak van de Reclassering), de uitvoering van de controle in de praktijk (zowel procesmatig als technisch) en de kenmerken die de effectiviteit van de controle bepalen. Deze onderwerpen komen aan bod in hoofdstukken 2 tot en met 6.

In hoofdstuk 2 beginnen we met een introductie van de juridische begrippen. Daarna volgen de ontwikkelingen in de jurisprudentie van de Hoge Raad (hoofdstuk 3) en de ontwikkelingen in de lagere rechtspraak door middel van een analyse (hoofdstuk 4). In hoofdstuk 5 beschrijven we de betrokken actoren en hun taken, de uitvoering van de controle in de praktijk en de kenmerken van effectiviteit. In hoofdstuk 6 toetsen we de praktijk aan de relevante grondrechten (artikel 6 en 8 EVRM). Vervolgens komt de opgehaalde informatie samen in hoofdstuk 8, waarin we de onderzochte praktijk toetsen aan het juridisch kader, aan de taak van de Reclassering en aan enkele kenmerken van effectiviteit. Op basis van deze evaluatie geven we vervolgens een advies over de doorontwikkeling van de controle.

Het derde deelonderzoek neemt een kleiner deel van het rapport in beslag, aangezien het om een eerste verkenning gaat. Per type online delict worden in hoofdstuk 7 de relevante gezichtspunten voor nader onderzoek beschreven. In hoofdstuk 8 geven we op basis van deze gezichtspunten een eerste doorkijkje naar de mogelijkheden om de controle uit te breiden.

2. Introductie begrippen uit het onderzoek

2.1 Inleiding

In dit rapport staat de controle van digitale gegevensdragers bij online seksueel kindermisbruik centraal. Maar wat zijn digitale gegevensdragers? En wat wordt in de context van dit onderzoek bedoeld met online seksueel kindermisbruik? Voor een goed begrip zetten we in dit hoofdstuk een aantal begrippen op een rij, leggen we uit waarom we kiezen voor het gebruik van bepaalde termen in het rapport en hoe deze termen in de praktijk gebruikt worden. Allereerst staan we stil bij de definitie van digitale gegevensdragers. Daarna gaan we in op het delict dat centraal staat in dit onderzoek. Ten slotte gaan we in op de betekenis van algemene en bijzondere voorwaarden.

2.2 De definitie van digitale gegevensdragers

Hoewel er momenteel nog geen wettelijke definitie is van ‘digitale gegevensdragers’, is in de literatuur wel aandacht besteed aan de omschrijving van dit begrip. Gegevens worden in het Wetboek van Strafrecht (Sr) wel gedefinieerd. Het gaat om:

Iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdacht, interpretatie of verwerking door personen of geautomatiseerde werken.

Van Hurk en De Vries leggen uit dat de term ‘digitale gegevens’ betekent dat de gegevens op een digitale manier worden weergegeven, in bits en bytes, met gebruik van het binaire stelsel.⁵ Zij wijzen erop dat – hoewel bits een zeer geschikte vorm hebben om elektronisch⁶ te worden opgeslagen – dit geen vereiste is. De ‘drager’ van binaire gegevens kan ook papier zijn. Digitale gegevens zijn daarmee mediumonafhankelijk. Doorgaans zal echter de meest voorkomende drager een elektronische zijn, wat mogelijk verklaart waarom de term ‘elektronische gegevensdrager’ ook terugkomt in de rechtspraak.⁷

Een digitale gegevensdrager staat niet gelijk aan een ‘geautomatiseerd werk’, zoals een computer. De term digitale gegevensdrager heeft betrekking op het medium waarop de digitale gegevens zijn opgeslagen, zoals een SSD-kaart, een USB-stick of een harde schijf. De gegevens op deze gegevensdragers kunnen worden overgedragen, geïnterpreteerd of verwerkt worden door ‘geautomatiseerde werken’, zoals computers en smartphones. Geautomatiseerde werken worden door artikel 80sexies Wetboek van Strafrecht als volgt gedefinieerd:

Onder geautomatiseerd werk wordt verstaan een apparaat of groep onderling verbonden of samenhangende apparaten, waarvan een of meer op basis van een programma automatisch computergegevens verwerken.

In het wetsvoorstel voor het nieuwe Wetboek van Strafvordering is in artikel 2.2.1 een begripsomschrijving van digitale gegevensdrager opgenomen die aansluit op de hiervoor genoemde beschrijvingen:

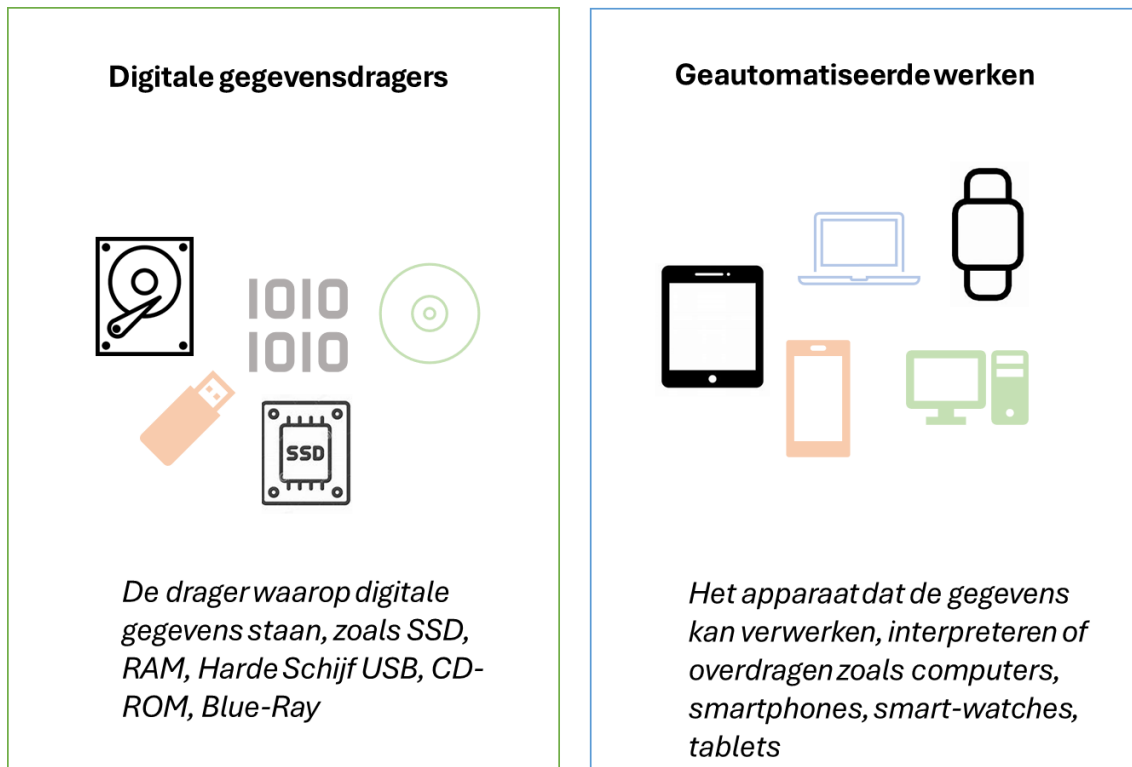
⁵ De Van Dale definieert binair als: tweevoudig, tweeledig, zich in tweeën verdelend. Het binair stelsel is een tweeledig talstelsel. Een binair cijfer is een nul of een één in het binaire stelsel.

⁶ In het kader van dit onderzoek beschouwen en gebruiken wij ‘elektronisch’ en ‘digitaal’ als synoniemen van elkaar.

⁷ Van Den Hurk & De Vries, *Onderzoek aan digitale-gegevensdragers. Een technische en juridische verkenning*, Wolters Kluwer, Deventer: 2021, p. 3-4.

*een gegevensdrager, niet zijnde een geautomatiseerd werk, bestemd of mede bestemd voor de opslag van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door geautomatiseerde werken.*⁸

Dit maakt het aannemelijk dat in de toekomst deze definitie ook in het strafrecht wordt gehanteerd. Om die reden hebben we deze definitie bij dit onderzoek gebruikt.



Figuur 2. weergave digitale gegevensdragers en geautomatiseerde werken

Opgemerkt moet worden dat uit de interviews met de Reclassering, politie en de rechtspraak de 'digitale gegevensdrager' en het 'geautomatiseerde werk' vaak met elkaar vereenzelvigd worden. Hoewel dat technisch gezien niet klopt, is het begrijpelijk, omdat digitale gegevensdragers in steeds mindere mate als 'losstaand object' zichtbaar zijn (zoals bij een USB-stick of een CD-ROM), maar geïntegreerd zijn in het geautomatiseerde werk. Dat maakt dat de 'digitale gegevensdrager' letterlijk moeilijk te onderscheiden is van het 'geautomatiseerde werk'.

2.3 Het delict dat centraal staat bij de oplegging van de controle

In principe kan de controle van digitale gegevensdragers als bijzondere voorwaarde opgelegd worden bij alle delicten waarbij sprake is van online seksueel kindermisbruik. Het gaat dan om de delicten die zijn opgenomen in de artikel 151e Sr (voorheen artikel 240a), artikel 251, eerste lid, onderdeel c, (voorheen 248e) Sr en artikel 252 (voorheen artikel 240b).

- **Artikel 151e Sr** stelt het tonen/verstrekken/aanbieden van schadelijk beeldmateriaal aan minderjarigen beneden de leeftijd van zestien jaar strafbaar;

⁸ Kamerstukken II 2022/2023, 36327, nr. 2, p. 44.

- **Artikel 251, eerste lid, onderdeel c, Sr** stelt het voorstellen van een ontmoeting met kinderen beneden de leeftijd van zestien jaar voor seksuele doeleinden strafbaar, maar alleen indien de pleger enige handeling onderneemt tot verwezenlijking van een ontmoeting (*grooming*).
- **Artikel 252 Sr** stelt het verspreiden, aanbieden, openlijk tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren, verwerven en bezitten of daartoe toegang verschaffen van pornografisch materiaal van minderjarigen (personen onder achttien jaar) strafbaar;

Uit de jurisprudentieanalyse (zie hoofdstuk 4.) en de praktijk is gebleken dat de controle in het overgrote deel van de gevallen wordt opgelegd bij het delict van artikel 252 Sr. Daarom hebben we ervoor gekozen om ons bij de online misbruikzaken te richten op artikel 252 Sr, met daarbij in het achterhoofd dat de controle in theorie ook voor grooming en het vertonen van schadelijk materiaal aan minderjarigen opgelegd kan worden.

Zowel in de rechtspraak als in de strafrechtketen wordt voor het duiden van de controle en het delict vastgehouden aan de termen ‘kinderporno’, ‘kinderpornografisch materiaal’, of afgekort tot ‘kp’. Men gebruikt niet de ‘modernere’ term ‘*sexual child abuse material*’ (materiaal van seksueel misbruik van kinderen/materiaal van seksuele uitbuiting van kinderen), hoewel dat wel de term is die volgens internationale organisaties moet worden gehanteerd.⁹ De reden om niet te spreken van ‘pornografie’, is dat deze term geen recht doet aan de ernst van de situatie en het slachtofferschap.¹⁰ Daarom is er in dit onderzoek voor gekozen om niet aan te sluiten bij de (belevingswereld van) de praktijk, maar bij de ‘modernere term’ materiaal van seksuele uitbuiting van kinderen, tenzij de termen ‘kinderporno’ of ‘kinderpornografisch materiaal’ in de onderzochte jurisprudentie worden gebruikt of in de geciteerde arresten van de Hoge Raad en literatuur worden aangehaald.

De bredere term ‘materiaal’ heeft de voorkeur boven ‘afbeeldingen’, omdat met de term ‘afbeeldingen’ andere vormen van materiaal (onbedoeld) worden uitgesloten, zoals videomateriaal. Daarnaast hebben we ervoor gekozen om te spreken van ‘seksuele uitbuiting’ en niet van ‘seksueel misbruik’. Reden hiervoor is dat hetgeen strafbaar is gesteld in artikel 252 Sr niet alleen materiaal van seksueel misbruik met kinderen betreft. Het gaat ook om materiaal dat kinderen seksualiseert en uitbuit, hoewel het materiaal niet expliciet het seksuele misbruik van het kind afbeeldt. Daarom is de bredere definitie van ‘seksuele uitbuiting’, waaronder zowel het misbruik, de seksualisering en uitbuiting vallen, passender.¹¹

Ten behoeve van de leesbaarheid wordt in een deel van de teksten verwezen naar ‘een delict als bedoeld in artikel 252 Sr’, of ‘plegers/daders van een delict als bedoeld in artikel 252 Sr’.

⁹ Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse Adopted by the Interagency Working Group in Luxembourg, 28 Januari 2016; ECPAT en Terre des Hommes, *Terminologiegids voor de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik*, februari 2022, p. 60.

¹⁰ Kritiek op deze term vloeit voort uit het feit dat ‘pornografie’ steeds meer genormaliseerd wordt en (al dan niet opzettelijk) bijdraagt om de ernst van seksueel misbruik en/of seksuele uitbuiting van kinderen te verminderen, te bagatelliseren of zelfs te legitimeren.

¹¹ ECPAT en Terre des Hommes, *Terminologiegids voor de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik*, februari 2022, p. 59.

De Wet seksuele misdrijven (WSM) is op 1 juli 2024 in werking getreden en brengt aanzienlijke veranderingen met zich mee ten aanzien van het aantal strafbare online seksuele delicten. Dat heeft te maken met twee belangrijke wijzigingen:

- Het Wetboek van Strafrecht vereiste voor veelvoorkomende zedendelictsvormen dat betrokkenen in elkaars aanwezigheid waren en dat er lichamelijk contact plaatsvond. Met de WSM worden online vormen van seksueel misbruik ook expliciet strafbaar gesteld. Denk hierbij aan het gedwongen verrichten van seksuele handelingen voor de webcam, aan *sextortion* en het op bestelling live streamen van kindermisbruik;
- Daarnaast stelt de WSM seksueel getint chatten met minderjarigen strafbaar. In tegenstelling tot grooming, is het daarbij niet noodzakelijk dat er sprake is van het ondernemen van stappen tot een ontmoeting.

De wetgever heeft de formulering van de strafbepalingen ‘techniekonafhankelijker’ gemaakt. De strafrechtelijke normstelling laat, zo wordt gesteld, ruimte voor maatschappelijke en technologische ontwikkelingen. Denkbaar is dat deze wetswijziging leidt tot een toename van opleggingen van de bijzondere voorwaarde die in dit onderzoek centraal staat. Hier gaan we in hoofdstuk 8. verder op in.

2.4 Algemene en bijzondere voorwaarden

Ten slotte is het van belang om enkele begrippen te duiden die verband houden met de juridische basis voor het opleggen van de controle van digitale gegevensdragers in het rechterlijk vonnis.

De rechter heeft – afhankelijk van de strafsoort en strafmaat – de optie om verschillende straffen op te leggen in geval van een veroordeling. Daarbij kan hij ervoor kiezen de straf (deels) voorwaardelijk op te leggen. We nemen in dit onderzoek de voorwaardelijke straf als uitgangspunt, maar het verbinden van voorwaarden is ook mogelijk voor andere strafrechtelijke titels, zoals bij tbs met voorwaarden en de voorwaardelijke invrijheidsstelling.

De algemene voorwaarde (artikel 14c, eerste lid, Sr)

De algemene voorwaarde volgt uit de wet en houdt in dat de verdachte zich niet schuldig maakt aan een strafbaar feit gedurende de proeftijd. De algemene voorwaarde valt volgens Bleichrodt alleen te begrijpen in verband met de dreiging van de tenuitvoerlegging van de voorwaardelijke straf. Het hoeft daarbij niet te gaan om een soortgelijk feit. De algemene voorwaarde ziet op ‘alle strafbare feiten’.¹²

De bijzondere voorwaarde (artikel 14c, tweede lid, Sr)

Een bijzondere voorwaarde is een gedragsvoorschrift dat de rechter kan opleggen met als doel het voorkomen van strafbaar gedrag. Bleichrodt wijst er in zijn proefschrift op dat met de bijzondere voorwaarde “met name [zou] moeten worden getracht herhaling van soortelijke delicten als het gepleegde te voorkomen veelal door druk op de veroordeelde uit te oefenen bepaalde risicovolle situaties te vermijden.”¹³ De wet kent een lijst met een aantal gedragsvoorwaarden die kunnen worden opgelegd, maar daarnaast wordt ruimte geboden om ‘andere voorwaarden, het gedrag van

¹² F.W. Bleichrodt, *Onder voorwaarde Een onderzoek naar de voorwaardelijke veroordeling en andere voorwaardelijke modaliteiten 1996*, p. 65; F.W. Bleichrodt & P.C. Vegter, *Sanctierecht*, 2021, p. 346.)

¹³ Bleichrodt 1996, p. 69

de veroordeelde betreffende' (artikel 14c, tweede lid, onder 14° Sr) op te leggen. Wat deze andere voorwaarden zijn wordt niet expliciet genoemd.

De bijzondere voorwaarden zien onder meer op het vergoeden van schade en het bijdragen aan het terugdringen van recidive in de tenuitvoerlegging van de straf of het toezicht. Als voorbeelden daarvan kunnen worden genoemd het verbod om verdovende middelen te gebruiken en om mee te werken aan een controle daarop, of opneming in een zorginstelling.

De voorwaarde die in dit onderzoek centraal staat, ziet ook op het terugdringen van recidive, maar levert, anders dan de andere voorwaarden die in artikel 14c, tweede lid, zijn opgesomd, bij schending ook – mogelijk – het vermoeden van een nieuw strafbaar feit op. In bijlage I bij dit rapport wordt nader ingegaan op de totstandkomingsgeschiedenis van de voorwaardelijke veroordeling en de mogelijkheid om daaraan bijzondere voorwaarden te verbinden. Op deze plaats is van belang om op te merken dat toen er in 2012 voor werd gekozen om bijzondere voorwaarden expliciet in de wet op te nemen, de voorwaarde die in dit onderzoek centraal staat, niet in de wet is opgenomen. De reden hiervoor is dat deze bijzondere voorwaarde waarschijnlijk nog niet door de rechter werd opgelegd.¹⁴

In de memorie van toelichting bij dat wetsvoorstel wordt over deze voorwaarde ook niet gesproken. Waar wel over gesproken wordt is de rol van de Reclassering en de mogelijke rol van de politie bij opgelegde voorwaarden. Daarbij wordt erop gewezen dat de Reclassering is belast met het toezicht op de naleving van de voorwaarden. Ook wordt gesteld dat de politie een belangrijke rol kan vervullen waarbij wordt gesteld dat de politie "uit hoofde van haar taken veelal een schending van de algemene voorwaarde [zich schuldig maken aan een strafbaar feit, toevoeging auteurs] zal kunnen constateren. Het is echter ook mogelijk dat bij de politie een schending van de bijzondere voorwaarde aan het licht komt, bijvoorbeeld bij overtreding van een locatieverbod." In het algemeen wordt gesteld dat vereist is dat de politie in bepaalde situaties op de hoogte wordt gesteld van bijzondere voorwaarden die zijn opgelegd en dat afspraken worden gemaakt tussen de reclassering en de politie over de controle hierop.

Zoals gezegd wordt in de memorie van toelichting niet verwezen naar de voorwaarde die centraal staat in dit onderzoek en is deze voorwaarde dus niet wettelijke verankerd. In de memorie van toelichting wordt wel benadrukt dat een wettelijk gespecificeerde bijzondere voorwaarde wordt gezien als een stimulans voor een succesvol toezicht, omdat het duidelijkheid geeft over de invulling van het toezicht. Het belang van een nadere omschrijving van de bijzondere voorwaarde wordt benadrukt onder verwijzing naar een arrest van de Hoge Raad¹⁵ waaruit afgeleid kan worden dat een bijzondere voorwaarde die een ingrijpende inbreuk pleegt op een verdragsrechtelijk beschermd recht van bewegingsvrijheid, een wettelijke grondslag dient te krijgen die voldoet aan de eisen van kenbaarheid en voorzienbaarheid.¹⁶

Voorwaarden die van rechtswege aan de bijzondere voorwaarden zijn verbonden (artikel 14c, derde lid, Sr)

In het geval dat de rechter ervoor kiest een bijzondere voorwaarde op te leggen, volgt uit de wet dat de betrokkene in elk geval moet meewerken:

- aan het nemen van een of meer vingerafdrukken of aan het inzage geven in een identiteitsbewijs;

¹⁴ J.W van den Hurk & S.J de Vries, Controle van zedendelinquenten: toezicht of opsporing? *NJB* 2020/571.

¹⁵ HR 25 november 2008, ECLI:NL:HR:2008:BF0836.

¹⁶ *Kamerstukken II*, 2009/10, 32 319, nr. 3. p. 4-7.

- aan het reclasseringstoezicht (inclusief medewerking aan huisbezoeken) en aan het zich melden bij de Reclassering zolang en zo vaak Reclassering dit noodzakelijk acht.

[Toezichtsoopdracht Reclassering \(artikel 14, zesde lid, Sr\)](#)

De rechter kan bepalen dat de Reclassering toezicht houdt op de naleving van de voorwaarden en de betrokkene hierbij begeleidt.

3. Ontwikkelingen jurisprudentie Hoge Raad

3.1 Inleiding

In het voorgaande hoofdstuk hebben we beschreven dat de rechter in geval van een voorwaardelijke veroordeling een bijzondere voorwaarde kan opleggen aan de veroordeelde. De controle van digitale gegevensdragers is een voorbeeld van zo'n bijzondere voorwaarde. Uit vooronderzoek weten we dat deze controle in elk geval vanaf 2012 door de rechter wordt opgelegd in zaken waarbij sprake is van materiaal van seksuele uitbuiting van kinderen.¹⁷ Vanaf 2016 heeft de Hoge Raad zich meermaals uitgelaten over de vraag binnen welke grenzen de rechter deze controle mag opleggen. De taak van de Hoge Raad als hoogste rechtsprekende instantie is om te beoordelen of de lagere rechter (een rechtbank of gerechtshof) het recht goed heeft toegepast. Daarmee zijn de arresten van de Hoge Raad een belangrijke bron voor de vraag aan welke juridische randvoorwaarden de controle van digitale gegevensdragers moeten voldoen. In dit hoofdstuk staan we stil bij deze rechtspraak van de Hoge Raad en bij het kader dat daaruit kan worden afgeleid voor het opleggen van de bijzondere voorwaarde van controle van digitale gegevensdragers. De ontwikkelingen in de jurisprudentie van de Hoge Raad zijn zowel van belang voor de evaluatie van de oude werkwijze van de controle als voor de doorontwikkeling ervan, omdat de jurisprudentie de grenzen waarbinnen de controle toelaatbaar is duidelijker zullen worden.

In dit hoofdstuk beantwoorden we het eerste deel van onderzoeksvraag 1, waar het gaat om het kader dat de Hoge Raad heeft gesteld. Deze vraag luidt:

1. Wat zijn, mede gelet op recente jurisprudentie, de juridische kaders waaraan controles van online gedrag betreffende seksueel kindermisbruik moeten voldoen?

Voordat we ingaan op de arresten van de Hoge Raad, staan we kort stil bij de inhoud van de bijzondere voorwaarde die de rechter kan opleggen op grond van artikel 14c, tweede lid, onder 14°, Sr. Daarna worden de arresten behandeld, waarbij ook wordt ingegaan op annotaties en wat over deze bijzondere voorwaarde is geschreven in de literatuur. Ten slotte beschrijven we het juridisch kader dat uit deze arresten is af te leiden.

3.2 Betekenis 'gedrag van de veroordeelde betreffende'

In paragraaf 0 zagen we dat de rechter, naast de bijzondere voorwaarden uit artikel 14c, tweede lid, Sr, 'andere voorwaarden, het gedrag van de veroordeelde betreffende' kan opleggen (14c, tweede lid, onder 14°, Sr). Omdat de wetgever 'het gedrag van de veroordeelde betreffende' nooit nader heeft gedefinieerd, bestaat nog steeds behoefte aan verduidelijking van de betekenis van deze bijzondere voorwaarde.

Uit jurisprudentie van de Hoge Raad volgt dat een voorwaarde 'het gedrag van de veroordeelde betreffende' kan worden aangemerkt als een voorwaarde die strekt ter bevordering van het goede levensgedrag van de veroordeelde of een gedraging betreft waartoe hij uit een oogpunt van maatschappelijke betamelijkheid gehouden is.¹⁸ In 2022 spoort Procureur-Generaal Bleichrodt de Hoge Raad aan de betekenis verder te verduidelijken. Volgens hem doet de maatstaf "maatschappelijke betamelijkheid" denken "aan het bepaalde in artikel 6:162 BW hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt", zo stelt hij in zijn conclusie

¹⁷ Zie hierover hoofdstuk 4.

¹⁸ HR 26 november 1986 NJ 1970/123, HR 23 februari 2016, ECLI:NL:HR:2016:302, HR 19 september 2017, ECLI:NL:HR:2017:2392, NJ 2017/389, HR 24 april 2018, ECLI:NL:HR:2018:667, NJ 2018/311 en HR 9 oktober 2018, ECLI:NL:HR:2018:1882, NJ 2019/252.

voorafgaande aan het arrest van de Hoge Raad van 31 mei 2022.¹⁹ Als het gaat om bijzondere voorwaarden kan worden gedacht aan fatsoensnormen die verplichten tot een gedraging naar aanleiding van een gepleegd delict en die een vorm van morele genoegdoening inhouden.²⁰ Bleichrodt geeft in zijn conclusie het advies om “voorwaarden het gedrag van de veroordeelde betreffende” te interpreteren als: “voorwaarden die strekken tot het voorkomen van strafbaar gedrag van de veroordeelde” of “die een gedraging betreffen waartoe hij uit een oogpunt van maatschappelijke betamelijkheid gehouden moet worden geacht.” Ook lijkt Bleichrodt een rol te zien voor de wetgever als het gaat om de vraag naar de reikwijdte van het reclasseringstoezicht, in het bijzonder ten aanzien van digitale gegevensdragers. Want dat is aan de hand van de huidige wettelijke regeling moeilijk te beantwoorden. “Gelet op de inbreuk op de persoonlijke levenssfeer die het onderzoek van gegevensdragers kan meebrengen, verdient het de voorkeur dat de wetgever bij de normering het voortouw neemt.”²¹

3.3 Inkadering van de bijzondere voorwaarde door de Hoge Raad

Hieronder bespreken we de relevante arresten die de Hoge Raad door de jaren heen heeft gewezen. Het gaat hierbij om zaken waarin een delict van artikel 252 (voorheen 240b) Sr is gepleegd en waaruit blijkt hoe de Hoge Raad het kader en de eisen waaraan de bijzondere voorwaarde van controle van digitale gegevensdragers moet voldoen, steeds verder heeft vormgegeven.

[HR 23 februari 2016, ECLI:NL:HR:2016:302](#)

De eerste uitspraak van de Hoge Raad over de voorwaarde van controle van digitale gegevensdragers betreft het arrest van 23 februari 2016.

De bijzondere voorwaarde die door het hof is opgelegd luidt dat:

“de verdachte gedurende de proeftijd zal meewerken aan politieke controles van zijn computer(s) en andere apparatuur waarop afbeeldingen (kunnen) zijn opgeslagen.”

Het middel klaagt over deze door het hof opgelegde bijzondere voorwaarde. Advocaat-Generaal Vegter stelt hierover in zijn conclusie: “De geformuleerde bijzondere voorwaarde onderscheidt niet helder tussen het gedrag dat moet worden bevorderd en de wijze waarop het toezicht (door politiecontrole) op de naleving plaatsvindt. Welk gedrag de rechter voor ogen heeft laat zich overigens betrekkelijk eenvoudig raden. In de gestelde bijzondere voorwaarde ligt namelijk besloten dat het te bevorderen levensgedrag is dat – heel kort geformuleerd – verdachte zich op welke wijze dan ook onthoudt van elke gedraging (waaronder de met name in art. 240b Sr vermelde gedragingen) met betrekking tot kinderporno. Dat is een voorwaarde die zonder meer is te rubriceren onder art. 14c tweede lid onder 14, Sr.”

In licht van het middel gaat het volgens Vegter vooral om de vraag of de wijze van toezicht, zoals de rechter voor ogen heeft gehad, ongeoorloofd is en met name om de vraag of het een te vergaande inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer is. “Formeel is het openbaar ministerie belast met het toezicht, maar de feitelijke uitvoering vindt in de praktijk plaats door de Reclassering en de politie.” Voor de Reclassering is dat bij wet voorzien, maar voor de politie niet. Volgens Vegter valt in het licht van de verhouding tussen het openbaar ministerie en de politie, en gelet op de taak van de politie, “aan te nemen dat het openbaar ministerie de politie de opdracht kan geven toezicht te houden.” Als het specifiek gaat om huisbezoeken in het kader van de uitvoering van het toezicht door de politie, ontberen huisbezoeken volgens Vegter weliswaar een

¹⁹ Conclusie PG, 22 februari 2022, ECLI:PHR:2022:170. We gaan hier verder op in, in paragraaf 3.3

²⁰ Conclusie PG, 22 februari 2022, ECLI:PHR:2022:170.

²¹ Conclusie PG, 22 februari 2022, ECLI:PHR:2022:170.

uitdrukkelijke wettelijke regeling, “maar ook daarvoor geldt dat ze inherent zijn aan het toezicht.” Alhoewel de bijzondere voorwaarde niet erg gelukkig is geformuleerd, snijdt het middel dat toezicht op de naleving van de voorwaarde door politiecontrole van computers en dergelijke een te vergaande inbreuk oplevert op grondrechten geen hout. Vegter concludeert tot verwerping van het middel.²²

De Hoge Raad vernietigde de bestreden uitspraak voor wat betreft de strafoplegging, onder verwijzing naar een arrest uit 1968.²³ In dat arrest is door de Hoge Raad bepaald dat het moet gaan om voorwaarden die strekken tot bevordering van het goede levensgedrag van de veroordeelde of gedragingen waartoe de veroordeelde vanuit het oogpunt van maatschappelijke betamelijkheid gehouden moet worden. Kennelijk had het hof, zo stelt de Hoge Raad in zijn arrest van 2016, weliswaar het oog op gedrag dat met (kort gezegd) kinderporno verband houdt, maar daartoe niet een voldoende precies gedragsvoorschrift geformuleerd. “Een bijzondere voorwaarde in de zin van artikel 14c, tweede lid, onder 14° Sr, kan niet geacht worden gedrag te omvatten dat in feite overeenkomt met het meewerken aan door de politie uit te oefenen dwangmiddelen op de veelomvattende en ingrijpende wijze zoals in de onderhavige voorwaarde is geformuleerd.”

Van den Hurk & De Vries komen in 2020 tot de conclusie dat het arrest van de Hoge Raad uit 2016 niet heeft geleid tot een eenduidige toepassing van het gedragsvoorschrift. Ook stellen zij dat het arrest minder effect heeft gehad op de rechtspraak dan verwacht. In hun bespreking van het arrest stellen zij dat de motivering van de Hoge Raad drie elementen bevat die tot de conclusie leiden dat de geformuleerde voorwaarde in strijd is met de daarvoor geldende maatstaven:

1) het gedragsvoorschrift is niet voldoende precies omschreven. Er wordt niet omschreven welk goed levensgedrag van de veroordeelde wordt verwacht. In een strafzaak die draait om gedragingen met kinderpornografisch materiaal zal voor de hand liggen dat het gewenste gedrag zal zijn dat de veroordeelde zich verder zal onthouden van gedragingen die verband houden met kinderpornografie;

2) het toezicht op de naleving is apart geregeld. De door het hof geformuleerde voorwaarde houdt in dat de veroordeelde dient mee te werken aan ‘politiecontroles’. Met een dergelijke formulering laat de rechter zich uit over de vraag welke instanties de controle moet uitvoeren, terwijl in art. 14d Sr is vastgesteld dat (formeel) het openbaar ministerie is belast met het toezicht op de naleving van de voorwaarde. In de praktijk wordt het toezicht door de Reclassering uitgeoefend;

3) het gedragsvoorschrift kan niet geacht worden gedrag te omvatten dat in feite neerkomt op het meewerken aan door de politie uit te oefenen dwangmiddelen op de veelomvattende en ingrijpende manier zoals in deze voorwaarde is geformuleerd. De auteurs stellen dat de Hoge Raad hiermee tot uitdrukking heeft willen brengen dat met deze formulering geen enkele begrenzing wordt gegeven aan het uitvoeren van een dergelijke (ingrijpende) controle, zodat sprake is van een meer dan geringe inbreuk op de grondrechten van de veroordeelde. Dat maakt de voorwaarde volgens de auteurs ook om die reden ontoelaatbaar.

Volgens Van den Hurk & De Vries kan uit de overweging van de Hoge Raad niet worden afgeleid dat een dergelijke controle niet is toegestaan. Het lijkt volgens hen mogelijk om een gedragsvoorschrift zodanig vorm te geven dat aan de hiervoor genoemde drie bezwaren in voldoende mate tegemoet kan worden gekomen.²⁴

²² PHR 1 december 2015, ECLI:NL:PHR:2015:2693; HR 26 november 1986 *NJ* 1970/123.

²³ HR 26 november 1968, ECLI:NL:HR:1968: AB6079, *NJ* 1970/123

²⁴ J.W van den Hurk & S.J de Vries, ‘Controle van zedendelinquenten: toezicht of opsporing?’, *NJB* 2020/571.

In zijn arrest van 7 juli 2020 buigt de Hoge Raad zich over de twee bijzondere voorwaarden:

“(i) Stelt als bijzondere voorwaarde dat de veroordeelde zich gedurende de proeftijd op welke wijze dan ook:

- onthoudt van het op digitale wijze met een seksuele intentie communiceren met minderjarigen/kinderen,
- zich onthoudt van gedragingen die zijn gericht op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen,
- zich onthoudt van gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met minderjarigen/kinderen wordt gecommuniceerd, terwijl het daarop uitgeoefende toezicht de afspraak omvat dat de veroordeelde geen wisprogramma's op zijn digitale apparatuur mag hebben of gebruiken.

(ii) Stelt als bijzondere voorwaarde dat de veroordeelde maximaal tweemaal per jaar in het kader van controle van zijn digitale gegevensdragers aan de reclassering en eventueel door de reclassering uitgenodigde politiemedewerkers de toegang verschaft tot zijn woning, waarbij de veroordeelde dan op verzoek van de reclassering, al zijn digitale gegevensdragers ter beschikking moet stellen dan wel overhandigen aan de reclassering- of politiemedewerkers. De veroordeelde moet de reclassering dan wel de door hen uitgenodigde politiemedewerkers de toegang verschaffen tot alle aanwezige digitale gegevensdragers, bijvoorbeeld door het geven van de benodigde wachtwoorden.”

De Hoge Raad verwijst in zijn arrest naar de hiervoor genoemde arresten uit 1968 en 2016 en stelt dat de geformuleerde voorwaarde onder (ii) niet aan de maatstaven voldoet: “Voor zover het hof met het formuleren van dit gedragsvoorschrift zou hebben beoogd het toezicht op de naleving van de onder (i) weergegeven bijzondere voorwaarde te regelen, heeft het hof dat niet voldoende duidelijk tot uitdrukking gebracht, terwijl het hof dan evenmin voldoende precies heeft geformuleerd dat het onderzoek aan de gegevensdragers – en het daarmee verbonden verlenen van toegang tot de woning en de gegevensdragers – beperkt dient te blijven tot dat toezicht op de naleving van die bijzondere voorwaarde en evenmin voldoende precies heeft geformuleerd op welke wijze dat onderzoek aan de gegevensdragers mag worden uitgevoerd en welke functionarissen daarbij de Reclassering (technische) ondersteuning mogen bieden, teneinde te waarborgen dat de persoonlijke levenssfeer van de verdachte niet meer dan nodig voor het beoogde toezicht wordt beperkt.” De zaak wordt teruggewezen naar het gerechtshof Den Haag.

Jörg gaat in zijn noot onder voornoemd arrest in op de vraag waar de grens ligt als het gaat om ‘andere voorwaarden het gedrag van de veroordeelde betreffende’. In de eerste plaats, zo stelt hij, moeten de opgelegde voorwaarden duidelijk, relevant en proportioneel zijn, terwijl de vervulling ervan geheel in de macht van de veroordeelde moet liggen. In de tweede plaats mogen de bijzondere voorwaarden niet komen op het terrein dat blijkens de toepasselijke regelgeving is voorbehouden aan een andere autoriteit. In de derde plaats, zo stelt Jörg, mag zonder afdoende wettelijke rugdekking geen bijzondere voorwaarde worden opgelegd die een grondrecht schendt. In de vierde plaats mogen bijzondere voorwaarden geen inbreuk maken op belangrijke rechtsbeginselen. Eén zo'n beginsel is, volgens Jörg, dat in het algemeen niemand hoeft mee te werken aan opsporingsonderzoek door de politie, wettelijke uitzonderingen daargelaten. Voornoemde auteur stelt onder verwijzing naar het hiervoor besproken arrest uit 2016 dat het antwoord van de Hoge Raad “klip en klaar” is. Jörg verwijst naar de “hybride positie van de Reclassering”: enerzijds is sprake van een vertrouwenspositie, maar anderzijds is de Reclassering een tot informatieverschaffing verplichte bron voor Justitie in het kader van de voorlichting aan de

rechter of van de tenuitvoerlegging van sancties. Volgens Jörg valt daaronder niet “het faciliteren van opsporingsonderzoek door de politie.”²⁵

[HR 9 maart 2021, ECLI:NL:HR:2021:248](#)

In het arrest dat de Hoge Raad op 9 maart 2021 heeft gewezen, staat de volgende bijzondere voorwaarde die het hof heeft geformuleerd centraal:

”dat de verdachte/veroordeelde: (...)

- gedurende de proeftijd mee zal werken aan gesprekken met de reclassering over:
- gedrag dat is gericht op een digitale omgeving waarin kinderpornografisch materiaal kan worden verkregen;
- gedrag dat is gericht op een digitale omgeving waarin over seksuele handelingen met minderjarigen wordt gecommuniceerd;
- en hoe hij denkt dit gedrag te voorkomen, in welk kader hij zal meewerken aan controles van digitale gegevensdragers door de politie.”

Verder heeft het hof het volgende beslist: “Geeft opdracht aan de reclassering tot het houden van toezicht op de naleving van voormelde bijzondere voorwaarden en verdachte/veroordeelde ten behoeve daarvan te begeleiden.”

De Hoge Raad verwijst ook in dit arrest naar het arrest van 1968 en het hiervoor besproken arrest van 7 juli 2020 en stelt dat de voorwaarde zoals door het hof geformuleerd niet voldoet aan de maatstaven uit voornoemde arresten. Meer specifiek stelt de Hoge Raad:

“De door het hof gestelde bijzondere voorwaarde is, voor zover deze behelst dat de verdachte/veroordeelde zal meewerken aan controles van digitale gegevensdragers door de politie, in strijd met artikel 14c lid 2, onder 14, Sr, omdat dit onderdeel niet voldoet aan de hiervoor onder 2.3.2 weergegeven maatstaven [in overweging 2.3.2 verwijst de Hoge Raad naar hetgeen overwogen in het hiervoor besproken arrest van de HR van 7 juli 2020, toevoeging auteurs]. In het bijzonder blijkt uit die voorwaarde niet hoe deze zich precies verhoudt met de in de bijzondere voorwaarde bedoelde gesprekken met de Reclassering. Ook blijkt daaruit niet met welke frequentie en op welke wijze de controles van de gegevensdragers mogen worden uitgevoerd, welke (politie)functionarissen daarbij betrokken mogen zijn en hoe is gewaarborgd dat de persoonlijke levenssfeer van de verdachte daarbij niet verdergaand wordt beperkt dan nodig is voor het beoogde toezicht.”

[HR 15 maart 2022, ECLI:NL:HR:2022:338](#)

In het arrest van de Hoge Raad van 15 maart 2022 wordt niet alleen de inhoud van de bijzondere voorwaarde ter discussie gesteld, maar ook de daaraan verbonden proeftijd van zes jaar.²⁶ Het eerste cassatiemiddel richt zich op de door het hof opgelegde proeftijd van zes jaar en het tweede middel klaagt over de opgelegde bijzondere voorwaarde dat de veroordeelde meewerkt aan controle van zijn digitale gegevensdragers tijdens een huisbezoek.

Voor wat betreft de opgelegde proeftijd oordeelt de Hoge Raad:

²⁵ HR 7 juli 2020, ECLI:NL:HR:2020:1215, *NJ* 2020/410 m.nt. N. Jorg.
²⁶ HR 15 maart 2022, ECLI:NL:HR:2022:338.

“Het hof heeft geoordeeld dat is voldaan aan de in artikel 14b, lid 2 Sr genoemde voorwaarde dat “er ernstig rekening mee moet worden gehouden dat de veroordeelde wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen.” Dat oordeel is volgens de Hoge Raad niet begrijpelijk “aangezien het hof geen feiten en omstandigheden heeft vastgesteld waaruit gedragingen van de verdachte kunnen worden afgeleid die onmiskenbaar zijn gericht tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen in de zin van artikel 14b lid 2 Sr, terwijl de misdrijven waaronder het bewezenverklaarde is gekwalificeerd (kort gezegd: een gewoonte maken van het in het bezit hebben van kinderporno en het verspreiden en aanbieden van kinderporno) ook niet zonder meer kunnen worden gekarakteriseerd als misdrijven die dergelijke gedragingen omvatten (vgl. HR 12 juni 2018, ECLI:NL:HR:2018:894). Het cassatiemiddel is terecht voorgesteld.”

Als het gaat om de geformuleerde bijzondere voorwaarde overweegt de Hoge Raad:

“Op grond van artikel 14c lid 3, aanhef en onder b, Sr is aan het stellen van een bijzondere voorwaarde van rechtswege onder meer de voorwaarde verbonden dat de veroordeelde medewerking verleent aan het reclasseringstoezicht, bedoeld in het zesde lid van artikel 14c Sr. Daarnaast voorziet artikel 6:3:14 Sv in voorschriften en bevoegdheden in verband met het toezicht op de naleving van aan een voorwaardelijke veroordeling verbonden voorwaarden. Deze regelingen staan er niet aan in de weg dat - voor zover dat, gelet op de mogelijkheden die de zojuist genoemde wettelijke bepalingen al bieden, aangewezen is - een bijzondere voorwaarde als bedoeld in artikel 14c lid 2, onder 14°, Sr wordt gesteld die een gedraging van de veroordeelde betreft en die ertoe strekt het toezicht op (een) andere door de rechter op grond van artikel 14c lid 2 Sr gestelde bijzondere voorwaarde(n) mogelijk te maken of te bevorderen. Ook hierbij geldt dat het moet gaan om een voldoende precies geformuleerd gedragsvoorschrift. Dat gedragsvoorschrift mag niet verder strekken dan voor het toezicht op de naleving van de andere bijzondere voorwaarde(n) noodzakelijk is (vgl. HR 28 september 2021, ECLI:NL:HR:2021:1403).”

De Hoge Raad overweegt verder:

“De door het hof gestelde bijzondere voorwaarde dat de veroordeelde “meewerkt aan controle van digitale gegevensdragers tijdens een huisbezoek” voldoet niet aan de onder 4.2. genoemde eisen [zie voorgaande alinea waarin 4.2 is verwoord, toevoeging auteurs] en is daarom in strijd met artikel 14c lid 2, onder 14°, Sr. Hoewel het hof - anders dan het cassatiemiddel betoogt - voldoende duidelijk tot uitdrukking heeft gebracht dat deze bijzondere voorwaarde het toezicht op de naleving van de bijzondere voorwaarde onder 3 beoogt te regelen, blijkt uit de voorwaarde immers niet met welke frequentie en op welke wijze de controles van de gegevensdragers mogen worden uitgevoerd, welke functionarissen daarbij betrokken mogen zijn en hoe is gewaarborgd dat de persoonlijke levenssfeer van de verdachte daarbij niet verdergaand wordt beperkt dan nodig is voor het beoogde toezicht.”

[HR 31 mei 2022, ECLI:NL2022:807 \(vervolg op 23 februari 2016, ECLI:NL:HR:2016:302\)](#)

Vornoemd arrest uit 2016 is door de Hoge Raad teruggewezen naar het gerechtshof Arnhem-Leeuwarden. Het hof heeft als bijzondere voorwaarde opgelegd dat de veroordeelde:

“wordt verplicht om zich te onthouden van:

(a) gedragingen die zijn gericht op internetomgevingen, waarin kinderpornografisch materiaal kan worden verkregen en

(b) gedragingen die zijn gericht op internetomgevingen, waarin over seksuele handelingen met kinderen wordt gecommuniceerd.

Ten behoeve van de naleving van deze verplichtingen is veroordeelde verder verplicht zijn medewerking te verlenen aan het steekproefsgewijs laten controleren van zijn digitale gegevensdragers. De reclassering bepaalt in welke gevallen, op welke manier, door wie en wanneer de feitelijke controle plaatsvindt. Die medewerking dient uit het volgende te bestaan:

- veroordeelde moet maximaal tweemaal per jaar in het kader van die controle aan de reclassering en eventueel door de reclassering uitgenodigde politiemedewerkers de toegang verschaffen tot zijn woning;

- veroordeelde moet dan op verzoek van de reclassering al zijn digitale gegevensdragers ter beschikking stellen dan wel overhandigen aan de reclasserings- of politiemedewerkers;

- veroordeelde moet de reclassering dan wel de door hen uitgenodigde politiemedewerkers de toegang verschaffen tot alle aanwezige digitale gegevensdragers, bijvoorbeeld door het geven van de benodigde wachtwoorden.

Geeft opdracht aan de reclassering tot het houden van toezicht op de naleving van voormelde bijzondere voorwaarde en de veroordeelde ten behoeve daarvan te begeleiden.”²⁷

Tegen de uitspraak van het hof wordt beroep in cassatie ingesteld. De klacht in cassatie richt zich op de drie hiervoor genoemde voorwaarden (gedachtstreepjes) waarin de medewerking die van de veroordeelde wordt vereist. De Hoge Raad formuleert de volgende eisen als het gaat om de medewerking/het toezicht:

“Op grond van artikel 14c lid 3, aanhef en onder b, Sr is aan het stellen van een bijzondere voorwaarde van rechtswege onder meer de voorwaarde verbonden dat de veroordeelde medewerking verleent aan het reclasseringstoezicht, bedoeld in artikel 14c lid 6 Sr. Daarnaast voorziet artikel 6:3:14 Sv in voorschriften en bevoegdheden in verband met het toezicht op de naleving van aan een voorwaardelijke veroordeling verbonden voorwaarden. Deze regelingen staan er niet aan in de weg dat – voor zover dat, gelet op de mogelijkheden die de zojuist genoemde wettelijke bepalingen al bieden, aangewezen is – een gedragsvoorwaarde wordt gesteld die een gedraging van de veroordeelde betreft en die ertoe strekt het toezicht op (een) andere door de rechter op grond van artikel 14c lid 2 Sr gestelde bijzondere voorwaarde(n) mogelijk te maken of te bevorderen. Ook hierbij geldt dat het moet gaan om een voldoende precies geformuleerd gedragsvoorschrift. Dat gedragsvoorschrift mag niet verder strekken dan voor het toezicht op de naleving van de

²⁷ Gerechtshof Arnhem-Leeuwarden, 2 december 2020, ECLI:NL:GHARL:2020:10058.

andere bijzondere voorwaarde(n) noodzakelijk is. (Vgl. HR 28 september 2021, ECLI:NL:HR:2021:1403).”

De hiervoor geformuleerde voorwaarde voldoet volgens de Hoge Raad niet aan de genoemde eisen en is daarom in strijd met artikel 14c, tweede lid, aanhef en onder 5°, (oud) Sr [het huidige artikel 14c, tweede lid, aanhef en onder 14° Sr, toevoeging auteurs].

“Hoewel het hof voldoende duidelijk tot uitdrukking heeft gebracht dat deze bijzondere voorwaarde het toezicht op de naleving van de bijzondere voorwaarden onder a en b beoogt te regelen, blijkt uit de voorwaarde immers niet op welke wijze de controles van de gegevensdragers mogen worden uitgevoerd en hoe is gewaarborgd dat de persoonlijke levenssfeer van de verdachte daarbij niet verdergaand wordt beperkt dan nodig is voor het beoogde toezicht.” De Hoge Raad vernietigt de uitspraak en verwijst de zaak naar het gerechtshof 's-Hertogenbosch.

Dit arrest is ook van belang omdat de Hoge Raad, mede daartoe uitgenodigd door Procureur-Generaal Bleichrodt (zoals hiervoor beschreven), ingaat op de vraag wat moet worden verstaan onder de gedragsvoorwaarde, genoemd in artikel 14c, tweede lid, onder 14° Sr. De Hoge Raad stelt daarover het volgende:

“Artikel 14c lid 2, aanhef en onder 14° Sr biedt de rechter de mogelijkheid om, naast de algemene voorwaarde uit lid 1 dat de veroordeelde zich binnen de proeftijd niet schuldig maakt aan een strafbaar feit, bepaalde gedragsvoorwaarden te stellen. Dat kan gebeuren in aanvulling op of in plaats van de overige in artikel 14c lid 2 Sr genoemde bijzondere voorwaarden. Onder ‘voorwaarden die strekken ter bevordering van goed levensgedrag van de veroordeelde’ moeten worden verstaan voorwaarden die strekken tot het voorkomen van strafbaar gedrag van de veroordeelde. Bij ‘voorwaarden die een gedraging betreffen waartoe hij uit een oogpunt van maatschappelijke betamelijkheid gehouden moet worden geacht’ gaat het om voorwaarden die een gedraging van de veroordeelde betreffen waartoe hij naar aanleiding van het bewezenverklarde feit uit een oogpunt van maatschappelijke betamelijkheid gehouden is, bijvoorbeeld jegens slachtoffers van het bewezenverklarde feit.”

Zowel de gedragsvoorwaarde als het toezicht moeten dus voldoende precies zijn omschreven, zo stelt ook Ten Voorde in zijn noot onder het arrest. De voorwaarde moet “voldoende precies het daarin vervatte gedragsvoorschrift” tot uitdrukking brengen. Volgens Ten Voorde lijkt echter onder verwijzing van rechtspraak van de Hoge Raad “aanmerkelijk precies” beter de lading te dekken dan voldoende precies.

Als het gaat om de verplichting tot medewerking aan toezicht verwijst Ten Voorde, net als overigens de Hoge Raad in zijn arrest, naar de mogelijkheid voor de rechter om de uitoefening van het toezicht op te dragen aan de Reclassering op grond van artikel 14c, zesde lid, Sr. Aan het opgedragen toezicht moet de veroordeelde medewerking verlenen, artikel 14c, derde lid, onderdeel b, Sr. Deze bepaling is volgens Ten Voorde tamelijk open geformuleerd en staat aan enige creativiteit bij het vormgeven van het toezicht niet in de weg. De gedragsvoorwaarde mag er ook toe strekken het toezicht op een andere door de rechter op grond van artikel 14c, tweede lid, Sr gestelde bijzondere voorwaarde mogelijk te maken of te bevorderen, waarbij van belang is dat er oog is voor de eisen van proportionaliteit en subsidiariteit.

Ook hier geldt dat het toezicht voldoende precies moet worden omschreven, waarbij Ten Voorde verwijst naar de hiervoor besproken arresten van 15 maart 2022 en van 7 juli 2020. Dit betekent dat:

- a) het toezicht betrekking heeft op hetgeen de veroordeelde moet doen of nalaten;
- b) het toezicht 'beperkt dient te blijven tot dat toezicht op de naleving van' de voorwaarde dat de veroordeelde iets doet of nalaat; en
- c) voldoende precies is geformuleerd waar, wanneer, hoe vaak, op welke wijze en door wie (naast de reclasseringsinstelling aan wie het oefenen van het toezicht door de strafrechter is opgedragen) het toezicht mag worden uitgeoefend.

Met het oog op het onder c genoemde stelt Ten Voorde dat "aanmerkelijke precisie" een passender criterium lijkt (in plaats van 'voldoende precies') nu de feitenrechter zich ook bij het stellen van de gedragsvoorwaarde moet afvragen of deze proportioneel is, dat wil zeggen de vrijheden van de veroordeelde niet meer beperken dan nodig is voor het beoogde toezicht.

Andere aandachtspunten zijn dat het gedragsvoorschrift "niet het gedrag van de verdachte mag omvatten dat in feite neerkomt op het meewerken aan door de politie uit te oefenen veelomvattende en ingrijpende dwangmiddelen" en dat een voorwaarde niet kan worden gesteld wanneer de naleving niet onder alle omstandigheden afhankelijk is van de wil van de veroordeelde. Met dit aandachtspunt, zo stelt Ten Voorde, lijkt de Hoge Raad duidelijk te willen maken dat een gedragsvoorwaarde die wordt aangevuld met toezichtsmaatregelen in onderlinge samenhang moeten staan.²⁸

De verwijzing van de Hoge Raad in dit arrest naar artikel 14c, zesde lid, jo. derde lid, onderdeel b, Sr, terwijl de geformuleerde voorwaarde zijn grondslag vindt in artikel 14c, tweede lid, aanhef en onderdeel 5 (oud) Sr (nu artikel 14, tweede lid, aanhef en onder 14° Sr, lijkt een vingerwijzing als het volgende arrest wordt gezien.

[HR 29 november 2022, ECLI: NL:HR: 2022: 1763 \(vervolg op HR 7 juli 2020, ECLI:NL:HR:2020:1215\)](#)

Na terugwijzing heeft het hof Den Haag de volgende bijzondere voorwaarde opgelegd:

"Stelt als bijzondere voorwaarden dat de veroordeelde:

(...)

4. zich gedurende de proeftijd op welke wijze dan ook:

- onthoudt van het op digitale wijze met een seksuele intentie communiceren met minderjarigen/kinderen,
- onthoudt van gedragingen die zijn gericht op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen,
- onthoudt van gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met minderjarigen/kinderen wordt gecommuniceerd,
- onthoudt van het aanwezig hebben of gebruiken van wisprogramma's op zijn digitale apparatuur;

(...)

Geeft opdracht aan de reclassering tot het houden van toezicht op de naleving van voormelde bijzondere voorwaarden en de veroordeelde ten behoeve daarvan te begeleiden. Het toezicht op de onder 4 vermelde voorwaarde kan onder andere bestaan uit controles van geautomatiseerde werken en digitale gegevensdragers; de verdachte werkt daaraan mee tijdens een huisbezoek; deze controles mogen gedurende de proeftijd van 3 jaren maximaal 3 keer worden uitgevoerd en mogen - voor zover het gedrag bedoeld onder het tweede en derde gedachtestreepje van de onder 4 gestelde voorwaarde betreft - slechts

²⁸ HR 31 mei 2022, ECLI:NL:HR:2022:807, NJ 2022/250 m. nt. J.M. ten Voorde.

op zodanige wijze worden uitgevoerd dat niet door een persoon kennis wordt genomen van de inhoud van afbeeldingen (geautomatiseerde controle is derhalve wel toegestaan). Ten behoeve van deze controle mag een deskundige (niet zijnde een opsporingsambtenaar) de reclassering (technische) ondersteuning bieden.”

Het cassatiemiddel klaagt over de door het hof aan de Reclassering verstrekte opdracht tot het houden van toezicht op de naleving van de bijzondere voorwaarde. Bijzonder aan deze zaak is, zo valt uit het arrest op te maken, dat het hof in de bestreden uitspraak een toezichtsoopdracht aan de Reclassering heeft gegeven als bedoeld in artikel 14c lid 6 Sr en daarbij nader heeft bepaald op welke manier dat toezicht kan plaatsvinden. In eerdere rechtspraak (daarbij wordt verwezen naar de hiervoor besproken arresten van de Hoge Raad van 15 maart 2022 en 31 mei 2022) ging het om zaken waar de rechter op grond van artikel 14c lid 2, onder 14° Sr een gedragsvoorwaarde had opgelegd die tot doel had het toezicht op de naleving van de bijzondere voorwaarde mogelijk te maken of te bevorderen. Daarbij wordt wel opgemerkt dat de uitgangspunten voor het toezicht, zoals geformuleerd in eerdere zaken, ook gelden voor het toezicht dat in dit arrest aan de orde is.

De Hoge Raad oordeelt dat bij de beoordeling van het cassatiemiddel het volgende vooropgesteld moet worden:

“Het Wetboek van Strafrecht en het Wetboek van Strafvordering voorzien niet in een regeling die is toegesneden op het in artikel 14c lid 6 Sr en het in artikel 6:3:14 lid 1, aanhef en onder a sub 4, Sv bedoelde toezicht voor gevallen zoals dit, waarin het toezicht ertoe strekt de naleving te controleren van de gedragsvoorwaarde voor zover deze inhoudt dat de veroordeelde zich onthoudt van gedragingen die zijn gericht op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen en/of dat de veroordeelde zich onthoudt van gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met minderjarigen/kinderen wordt gecommuniceerd. Het ontbreken van zo’n specifieke wettelijke regeling betekent niet dat de rechter bij het geven van een toezichtsoopdracht geen nadere invulling kan geven aan de manier waarop dat toezicht kan plaatsvinden. Wel zal bij het geven van zo’n opdracht moeten zijn gewaarborgd dat het toezicht niet leidt tot een meer dan beperkte inbreuk op de persoonlijke levenssfeer van de veroordeelde. Daarbij komt betekenis toe aan de vraag met welke frequentie en hoe de controles mogen worden uitgevoerd en welk (politie)functionarissen daarbij betrokken mogen zijn (Vgl. HR 9 maart 2021, ECLI:HR:NL:2021:248).”

De Hoge Raad oordeelt dus dat het ontbreken van een specifieke wettelijke regeling er niet aan in de weg hoeft te staan dat de rechter invulling geeft aan de wijze waarop het toezicht kan plaatsvinden. Daarbij lijkt de Hoge Raad niet verder in te gaan op hetgeen Advocaat-Generaal Vegter stelt in zijn conclusie in deze zaak. Zo stelt Vegter dat goed verdedigbaar is dat wanneer “de wet (nog) niet voorziet in een grondslag om inbreuken op grondrechten te voorkomen er een taak voor de rechter is weggelegd”. Ook stelt Vegter: “Bij dreiging van een (ernstige) inbreuk op grondrechten lijkt mij deze vorm van rechterlijke bemoeienis met het toezicht zelfs aangewezen. Dat is ook de lijn van de rechtspraak van de Hoge Raad waarin is overwogen dat de persoonlijke levenssfeer van de verdachte niet verdergaand wordt beperkt dan nodig is voor het beoogde toezicht.”²⁹

Van belang is verder dat de Hoge Raad oordeelt: “Voor zover het cassatiemiddel klaagt dat het hof heeft geoordeeld dat controles van geautomatiseerde werken en digitale gegevensdragers door een

²⁹ HR 11 oktober 2022, ECLI:NL:PHR:2022:915.

opsporingsambtenaar in het kader van het toezicht op de naleving van de gedragsvoorwaarde in het geheel niet zijn toegestaan, berust het op een onjuiste lezing van de overwegingen van het hof en mist het in zoverre feitelijke grondslag.” De Hoge Raad verwerpt het beroep.

Mevis stelt in zijn bespreking dat de Hoge Raad een voorkeur uitspreekt “voor de thans gevolgde variant”, te weten dat de nadere inrichting van het toezicht via de weg van artikel 14c, zesde lid jo. derde lid, Sr plaatsvindt. Ook stelt Mevis: “Omgekeerd levert de acceptatie van de nadere inrichting van het toezicht door de strafopleggende rechter via de weg van art. 14c lid 6 juncto lid 3 Sr in bovenstaande zaak, als ik het goed zie, geen harde belemmeringen op om ook de weg van artikel 14c lid 2 onder 14° te blijven volgen.” Hij noemt de weg van artikel 14c, zesde lid, Sr op niet vanzelfsprekend, omdat het toezicht op de naleving van de bijzondere voorwaarden op grond van artikel 6:3:14, eerste lid, aanhef en onderdeel a, sub 4, Sv, van rechtswege is opgedragen aan het openbaar ministerie. Het toezicht is ook de Reclassering opgedragen, zo stelt Mevis, indien de rechter daartoe op de voet van artikel 14c, zesde lid, Sr in zijn sanctiebeslissing opdracht geeft. In dat geval rust op de veroordeelde van rechtswege de plicht hieraan mee te werken (zie artikel 14c, derde lid, aanhef en onderdeel b, Sr.

Verder stelt Mevis in zijn noot dat ook de Hoge Raad (naast de praktijk die volgens hem worstelt) ‘worstelde’ met de inrichting van het toezicht. Daarbij verwijst Mevis naar de zaak die voor de tweede keer in cassatie werd behandeld, hiervoor besproken arrest van 31 mei 2022. Mevis stelt: “Voortvarende strafvordering en effectieve tenuitvoerlegging zien er anders uit.”³⁰

Interessant is tot slot nog dat Advocaat-Generaal Vegter in zijn conclusie bij dit arrest ingaat op het feit dat door de Advocaat-Generaal tijdens de zitting bij het hof is gesteld dat door bijstand van de politie uit te sluiten, de door het hof voorgestane controle is verworden tot een “lege huls”. Vegter wijst erop dat de inzet van de politie in de cassatieschriftuur vooral in verband wordt gebracht met de expertise van de politie. Dat toezicht door uitsluiting van de politie bij de controle op de naleving van de voorwaarde een lege huls wordt, brengt de Advocaat-Generaal vooral in verband met de voorspelbaarheid van het toezicht door beperking van de frequentie en niet zozeer met de controle door juist een politieambtenaar. In feitelijke aanleg komt de effectiviteit van toezicht in het licht van de voorwaarden, zo stelt Vegter, niet goed uit de verf. Het ontbreken van een context aan de hand van feitelijke vaststellingen over de effectiviteit van het door het hof beperkte toezicht, belemmert volgens Vegter de verdere toetsing in cassatie ernstig. Het wordt wel gesteld, zo stelt Vegter, maar de daarvoor aangevoerde gronden zijn er in cassatie niet of nauwelijks. Vegter: “Ik schrijf dit niet op als een verwijt, maar vooral als een aanmoediging om over de gang van zaken bij het toezicht en de effectiviteit ervan in feitelijke aanleg meer te stellen en dit onderwerp van debat ter terechtzitting te maken.”

3.3.1 Welk kader kan uit de uitspraken van de Hoge Raad worden afgeleid?

Uit de hiervoor besproken arresten kan het volgende kader worden afgeleid voor het opleggen van de bijzondere voorwaarde. Dit kader betreft het karakter van de voorwaarde, de formulering van de gedragsvoorwaarden en het toezicht en de proeftijd waarop de voorwaarde betrekking heeft.

Het karakter van de bijzondere voorwaarde

De bijzondere voorwaarde in het algemeen dient te strekken tot de bevordering van *het goede levensgedrag* van de veroordeelde. Hieronder moet worden verstaan: het voorkomen van strafbaar gedrag.

³⁰ HR 29 november 2022, ECLI:NL:HR:2022:1763, NJ 2023/364, m.nt. P.A.M. Mevis

De formulering van de gedragsvoorwaarden en het toezicht

In het algemeen geldt dat voldoende precies omschreven moet worden i) welk gedrag de veroordeelde dient te vertonen of na te laten; en ii) hoe het toezicht op de naleving van de voorwaarde wordt ingericht. De variant die de “voorkeur” lijkt te hebben, om met Mevis te spreken, is dat naast de gedragsvoorwaarde die wordt bepaald op grond van artikel 14c, tweede lid, onder 14°, het toezicht verder wordt “ingericht” op grond van artikel 14c, zesde lid, jo. derde lid, Sr.

Kenmerken van gedragsvoorwaarden die op basis van de besproken jurisprudentie kunnen worden genoemd:

- Voldoende precies moet worden omschreven van welk gedrag de veroordeelde zich dient te onthouden met het oog op het digitale wijze communiceren met kinderen;
- Voldoende precies moet worden omschreven van welk gedrag de veroordeelde zich dient te onthouden met het oog op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen;
- Voldoende precies moet worden omschreven van welk gedrag de veroordeelde zich dient te onthouden bijvoorbeeld van gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met minderjarigen/kinderen wordt gecommuniceerd;
- Voldoende precies moet worden omschreven van welk gedrag de veroordeelde zich dient te onthouden, bijvoorbeeld het aanwezig hebben of gebruiken van wisprogramma's op zijn digitale apparatuur.

Kenmerken van het toezicht die op basis van de besproken jurisprudentie kunnen worden genoemd:

- Voldoende precies moet worden omschreven waar het toezicht zich op richt en waartoe het beperkt dient te blijven met het oog op de geformuleerde gedragsvoorwaarde;
- Voldoende precies moet worden omschreven dat het toezicht op de geformuleerde gedragsvoorwaarde kan bestaan uit controles van geautomatiseerde werken en digitale gegevensdragers en dat de verdachte daaraan meewerkt tijdens een huisbezoek;
- Voldoende precies moet worden omschreven waar, wanneer, hoe vaak, op welke wijze en door wie het toezicht mag worden uitgeoefend. Bijvoorbeeld: deze controles mogen gedurende een proeftijd van drie jaar maximaal drie keer worden uitgevoerd en mogen slechts op zodanige wijze worden uitgevoerd dat niet door een persoon kennis wordt genomen van de inhoud van afbeeldingen (geautomatiseerde controle is derhalve wel toegestaan). Ten behoeve van deze controle mag een deskundige (niet zijnde een opsporingsambtenaar) de Reclassering (technische) ondersteuning bieden.

De proeftijd waarop de voorwaarde betrekking heeft

Over de proeftijd waarop de voorwaarde betrekking heeft kan nog het volgende worden ontleend aan de jurisprudentie. Uit het arrest van de Hoge Raad van 15 maart 2021, ECLI:NL:HR:2022:338 lijkt te kunnen worden afgeleid dat een proeftijd van tien jaar niet kan worden verbonden aan deze bijzondere voorwaarde. De Hoge Raad verwijst in voornoemd arrest naar zijn arrest van 12 juni 2018, ECLI:NL:HR:2018:894. In dat arrest werd de betrokkene veroordeeld wegens, kort gezegd, het maken/verspreiden/aanbieden van materiaal van seksuele uitbuiting van kinderen. In die zaak was ook de voorwaarde opgelegd dat de veroordeelde moest meewerken aan controle van zijn gegevensdragers. Maar het middel in cassatie zag alleen op de proeftijd van vijf jaar die was verbonden aan het voorwaardelijke deel van de opgelegde gevangenisstraf. In het arrest van 12 juni 2018 deed de Hoge Raad de zaak zelf af en bepaalde de proeftijd op twee jaren.

Zoals in bijlage 1 bij dit rapport wordt benoemd, bedraagt de proeftijd sinds 1 april 2012 ten hoogste drie jaar en kan deze tien jaar bedragen indien er ernstig rekening mee moet worden gehouden dat de veroordeelde wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen. Dat in het arrest

van 2018 de proeftijd op twee jaar werd gesteld, heeft waarschijnlijk te maken met het feit dat de delicten deels waren gepleegd in een periode van voor de wetswijziging van 2012.

In het genoemde arrest van 12 juni 2018, maar ook in het arrest van 28 maart 2017, ECLI:NL:HR:2017:524 en 30 januari 2018, ECLI:NL:HR:2018:116 heeft de Hoge Raad bepaald dat misdrijven zoals "een gewoonte maken van het verspreiden van het verspreiden, en/of aanbieden, en/of in het bezit hebben van kinderporno – ook niet zonder meer kunnen worden gekarakteriseerd als misdrijven die dergelijke gedragingen [gericht tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen, toevoeging auteurs] omvatten". Op grond van het voorgaande lijkt aan de voorwaarde die in dit onderzoek centraal staat dus een proeftijd van ten hoogste drie jaar te kunnen worden verbonden.

3.4 Conclusie

De rechtspraak heeft de afgelopen jaren geworsteld met de bijzondere voorwaarden en het toezicht op naleving van die bijzondere voorwaarden. Die worsteling richt zich met name op de vraag door wie de controle mag worden verricht, de intensiteit van de controle, de frequentie en wijze waarop de controle wordt uitgevoerd. Door de jaren heen heeft de Hoge Raad de grenzen waarbinnen de bijzondere voorwaarde en het toezicht daarop toelaatbaar zijn nader uitgewerkt. Het is de taak van de lagere rechtspraak om concreet invulling te geven aan de bijzondere voorwaarde en het toezicht binnen deze grenzen. In het volgende hoofdstuk gaan we in op de vraag of, en zo ja, op welke wijze de lagere rechtspraak daaraan door de jaren heen invulling heeft gegeven.

Wat uit het kader van de Hoge Raad blijkt, is dat de bijzondere voorwaarde voldoende precies moet zijn omschreven en er op gericht moet zijn goed levensgedrag te bevorderen. Ook het toezicht daarop moet voldoende precies worden omschreven, zodat dit een niet meer dan beperkte inbreuk op de persoonlijke levenssfeer oplevert. Het gaat dan om een omschrijving van de aspecten waar het toezicht zich op richt en waartoe het zich beperkt, waar de controles uit bestaan (voorwerp van controle), en waar, wanneer, hoe vaak en door wie en op welke wijze het toezicht wordt uitgeoefend. De Hoge Raad oordeelt niet expliciet dat opsporingsambtenaren (de politie) de controle niet mogen uitvoeren.

Wel oordeelt de Hoge Raad dat het Wetboek van Strafrecht en het Wetboek van Strafvordering niet voorzien in een regeling die is toegesneden op het toezicht³¹ op naleving van de gedragsvoorwaarde dat de veroordeelde zich onthoudt van gedragingen die gericht zijn op internetomgevingen waar materiaal van seksuele uitbuiting van kinderen kan worden verkregen. Dat deze wettelijke regeling ontbreekt, betekent niet dat de rechter bij het opleggen van de voorwaarde geen nadere invulling kan geven aan de manier waarop het toezicht kan plaatsvinden. Belangrijk is dan wel dat wordt gewaarborgd dat het toezicht niet leidt tot een meer dan beperkte inbreuk op de persoonlijke levenssfeer van de veroordeelde.

De Hoge Raad spreekt zich in de besproken arresten niet expliciet uit voor een specifieke wettelijke regeling voor deze vorm van toezicht, terwijl hij dat wel deed in zijn arrest van 25 november 2008 (ECLI:NL:HR:2008:BF038) zoals besproken in hoofdstuk 2. In dat geval ging het om een "ingrijpende inbreuk op de bewegingsvrijheid", terwijl de Hoge Raad ten aanzien van de bijzondere voorwaarde die centraal staat in dit onderzoek ook stelt dat het gaat om een inbreuk op de persoonlijke levenssfeer.

³¹ Van artikel 14c lid 6 Sr en artikel 6: 3: 14 lid 1 aanhef en onder a sub 4 Sv.

Op grond van de jurisprudentie lijkt een proeftijd langer dan drie jaar niet aan de voorwaarde te kunnen worden verbonden.

4. Cijfermatige analyse jurisprudentie lagere rechtspraak

4.1 Inleiding

In het voorgaande hoofdstuk hebben we gezien dat de Hoge Raad door de jaren heen grenzen heeft gesteld aan de controle van digitale gegevensdragers. Het is de taak van de lagere rechtspraak om binnen deze grenzen de bijzondere voorwaarde te formuleren. In dit hoofdstuk staan we stil bij de ontwikkelingen in de lagere rechtspraak in het kader van de controle van digitale gegevensdragers, door te bekijken hoe lagere rechters de bijzondere voorwaarde formuleren. Dat doen we aan de hand van een cijfermatige analyse van de rechtspraak.

In dit hoofdstuk beantwoorden we het tweede deel van onderzoeksvraag 1, voor zover het gaat om het kader dat uit de lagere rechtspraak volgt:

1. Wat zijn, mede gelet op recente jurisprudentie, de juridische kaders waaraan controles van online gedrag betreffende seksueel kindermisbruik moeten voldoen?

Het jurisprudentieonderzoek richt zich op de periode vanaf 24 februari 2016 tot en met 31 december 2023 en is uitgevoerd op de database met gepubliceerde uitspraken van rechtspraak.nl. We hebben dit als startpunt genomen omdat de Hoge Raad – voor zover bekend – op de eerstgenoemde datum voor het eerst arrest wees over de bijzondere voorwaarde die in dit onderzoek centraal staat.

Als zoektermen zijn de volgende trefwoorden gebruikt: kinderporno | gegevensdragers | controle. Eerst is een vooronderzoek gedaan van de zaken tussen 1 april 2012 (invoering van de wetwijziging van de bijzondere voorwaarden) en 23 februari 2016, onder andere om vast te kunnen stellen of de zoektermen goed functioneren. Over deze periode zijn 104 hits aangetroffen, waarvan in 60 zaken een bijzondere voorwaarde is opgelegd. Uit het vooronderzoek is gebleken dat met de zoektermen ook uitspraken naar voren komen waarin niet de bijzondere voorwaarde wordt opgelegd, maar het woord ‘controle’ wordt gevonden in het kader van het onderzoek dat is gedaan door bijvoorbeeld het OM, of de ‘controle’ die de verdachte heeft over zijn gedrag. Met specifiekere zoektermen kan dit mogelijk worden voorkomen, maar dan bestaat een kans dat relevante zaken gemist worden. Om dat te voorkomen, hebben we ervoor gekozen deze zoektermen te handhaven en zaken waarin de bijzondere voorwaarde niet is opgelegd te registreren, maar verder niet te analyseren.

In de geanalyseerde periode van februari 2016 tot en met 2023 zijn in totaal 395 gepubliceerde zaken op rechtspraak.nl aangetroffen waarin de bijzondere voorwaarde tot controle van digitale gegevensdragers is opgelegd. Opgemerkt moet worden dat niet alle uitspraken op rechtspraak.nl worden gepubliceerd.³² Wel geven de gevonden uitspraken voldoende inzicht in de lagere rechtspraak. De bijzondere voorwaarde wordt onder verschillende strafrechtelijke titels opgelegd (zie hiervoor tabel 1).³³ In het merendeel van de gevallen gaat het om een bijzondere voorwaarde bij een voorwaardelijke straf, daarna volgt tbs met voorwaarden. In enkele gevallen is de voorwaarde bij een voorwaardelijke straf voor jeugdigen opgelegd. In een geval is de voorwaarde opgelegd bij een maatregel betreffende het gedrag van een jeugdige en bij een voorwaardelijke beëindiging van de plaatsing in een inrichting voor jeugdigen.

³² Dit verklaart waarschijnlijk ook de discrepantie tussen de 300 zaken per jaar waar de startnotitie van het WODC over spreekt en het aantal gevonden zaken op rechtspraak.nl

³³ Hoewel in dit onderzoek de titel voorwaardelijke straf centraal staat, zijn voor de volledigheid in het jurisprudentieonderzoek ook de andere titels meegenomen.

Totaal opgelegde controles	Voorwaardelijke straf (art. 14a jo. 14c Sr)	Tbs met voorwaarden (art. 38 Sr)	Voorwaardelijke straf jeugdige (art. 77x jo. 77z Sr)	Gedragmaatregel jeugdige (art. 77w Sr)	Voorwaardelijke beëindiging PIJ (art. 6:6:31 jo. 6:6:32 Sv)
395	303	81	9	1	1

Tabel 1: totaaloverzicht aantal opgelegde controles

4.2 Algemene en specifieke formuleringen

In de jurisprudentieanalyse is een onderscheid gemaakt tussen de bijzondere voorwaarden die algemeen zijn geformuleerd en bijzondere voorwaarden die specifiek zijn geformuleerd. Om tot deze indeling te komen zijn de volgende criteria gehanteerd.

Een bijzondere voorwaarde is algemeen geformuleerd indien de voorwaarde een van de volgende elementen bevat:

- Er is bepaald dat de veroordeelde mee moet werken aan de controle³⁴ en/of;
- De controle is geformuleerd als onderdeel van het reclasseringstoezicht;³⁵

en alle de volgende elementen bevat:

- Het voorwerp van controle wordt aangeduid (vb. *gegevensdragers, computers*);
- Er is een proeftijd van X jaar vastgesteld;
- Er is bepaald wie met de controle is belast.

Een bijzondere voorwaarde is specifiek geformuleerd, indien deze een van de volgende onderdelen specificeert:

- De wijze van de controle;
- De frequentie van de controle is vastgesteld op Y keer;
- De wijze van de medewerking van de veroordeelde is nader omschreven.

Als ondergrens voor een kwalificatie als specifiek geformuleerde bijzondere voorwaarde is genomen dat de bijzondere voorwaarde minimaal drie verschillende specificerende elementen bevat over de wijze van de controle en/of de frequentie en/of de wijze van de medewerking. Door deze ondergrens te hanteren wordt voorkomen dat een formulering die relatief beknopt en overwegend algemeen is van aard, als specifiek wordt bestempeld. Het gaat om de elementen weergegeven in figuur 3.

Door middel van deze scoringsmethode is in kaart gebracht in hoeveel zaken de rechter een bijzondere voorwaarde algemeen heeft geformuleerd en in hoeveel zaken de formulering is gespecificeerd (zie hiervoor tabel 2). In paragraaf 4.3 worden de kenmerken van de algemeen

³⁴ Een dergelijke formulering luidt als volgt of gelijkloidend: “dat veroordeelde zijn medewerking verleend aan controles op zijn digitale gegevensdragers”.

³⁵ Een dergelijke formulering luidt als volgt of gelijkloidend: “terwijl het daarop uitgeoefende toezicht mede kan bestaan uit controle aan digitale gegevensdragers”.

geformuleerde bijzondere voorwaarden behandeld. In paragraaf 4.4 volgen de kenmerken van de specifiek geformuleerde bijzondere voorwaarden.

Wijze controle	Wijze medewerking	Frequentie
<ul style="list-style-type: none"> ➤Reclassering bepaalt wijze uitvoering ➤Onaangekondigd ➤Zoekwoorden gebruiken ➤Software kan gebruikt worden ➤Verplicht geautomatiseerde controle ➤Handmatige controle toegestaan ➤Geen stelselmatige inbreuk persoonlijke levenssfeer ➤Controle strekt niet tot verkrijgen beeld persoonlijke leven ➤Beperkt tot verboden gedraging(en) ➤Kopie maken ➤Geheimhouding externe functionaris ➤Toestemming vereist voor binnen treden/controle door politie 	<ul style="list-style-type: none"> ➤Toegang verschaffen tot woning ➤Alle gegevensdragers ter beschikking stellen ➤Toegang geven tot alle gegevensdragers ➤Gegevensdragers drie dagen ter beschikking stellen ➤Geen data wissen ➤Wachtwoorden geven ➤Inloggegevens geven ➤Op aanwijzing ontsleutelen ➤Geen wisprogramma's gebruiken/aanwezig hebben ➤Geen verhullende apps gebruiken ➤Geen TOR browser/Tailz gebruiken 	<ul style="list-style-type: none"> ➤x aantal keren per jaar ➤x aantal keren gedurende proeftijd

Figuur 3. Overzicht specificerende elementen

Uit de scoring van de bijzondere voorwaarden is de volgende ontwikkeling in de jurisprudentie waarneembaar. In de jaren 2016 en 2017 zijn alle bijzondere voorwaarden algemeen geformuleerd. In 2018 worden voor het eerst bijzondere voorwaarden specifiek geformuleerd. De algemeen geformuleerde bijzondere voorwaarden blijven echter dominant in de periode van 2018 tot en met 2020. Het omslagpunt ligt in 2021, waarin het aantal specifieke formuleringen voor het eerst het aantal algemene formuleringen overstijgt. In 2022 neemt het aantal specifiek geformuleerde bijzondere voorwaarden nog verder toe. In 2023 zijn alle bijzondere voorwaarden specifiek geformuleerd.

Jaar	Aantal keren opgelegd	Algemene formulering	Specifieke formulering
2016	14	14	-
2017	31	31	-
2018	49	43	6
2019	46	41	5
2020	51	38	13
2021	62	26	36
2022	64	7	57
2023	78	-	78
Totaal	395	200	195

Tabel 2: overzicht opgelegde algemene en specifiek geformuleerde bijzondere voorwaarden

4.3 Kenmerken van de algemeen geformuleerde bijzondere voorwaarden

In deze paragraaf staan we stil bij de kenmerken van de algemeen geformuleerde bijzondere voorwaarden. We bekijken hoe de bijzondere voorwaarde is geformuleerd, hoe het voorwerp van controle wordt aangeduid, welke specificerende elementen daarin terugkomen, welke instanties worden belast met het toezicht en welke proeftijd is opgenomen. Het gaat in totaal om 200 zaken (zie tabel 2). De kenmerken van de algemeen geformuleerde bijzondere voorwaarden zijn onderzocht door de inhoud van de uitspraken te labelen aan de hand van de verschillende elementen die zijn benoemd in de voorgaande paragraaf. Allereerst is bekeken op welke wijze de bijzondere voorwaarde is geformuleerd (zie hierover tabel 3).

Medewerking

De nadruk in de bijzondere voorwaarde ligt op de medewerking van de veroordeelde bij de controle. Deze formulering luidt als volgt of vergelijkbaar: *“dat veroordeelde zijn medewerking verleent aan controles aan zijn digitale gegevensdragers.”*

Onderdeel van het toezicht

Hier ligt de nadruk niet op de medewerking maar op de controle als onderdeel van het uit te oefenen reclasseringstoezicht. Deze luidt als volgt of in vergelijkbare bewoordingen: *“terwijl het daarop uitgeoefende toezicht mede kan bestaan uit controle aan digitale gegevensdragers.”*

Combinatie van medewerking en onderdeel toezicht

In een deel van de gevallen zijn beide elementen opgenomen bij de algemeen geformuleerde bijzondere voorwaarde. Dat is uit tabel 3 af te leiden, omdat de twee elementen opgeteld het totaal aantal opgelegde bijzondere voorwaarden van tabel 2 overstijgen. Vanaf 2018 wordt de combinatie in minstens de helft van de gevallen opgelegd.

<i>Jaar</i>	Medewerking	Controle als onderdeel toezicht
2016	10	5
2017	16	15
2018	32	23
2019	36	23
2020	37	28
2021	24	16
2022	6	7

Tabel 3: overzicht formulering van de algemeen geformuleerde bijzondere voorwaarden

4.3.1 Aanduiding voorwerp van controle

De rechter gebruikt verschillende aanduidingen van het voorwerp van controle (zie hiervoor tabel 4). Meest gehanteerd zijn 'digitale gegevensdragers' 'computers' en 'andere apparatuur'. Veelvoorkomend is de combinatie 'computers en andere apparatuur'. Uit de analyse blijkt dat in een deel van de gevallen alle drie aanduidingen cumulatief worden gebruikt. In enkele gevallen is uit de analyse naar voren gekomen dat apparatuur nader wordt omschreven als apparatuur waarop afbeeldingen kunnen worden opgeslagen of waarmee het internet kan worden benaderd. Om wat voor type digitale gegevensdragers het gaat wordt niet gespecificeerd (zoals een USB-stick, CD-ROM, harde schijf, SSD).

<i>Jaar</i>	Gegevensdragers	Digitale gegevensdragers	Communicatiemiddelen	Computer(s)	Andere apparatuur	Telefoon	Digitale apparaten
2016	6	1	1	7	6	1	-
2017	11	7	1	20	17	5	-
2018	11	19	-	29	22	3	-
2019	5	25	-	30	30	1	-
2020	3	30	-	31	29	1	-
2021	4	18	-	20	18	-	1
2022	2	4	-	7	6	-	-

Tabel 4: overzicht aanduiding voorwerp van controle

4.3.2 Een of twee specificerende elementen

Bij een aantal algemeen geformuleerde bijzondere voorwaarden zijn een of twee specificerende elementen opgenomen, waardoor – zoals is aangegeven in paragraaf 4.2 – deze niet kwalificeren als een specifiek geformuleerde bijzondere voorwaarde (zie hiervoor tabel 5).

Jaar	Reclassering bepaalt wijze uitvoering	Wachtwoorden geven	Geen wis-programma's	Ontgrendelen bestanden	Geen verhullende apps	Geen data wissen	Geen Tor browser
2016	1	1	-	1	-	-	-
2017	1	1	2	-	-	-	-
2018	3	1	2	-	-	-	-
2019	2	-	1	-	-	-	-
2020	1	-	-	-	-	-	-
2021	1	-	-	-	1	1	1
2022	-	-	-	-	-	-	-

Tabel 5: overzicht specificerende elementen

4.3.3 Instanties belast met controle

Bij de algemeen geformuleerde bijzondere voorwaarden zijn in de rechterlijke vonnissen zes verschillende (combinaties van) instantie(s) aangetroffen die worden aangewezen om de controle uit te voeren. Het gaat om de Reclassering, de Reclassering en de politie, de politie, de Reclassering en een technisch deskundige, de Reclassering en een medewerker van het TBKK³⁶ en de Reclassering en een behandelaar (zie hiervoor tabel 6).³⁷ In het merendeel van de gevallen wordt de Reclassering aangewezen als controlerende instantie. Daarna volgen de varianten Reclassering en politie en de politie. De overige varianten zijn slechts bij enkele algemeen geformuleerde bijzondere voorwaarden aangetroffen.

³⁶ Team ter bestrijding van Kinderpornografie en Kindersekstoerisme.

³⁷ NB: de technisch deskundige wordt in vonnissen andere wijzen geformuleerd zoals technisch specialist, en ICT-deskundige. Er is voor gekozen om deze onder dezelfde noemer van "technisch deskundige" in te delen.

<i>Jaar</i>	Reclassering	Reclassering en politie	Politie	Reclassering en technisch deskundige	Reclassering en medewerker TBKK	Reclassering en behandelaar
2016	11	-	2	1	-	-
2017	25	1	2	1		2
2018	36	5	2	-	-	-
2019	34	3	3	1	-	-
2020	36	-	1	-	1	-
2021	21	3	2	-	-	-
2022	6	-	-	1	-	-

Tabel 6: overzicht controlerende instanties

4.3.4 Proeftijd

Ten slotte is de proeftijd gescoord. Voor de titel voorwaardelijke straf zijn de volgende proeftijden bij de algemeen geformuleerde bijzondere voorwaarden opgelegd: twee jaar, drie jaar, vier jaar, vijf jaar, zes jaar en tien jaar (zie hiervoor tabel 7). In de gevallen van de aangetroffen titels tbs met voorwaarden, en de voorwaardelijke beëindiging PIJ, volgt de proeftijd uit het Wetboek van Strafrecht.³⁸ De meest voorkomende proeftijd is die van drie jaar. Daarna volgen proeftijden van twee en vijf jaar. Gemiddeld één keer per jaar wordt een proeftijd van tien jaar opgelegd bij de algemeen geformuleerde bijzondere voorwaarde. In één zaak werd de proeftijd niet vastgesteld.

<i>Jaar</i>	2 jaar	3 jaar	4 jaar	5 jaar	6 jaar	10 jaar ³⁹	Volgt uit WvSr
2016	1	6	-	2	-	1	4
2017	6	11	1	3	-	1	9
2018	5	24	1	2	-	1	10
2019	7	18	-	5	-	1	10
2020	6	13	-	5	1	1	12
2021	7	8	-	4	-	-	7
2022	2	1	-	1	-	-	3

Tabel 7: overzicht proeftijd

³⁸ Volgens artikel 38, eerste lid, Sr is de termijn van de tbs met voorwaarden twee jaar, waarna deze kan worden verlengd voor een periode van twee jaar. De maximale duur is bepaald op negen jaar. Volgens artikel 77s en 77t Sr eindigt de voorwaardelijke beëindiging van de PIJ-maatregel na een jaar onvoorwaardelijk.

³⁹ In het geval de rechter een proeftijd van tien jaar oplegt, onderbouwt de rechter dat er gelet op de omstandigheden ernstig rekening mee moet worden gehouden dat de verdachte wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen. Het verschilt per zaak hoe uitgebreid de rechter ingaat op de concrete omstandigheden die daartoe aanleiding geven.

4.4 Kenmerken van specifiek geformuleerde bijzondere voorwaarden

In deze paragraaf staan we stil bij de kenmerken van specifiek geformuleerde bijzondere voorwaarden. Zoals in paragraaf 4.2 is vermeld, is een specifiek geformuleerde bijzondere voorwaarde op een of meer onderdelen nader uitgewerkt, namelijk wat betreft de wijze van de controle, de wijze van de medewerking en/of de frequentie van de controle. Als ondergrens is genomen dat de bijzondere voorwaarde ten minste drie specificerende elementen bevat. In tegenstelling tot de algemeen geformuleerde bijzondere voorwaarde is hierdoor bij de specifieke formuleringen meer variatie te zien en zijn de formuleringen meer toegespitst op de wijze waarop de controle mag plaatsvinden. Om de kenmerken van de specifiek geformuleerde bijzondere voorwaarden in kaart te brengen zijn per onderdeel de terugkomende elementen geïdentificeerd en vervolgens gescoord. Per element wordt toegelicht wat dit inhoudt, hoe het element zich heeft ontwikkeld en of het element regelmatig voorkomt of niet. Daarna volgt een bespreking van de opgelegde frequentie van de controle, de aanduiding van het voorwerp van controle, de instanties belast met controle en de opgelegde proeftijd bij de specifiek geformuleerde bijzondere voorwaarden. In totaal gaat het om 195 uitspraken (zie tabel 2).

4.4.1 Elementen die zien op de wijze van controle

Het totaaloverzicht van de elementen in de wijze van controle per jaartal staan in tabel 8. Eerst worden de elementen besproken die in een relatief groot deel van het aantal opgelegde bijzondere voorwaarde van een bepaald jaar of jaren voorkomen (minimaal in een derde van de gevallen in een of meer onderzochte jaren). Daarna volgt bespreking van de elementen die minder vaak voorkomen. Het gaat daarbij om elementen die in minder dan een derde van de gevallen over de onderzochte jaren voorkomen. Doordat de elementen in combinatie met elkaar worden opgelegd in de vonnissen, overstijgen de weergegeven getallen in tabel 8 het totaal aantal opgelegde specifiek geformuleerde bijzondere voorwaarden van tabel 2.

Veelvoorkomend

- De Reclassering bepaalt de wijze van de uitvoering

Dit betreft een passage in de voorwaarde waarin de rechter vaststelt dat de Reclassering bepaalt op welke wijze, wanneer, door wie en wanneer de controle plaatsvindt. In de meeste gevallen is de 'wie-vraag' begrensd doordat de rechter bijvoorbeeld heeft bepaald dat de Reclassering politiemedewerkers mag meenemen of een technisch deskundige. Dit element komt voornamelijk voor in bepalingen tussen 2018-2020. Daarna neemt de aanwezigheid van dit element af en in 2023 is het in geen van de gevallen meer bepaald.

- Er mag software gebruikt worden

Vanaf 2021 wordt een nieuw element geïntroduceerd, namelijk dat de controlerende instantie gebruik mag maken van software om de gegevensdragers mee te onderzoeken. Dit wordt door de rechter aangeduid als 'kinderpornoherkenningssoftware', als 'een hulpmiddel dat een indicatie geeft of kinderpornografisch materiaal aanwezig is' of als 'software-programmatuur'. Uit het feit dat het gebruik van de software facultatief is, kan worden afgeleid dat het is toegestaan om de controle handmatig uit te voeren. In 2022 is dit element in de helft van de zaken opgenomen en in 2023 is het in twee derde van de gevallen bepaald.

- De controle moet geautomatiseerd plaatsvinden

Vanaf 2021 wordt een nieuw element geïntroduceerd dat voorschrijft dat de controle verplicht op geautomatiseerde wijze moet plaatsvinden. Verplichte geautomatiseerde controle wordt minder vaak bevolen dan de facultatieve variant. Het aantal keren dat deze werd opgelegd is wel toegenomen sinds 2021. In een derde van de zaken uit 2023 werd geautomatiseerde controle verplicht gesteld.

- De controle is beperkt tot de verboden gedraging(en)

Vanaf 2020 wordt in toenemende gevallen het element opgenomen dat de controle zich moet beperken tot de naleving van de gedragingen geformuleerd in de gedragsvoorwaarden, zoals het zich onthouden van het verzamelen van kinderporno en het zich onthouden van chatten met minderjarigen. Dit element veronderstelt dat enkel gericht mag worden gezocht op onderdelen van de gegevensdragers waarvan het aannemelijk is dat de genoemde gedragingen daar plaatsvinden.

- De controle strekt er niet toe een beeld te krijgen van het persoonlijke leven

In 2021 is het element geïntroduceerd dat de controle niet strekt tot het verkrijgen van een beeld van het persoonlijke leven van de veroordeelde. In 2022 en 2023 wordt dit element in toenemende mate opgenomen in de bijzondere voorwaarde. In 2022 ging het om de helft van de zaken en in 2023 is het element in twee derde van de onderzochte uitspraken opgenomen. Wat de precieze betekenis van het element is voor de begrenzing van de controle is niet geheel duidelijk. Een te strikte lezing leidt ertoe dat de controle in zijn geheel niet zou mogen plaatsvinden. Immers, elke controle levert een inbreuk op de persoonlijke levenssfeer op. In andere zaken zien we het vergelijkbare element dat geen sprake mag zijn van een stelselmatige inbreuk op de persoonlijke levenssfeer (zie hierna). Of beide elementen hetzelfde beogen is niet geheel zeker, maar wel aannemelijk. Beide lijken erop te doelen dat een zekere inbreuk op de persoonlijke levenssfeer mag plaatsvinden, maar dat dit er niet toe mag leiden dat een volledig beeld wordt gekregen van het persoonlijke leven van de veroordeelde.

Minder voorkomend

- Onaangekondigd

In achttien gevallen in de periode van 2020-2023 is expliciet bepaald dat de controles onaangekondigd plaatsvinden. In het overige deel van de zaken zwijgt de rechter over de vraag of de controles aangekondigd of onaangekondigd dienen plaats te vinden. Er zijn geen bepalingen aangetroffen waarin wordt gesteld dat controles aangekondigd moeten worden. Dat roept de vraag op of in het geval de rechter hierover zwijgt, het aan de Reclassering of andere controlerende instantie(s) is om te bepalen of de controles al dan niet aangekondigd worden.

- Er moeten zoekwoorden worden gebruikt met een geschikt zoekprogramma

In vier zaken in 2021 en 2022 is bepaald dat de controle moet plaatsvinden door gebruikmaking van zoekwoorden die zijn gericht op de opsporing van kinderpornografisch materiaal door middel van een daarvoor geschikt zoekprogramma.

- Handmatige controle is expliciet toegestaan

In drie uitspraken in 2022 en 2023 is expliciet benoemd dat behalve met software, de controle handmatig mag plaatsvinden. In het merendeel van de gevallen zwijgt de rechter op dit punt. Aangenomen kan worden dat handmatige controle is toegestaan, tenzij de rechter expliciet heeft opgenomen dat de controle verplicht geautomatiseerd moet plaatsvinden.

- Er mag geen stelselmatige inbreuk worden gemaakt op de persoonlijke levenssfeer

In de periode van 2020-2022 is in elf gevallen in de bijzondere voorwaarde opgenomen dat geen stelselmatige inbreuk mag worden gemaakt op de persoonlijke levenssfeer. In 2023 is dit element niet meer teruggekomen.

- Er mag een kopie worden gemaakt van de gegevensdrager

In dertien uitspraken in 2021-2023 is bepaald dat in het geval het onderzoek ter plaatse onvoldoende kan worden uitgevoerd, een kopie van de gegevensdrager mag worden gemaakt, waarna deze op een andere plek door een deskundige onderzocht mag worden. Deze onderzoeker mag uitsluitend aan de Reclassering rapporteren. De voorwaarde vervolgt dat voor de vraag of sprake is van strafbare kinderporno, de Reclassering een gecertificeerd zedenrechercheur mag raadplegen, die wederom alleen aan Reclassering mag rapporteren. Indien geen schending heeft plaatsgevonden, moet de kopie na twee weken worden vernietigd.

- Een externe controlerende functionaris is verplicht tot geheimhouding

In vijf uitspraken (in 2020 en in 2022) is opgenomen dat voor gevallen waarin de controle door een externe functionaris wordt uitgevoerd (niet de politie/Reclassering), deze tot geheimhouding is verplicht. In drie van deze uitspraken werd daaraan toegevoegd dat er toestemming moet worden gevraagd voor het betreden van de woning door deze externe partij.

- Er is toestemming vereist voor het betreden van de woning door de politie en voor het overgaan tot uitvoeren van de controle⁴⁰

In drie uitspraken in 2022 is bepaald dat in het geval de politie als deskundige meegaat met de controle, deze toestemming nodig heeft voor het binnentreden van de woning en voor het overgaan tot het uitvoeren van de controle.

4.4.2 Overkoepelende bevindingen wijze controle

In de periode 2018-2020 concretiseert de rechter de wijze waarop de controle moet plaatsvinden weinig en wordt de invulling hiervan aan de Reclassering opgedragen en overgelaten. Vanaf 2021 wordt de wijze van controle vaker en op verschillende manieren nader uitgewerkt. Dat is terug te zien in een toename van de gescoorde elementen. In 2023 neemt deze variatie in elementen af en worden de volgende elementen dominanter: de verplichte geautomatiseerde controle, de facultatieve variant om software te gebruiken, de beperking van de controle tot de verboden gedragingen en de beperking dat de controle er niet toe strekt een beeld te krijgen van het persoonlijke leven.

⁴⁰ Dit element valt strikt genomen zowel onder 'wijze controle' als 'wijze medewerking'. Voor de overzichtelijkheid is het element enkel bij de wijze van controle opgenomen.

Jaar	Reclassering bepaalt wijze uitvoering	Onaan-gekondigd	Zoek-woorden	Software kan gebruikt worden	Verplicht geautoma-tiseerd	Hand-matig toegest aan	Geen stelsel-matige inbreuk	Geen beeld persoonlijke leven	Beperkt tot verboden gedraging	Kopie	Geheim-houding externe control-eur	Toe-stem-ming politie
2018	6	-	-	-	-	-		1	-	-		-
2019	5	-	-	-	-	-		-	-	-		-
2020	11	2	-	-	-	-	2	-	1	-	1	-
2021	4	6	1	13	2	-	4	8	12	2	-	-
2022	1	6	3	30	9	2	5	29	48	8	4	3
2023	-	4	-	51	25	1	-	53	70	3	-	-

Tabel 8: overzicht elementen wijze controle

4.4.3 Elementen die zien op de wijze van medewerking

Het totaaloverzicht van de gescoorde elementen met betrekking tot de wijze van medewerking staan in tabel 9. Eerst worden de elementen besproken die regelmatig terugkomen (in ten minste een derde van de gevallen in een of meer onderzochte jaren). Daarna volgt bespreking van de elementen die in enkele zaken zijn opgenomen (in minder dan een derde van de gevallen over de onderzochte jaren). Aangezien de elementen in combinatie met elkaar worden opgelegd in de vonnissen, overstijgen de weergegeven getallen in tabel 9 het totaal aantal opgelegde specifieke formuleringen.

Veelvoorkomend

- Toegang tot de woning verschaffen

In de periode van 2018-2020 is bij vrijwel alle specifiek geformuleerde bijzondere voorwaarden opgenomen dat de veroordeelde de instantie(s) die aangewezen waren om de controle uit te voeren, toegang moet verschaffen tot zijn woning. In de jaren hierna komt dit element steeds minder vaak voor. In 2023 is het nog slechts in twee gevallen aangetroffen.

- De veroordeelde moet alle gegevensdragers ter beschikking stellen dan wel overhandigen

Dit element komt meestal terug in combinatie met het verlenen van toegang tot de woning. Voor dit element geldt dezelfde ontwikkeling als het element 'toegang tot de woning verschaffen'.

- De veroordeelde moet toegang verlenen tot alle gegevensdragers

Dit element wordt in de periode van 2018-2020 opgenomen bij bijna alle specifiek geformuleerde bijzondere voorwaarden, in combinatie met de elementen 'toegang woning' en 'overhandigen gegevensdragers'. Ander dan bij de vorige twee elementen, wordt dit element ook in de periode van 2021-2023 nog in minstens de helft van de gevallen opgenomen. Zo is in 2023 in 51 gevallen bepaald dat de veroordeelde toegang moet verlenen tot alle gegevensdragers.

- De veroordeelde verstrekt wachtwoorden die nodig zijn voor controle⁴¹

Voor het opnemen van het element dat de veroordeelde de wachtwoorden moet verstrekken die nodig zijn voor de controle, geldt een ontwikkeling die vergelijkbaar is met de eis dat de veroordeelde toegang moet verlenen tot alle gegevensdragers. Deze twee elementen worden bijna in alle specifieke geformuleerde voorwaarden in combinatie met elkaar opgenomen, of in combinatie met de eis dat veroordeelde zijn gegevensdragers ter beschikking stelt. In 2023 is het geven van de wachtwoorden ook in enkele gevallen opgelegd zonder te specificeren dat de veroordeelde de gegevensdragers ter beschikking moet stellen dan wel toegang daartoe moet verlenen.

Minder voorkomend

- De veroordeelde moet de gegevensdragers voor drie dagen ter beschikking stellen

In drie gevallen in 2022 is bepaald dat de veroordeelde voor een periode van maximaal drie dagen zijn gegevensdragers ter beschikking moet stellen ten behoeve van de controle.

- De veroordeelde ontsleutelt op aanwijzing versleutelde gegevens

In dertien gevallen in de periode van 2021-2023 is bepaald dat in het geval versleutelde, verborgen of niet-toegankelijke bestanden op de gegevensdrager staan, de veroordeelde deze op aanwijzing moet ontsleutelen of toegankelijk moet maken.

- De veroordeelde wist geen data

In vier gevallen heeft de rechter bepaald dat de veroordeelde geen data mag wissen. In één zaak gaat het om bestanden, documenten, apps, zoekhistorie, en/of contacten. In de drie andere zaken wordt alleen de internetgeschiedenis genoemd.

- De veroordeelde verstrekt zijn inloggegevens

Hoewel in het merendeel van de zaken alleen wordt bepaald dat de veroordeelde zijn wachtwoorden dient te verstrekken, is in vier uitspraken bepaald dat de veroordeelde zijn inloggegevens moet geven in het kader van de medewerking (gebruikersnamen/emailadressen en wachtwoorden).

- Veroordeelde mag geen wisprogramma's gebruiken

In zeven zaken is bepaald dat de veroordeelde geen wisprogramma's mag gebruiken of aanwezig mag hebben op zijn gegevensdragers.

- Veroordeelde mag geen verhullende apps gebruiken

In drie zaken is bepaald dat veroordeelde geen gebruik mag maken van internetgebruik verhullende apps en/of programma's.

- Veroordeelde mag geen gebruik maken van TOR/Tailz/VPN

In 2023 is in één zaak bepaald dat de veroordeelde geen gebruik mag maken van de Tor Browser, Tailz of een VPN. In principe gaat het om eenzelfde soort bepaling als bij het verbod van verhullende apps, maar in dit geval heeft de rechter het verbod verder toegespitst op specifieke software.

⁴¹ Het is mogelijk dat veroordeelde een vrouw betreft, en de bepaling zou luiden; veroordeelde verstrekt *haar* wachtwoorden. In het merendeel van de gevallen betreffen de veroordeelden echter mannen, en gebruikt de rechter daarom 'zijn'. daarom is ervoor gekozen deze formulering aan te houden.

4.4.4 Overkoepelende bevindingen wijze medewerking

- In de periode 2018-2020 worden in nagenoeg alle zaken dezelfde vier elementen opgenomen over de wijze van de medewerking, namelijk dat veroordeelde toegang tot zijn woning verschaft, alle gegevensdragers ter beschikking stelt, toegang geeft tot deze gegevensdragers en de benodigde wachtwoorden verstrekt.
- In de periode 2021-2023 wordt in steeds minder gevallen de toegang tot de woning en het ter beschikking stellen van de gegevensdragers genoemd. In het merendeel van de gevallen wordt bepaald dat de veroordeelde toegang moet verlenen tot alle gegevensdragers en zijn wachtwoorden moet geven. Wel ontstaat meer variatie in de elementen, hoewel die in een relatief klein deel van de zaken worden opgenomen. Opmerkelijk is dat het voorschrift dat veroordeelde geen wisprogramma's mag gebruiken – dat in de periode van 2017-2019 bij een aantal algemeen geformuleerde bijzondere voorwaarden is opgelegd – in de jaren daarna niet is opgelegd en in 2022 weer in een aantal zaken is opgenomen.

Jaar	Toegang woning verschaffen	Alle gegevensdragers overhandigen	Toegang geven tot alle gegevensdragers	Gegevensdragers 3 dagen ter beschikking stellen	Geen data wissen	Wachtwoorden geven	Inloggegevens geven	Op aanwijzing ontsleutelen	Geen wisprogramma's	Geen verhandelende apps	Geen TOR browser/ tailz/ VPN
2018	6	6	6	-	-	6	-	-	-	-	-
2019	5	5	5	-	-	5	-	-	-	-	-
2020	11	11	11	-	1	12	2	-	-	-	-
2021	11	14	20	-	-	22	1	2	-	-	-
2022	7	4	29	3	1	33	-	8	1	-	-
2023	2	1	51	-	1	58	1	3	6	2	1

Tabel 9: overzicht wijze medewerking

4.4.5 Frequentie van de controle

Tabel 10 bevat het overzicht van de opgelegde maximale frequenties van de controles. In het merendeel van de gevallen wordt de maximale frequentie per jaar vastgesteld. In de jaren 2022-2023 koppelt de rechter in een aantal uitspraken het maximaal aantal controles aan de gehele duur van de proeftijd.⁴² In elf gevallen is de frequentie niet vastgesteld. Uit het overzicht is af te leiden dat in de periode 2018-2020 de frequentie in bijna alle gevallen werd vastgesteld op maximaal twee keer per jaar. In de periode 2020-2023 wordt de frequentie het vaakst vastgesteld op maximaal drie keer per jaar en ontstaat ook meer differentiatie.

Jaar	1 keer per jaar	2 keer per jaar	3 keer per jaar	4 keer per jaar	5 keer per jaar	6 keer per jaar	8 keer per jaar	2 keer gedurende proeftijd	3 keer gedurende proeftijd	5 keer gedurende proeftijd	6 keer gedurende proeftijd	9 keer gedurende proeftijd	10 keer gedurende proeftijd	Niet vastgesteld
2018	-	5	-	-	-	-	-	-	-	-	-	-	-	1
2019	-	5	-	-	-	-	-	-	-	-	-	-	-	-
2020	-	5	-	3	1	-	-	-	-	-	-	-	-	4
2021	1	7	17	6	-	1	-	-	1	1	1	-	-	1
2022	-	2	35	5	-	1	1	-	6	-	2	-	1	4
2023	-	2	60	-	-	1	-	2	3	1	7	1	-	1

Tabel 10: overzicht maximale frequentie controle

4.4.6 Aanduiding voorwerp van controle

In de periode 2018-2020 duidt de rechter het voorwerp van controle – op enkele uitzonderingen na – aan als 'digitale gegevensdragers'.⁴³ In de jaren 2021-2023 wordt daaraan in een toenemend aantal gevallen toegevoegd dat 'computers en smartphones' of meer in algemene zin de 'geautomatiseerde werken' gecontroleerd worden. In enkele gevallen wordt volstaan met de term 'gegevensdragers'. Digitale gegevensdragers worden in geen van de uitspraken nader gespecificeerd. Zie tabel 11.

⁴² Het maximale totaal aantal controles is altijd gekoppeld aan de loop van de proeftijd. Daar geeft dit tabel geen inzicht in.

⁴³ Door de jaren heen werd in elf uitspraken digitale gegevensdragers niet genoemd. Dat blijkt uit tabel 11 (184 van de 195 gevallen).

<i>Jaar</i>	Gegevensdragers	Digitale gegevensdragers	Geautomatiseerde werken	Computer(s)	Andere apparatuur	Smartphone(s)
2018	-	6	-	-	-	
2019	-	5	-	-	-	
2020	-	13	-	1	-	-
2021	3	34	10	13	2	8
2022	8	49	22	30	2	29
2023	1	77	27	58	4	50

Tabel 11: overzicht aanduiding voorwerp van controle

4.4.7 Instanties belast met de controle

Bij de specifiek geformuleerde bijzondere voorwaarden worden zes verschillende (combinaties van) instantie(s) aangewezen om de controle uit te voeren, zie tabel 12. Deze aanduidingen zijn overgenomen uit de vonnissen. In de periode 2018-2019 wordt de controle in alle gevallen opgelegd aan de Reclassering en de politie. In 2020 geldt dit ook voor de meeste gevallen, maar vanaf dat jaar wordt in toenemende mate de controle opgedragen aan de Reclassering en een technisch deskundige. Dat mag in deze gevallen ook een politieambtenaar zijn. In 2021 wordt voor het eerst in twee zaken bepaald dat de technisch deskundige geen opsporingsambtenaar mag zijn. In 2023 wordt in een derde van de zaken bepaald dat de technisch deskundige geen opsporingsambtenaar mag zijn en in ongeveer twee derde van de zaken dat dit wel is toegestaan. In de jaren 2021-2022 zien we de meeste variatie in controlerende instanties, waarbij de controle in enkele gevallen wordt opgedragen aan de Reclassering met een digitaal rechercheur van de TBKK of aan de Reclassering en een betrokken hulpverlener.

<i>Jaar</i>	Reclassering	Reclassering en politie	Politie	Reclassering en technisch deskundige*	Reclassering en technisch deskundige (geen opsporingsambtenaar)	Reclassering en digitaal rechercheur TBKK	Reclassering, betrokken en hulpverlener
2018	-	6	-	-	-	-	-
2019	-	5	-	-	-	-	-
2020	1	9	1	2	-	-	-
2021	4	4	2	13	2	9	2
2022	4	1	-	38	8	7	3
2023	-	-	-	54	23	2	-

Tabel 12: overzicht controlerende instanties

4.4.8 Proeftijd

Wat betreft de proeftijd is deze bij de specifiek geformuleerde bijzondere voorwaarden op twee jaar, drie jaar, vier jaar, vijf jaar en tien jaar vastgesteld, zie tabel 13. In de gevallen van de aangetroffen titels tbs met voorwaarden en de voorwaardelijke beëindiging PIJ, volgt de proeftijd uit het Wetboek van Strafrecht.⁴⁴ De meest voorkomende proeftijd voor de voorwaardelijke straf is drie jaar, daarna volgen die van vijf en twee jaar. Proeftijden van tien en vier jaar zijn beide slechts in één zaak opgelegd.

	2 jaar	3 jaar	4 jaar	5 jaar	10 jaar ⁴⁵	Volgt uit WvSr
<i>Jaar</i>						
2018	-	5	-	-	-	1
2019	1	1	-	2	-	1
2020	3	5	-	1	1	3
2021	3	18	-	9	-	6
2022	5	37	-	8	-	7
2023	11	49	1	6	-	11

Tabel 13: overzicht proeftijd

4.5 Conclusie

Uit de cijfermatige jurisprudentieanalyse is gebleken dat de formulering van de controle van digitale gegevensdragers in de onderzochte jaren (2016 tot en met 2023) aan de nodige veranderingen onderhevig is geweest. De eerste uitspraak van de Hoge Raad in 2016 heeft in eerste instantie niet tot navolging geleid wat betreft de formulering van de bijzondere voorwaarde door de rechter in eerste aanleg. Pas in 2018 zien we een voorzichtige ontwikkeling op gang komen waar de rechter in een beperkt aantal zaken meer eisen stelt aan de medewerking en het toezicht.

De arresten van de Hoge Raad in 2020, 2021 en 2022 veranderen deze trend. Vanaf 2021 zien we dat de rechter meer eisen gaat stellen en ontstaat steeds meer variatie in die eisen. Dit geldt zowel voor de medewerking van de veroordeelde als voor het toezicht zelf. Mogelijk is deze toename in variatie te verklaren door een worsteling van de rechter om het kader van de Hoge Raad toe te passen in de formulering, of doordat de ruimte voor wat de Hoge Raad in die periode toelaatbaar achtte wat betreft formulering, groter werd gevonden, terwijl deze ruimte in de latere arresten van 2022 verder wordt beperkt. Dat zou ook kunnen verklaren dat de variatie van elementen in 2023 juist weer afneemt en alle bijzondere voorwaarden specifiek zijn geformuleerd. Op basis van de ontwikkelingen in de feitenrechtspraak zien we meer in het algemeen dat de rechter in 2022 en 2023 de focus is gaan verleggen naar het beperken van de inbreuk op persoonlijke levenssfeer. Ook scheidt de rechter in die periode in toenemende mate de controle van de opsporing van strafbare feiten door de inzet van opsporingsambtenaren steeds vaker te verbieden.

⁴⁴ Volgens artikel 38, eerste lid, Sr is de termijn van de tbs met voorwaarden twee jaar, waarna deze kan worden verlengd voor een periode van twee jaar. De maximale duur is bepaald op negen jaar. Volgens artikel 77s en 77t Sr eindigt de maatregel na een jaar onvoorwaardelijk.

⁴⁵ In het geval de rechter een proeftijd van tien jaar oplegt, onderbouwt de rechter dat gelet op de omstandigheden ernstig rekening mee moet worden gehouden dat de verdachte wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen. Het verschilt per zaak hoe uitgebreid de rechter ingaat op de concrete omstandigheden die daartoe aanleiding geven.

In 2022 en 2023 is een toename zichtbaar van formuleringen die stellen dat geen volledig beeld van het persoonlijke leven mag worden verkregen en dat de controle beperkt moet blijven tot de verboden gedragingen. Daarnaast wordt in het grootste deel van de gevallen bepaald dat software mag worden gebruikt, dan wel dat de controle geautomatiseerd moet plaatsvinden. Dit vereiste is dienstbaar aan de voorwaarde dat geen volledig beeld wordt verkregen van het persoonlijke leven van de betrokkene.

Wat betreft de wijze van medewerking, zien we dat de rechter net als de jaren ervoor blijft eisen dat de veroordeelde toegang verleent tot alle gegevensdragers en dat wachtwoorden moeten worden verstrekt. Het verschaffen van toegang tot de woning en het overhandigen van de gegevensdragers wordt in 2022 en 2023 nauwelijks meer genoemd, terwijl deze in voorgaande jaren wel werd opgenomen. De precieze reden hiervoor is onduidelijk. Mogelijk heeft dit te maken met de beperking van de inbreuk op de persoonlijke levenssfeer of met het verleggen van de focus door de rechter naar het specificeren van de wijze van controle in plaats van de wijze van medewerking. Een andere mogelijke verklaring is dat het verlenen van toegang tot de gegevensdragers, het verlenen van toegang tot de woning en het overhandigen van de gegevensdragers impliceert.

De meest voorkomende proeftijd voor de voorwaardelijke veroordeling is drie jaar. Dat is begrijpelijk, aangezien dit de standaard proeftijd is die sinds 2012 volgt uit het Wetboek van Strafrecht.⁴⁶ Uit het jurisprudentieonderzoek blijkt dat de proeftijd ook wel op twee jaar is gesteld. Een verklaring hiervoor is dat het in die desbetreffende uitspraken gaat om delicten die gepleegd zijn voor de wetwijziging in 2012, waarmee de proeftijd werd verhoogd van ten hoogste twee jaar naar ten hoogste drie jaar.

⁴⁶ Zie Hoofdstuk 3. paragraaf 3.3.1.

5. Controle van digitale gegevensdragers in de praktijk

5.1 Inleiding

De controle van digitale gegevensdragers werd in de periode van 2012 tot medio 2023 uitgevoerd bij zaken waarin het ging om materiaal van seksuele uitbuiting van kinderen, als onderdeel van een set aan maatregelen om het gedrag van de betrokkene te beïnvloeden. Binnen deze periode is de controle aan de nodige ontwikkelingen onderhevig geweest, die mede bepalend zijn geweest voor de stopzetting van de controle in 2023. Kenmerkend voor het opleggen en uitvoeren van de controle is dat op verschillende momenten in het proces verschillende partijen uit de strafrechtketen betrokken zijn, elk met hun eigen taken en rollen. Daardoor heeft elk van deze partijen ook een andere verhouding tot degene die de controle opgelegd krijgt.

In dit hoofdstuk staan we stil bij deze betrokken partijen, hun taken en verhouding tot de betrokkene, de praktijk van de controle, aan welke ontwikkelingen de controle onderhevig is geweest en welke kenmerken de effectiviteit van de controle bepalen. Ook wordt stilgestaan bij het perspectief van de betrokken partijen die sinds 2012 betrokken waren bij de controle en hoe zij deze uitvoeringspraktijk hebben ervaren.

Onderzoeksvragen 2, 4 en 5 staan hierbij centraal:

2. Wat houden de controles van digitale gegevensdragers in de praktijk in en welke actoren zijn daarbij betrokken?

4. Hoe verhouden de controles in de huidige vorm zich tot het werk van de Reclassering?

5. In hoeverre kan met de huidige controlemethodes inzicht worden gekregen in online gedrag betreffende seksueel kindermisbruik en hoe effectief zijn de controles?

Het antwoord op deze vragen biedt de basis om in hoofdstuk 8 deze praktijk te kunnen evalueren.

Het hoofdstuk is gebaseerd op interviews met de politie, de Reclassering, het openbaar ministerie en rechtspraak, op literatuur (waaronder het handboek *Werken in gedwongen kader* uit 2024⁴⁷) en Kamerbrieven over het onderwerp. Allereerst wordt ingegaan op de relevante actoren en hun betrokkenheid en rol bij een delict als bedoeld in artikel 252 Sr. Hierbij gaan we wat dieper in op de rol van de Reclassering, aangezien dat van belang is voor de vraag hoe de controle zich verhoudt tot de taak van de Reclassering. Daarna wordt beschreven waarom de controle van digitale gegevensdragers zijn intrede deed en hoe de praktijk zich ontwikkelde tot medio juli 2023. Vanaf die periode zijn er geen controles meer uitgevoerd vanwege verschillende knelpunten in de praktijk. Dan staan we stil bij de kenmerken die belangrijk zijn voor de effectiviteit van de controle. Ten slotte volgt een beschrijving van de knelpunten die de betrokken partijen hebben ervaren bij de uitvoering van de controle.

⁴⁷ J. Bosker & A. Menger, *Werken in gedwongen kader*, Amsterdam: 2024

5.2 Betrokken actoren

Politie

Bestrijden en terugdringen van materiaal van seksuele uitbuiting van kinderen

Een van de kerntaken van de politie is die van de handhaving van de rechtsorde in overeenstemming met de daarvoor geldende rechtsregels.⁴⁸ Een van de fundamentele pijlers van het handhaven van de rechtsorde is het opsporen van strafbare feiten als bedoeld in artikel 252 Sr. In het kader van de opsporing wordt in de Veiligheidsagenda elke vier jaar de aanpak en prioritering bepaald. In de Veiligheidsagenda 2015-2018 is bepaald dat het voornaamste doel van de politie was om materiaal van seksuele uitbuiting van kinderen terug te dringen, met een focus op slachtoffers, vervaardigers en verspreiders. In de dadergerichte aanpak werd gekozen om onder andere te focussen op recidivisten.⁴⁹

Gezien de exponentiële groei van het aantal meldingen van strafbaar online beeldmateriaal,⁵⁰ is in de agenda 2019-2022 de prioriteit verschoven naar het bereiken van een zo groot mogelijk maatschappelijk effect, door met name in te zetten op het aanpakken van de *keyplayers* en (internationale) netwerken, vervaardigers en misbruikers.⁵¹ In de Veiligheidsagenda 2023-2026 is deze focus doorgezet. Volgens de politie verhoudt deze aanpak en prioritering zich slecht tot de controle van digitale gegevensdragers als er geen sterke signalen zijn dat er beeldmateriaal op de digitale gegevensdragers staat.⁵²

Openbaar Ministerie

Opsporen en vervolgen van strafbare feiten als bedoeld in artikel 252 Sr

Het openbaar ministerie is verantwoordelijk voor het opsporen en vervolgen van strafbare feiten als bedoeld in artikel 252 Sr, met als doel passende straftoemeting. Het openbaar ministerie geeft leiding aan de politie in opsporingsonderzoeken en bepaalt of iemand uiteindelijk wordt vervolgd. Dit kan het openbaar ministerie doen door zelf een strafbeschikking op te leggen of door de zaak voor de strafrechter te brengen.⁵³

Toezicht uitvoering strafvonnissen, waaronder naleving voorwaarden

Het openbaar ministerie is ervoor verantwoordelijk dat strafrechtelijke vonnissen worden uitgevoerd en is formeel belast met het toezicht op de naleving van de opgelegde voorwaarden.⁵⁴ In de praktijk wordt het toezicht en de begeleiding van de bijzondere voorwaarden vrijwel geheel aan de Reclassering overgelaten. In beginsel is het dan ook de Reclassering die het toezicht op de naleving van de bijzondere voorwaarden zal moeten uitvoeren.

Strafrechter

Beoordelen strafbaar feit, schuld en beslissen over de straf

⁴⁸ Artikel 3 Politiewet.

⁴⁹ Veiligheidsagenda politie 2015-2018, p. 8.

⁵⁰ Ter illustratie: de politie ontving in 2021 36.000 meldingen en de verwachting voor 2022 werd op 50.000 meldingen gesteld, zie Veiligheidsagenda politie 2023-2026, p. 15.

⁵¹ Veiligheidsagenda politie 2019-2022, p. 10

⁵² *Kamerstukken II 2023/2024 29270*, nr. 156, p. 2.

⁵³ Het openbaar ministerie kan een strafbeschikking opleggen voor overtredingen en misdrijven waar maximaal een gevangenisstraf van 6 jaar kan worden opgelegd (art. 257a Sv).

⁵⁴ Sinds de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen (USB) is de eindverantwoordelijkheid hiervoor bij de Minister van JenV belegd (*Stb* 2019 nr. 507), maar artikel 6:3:14 Sv houdt alsnog het openbaar ministerie verantwoordelijk voor het houden van toezicht op de naleving van gestelde voorwaarden.

De strafrechter beoordeelt of bewezen kan worden dat de verdachte zich heeft schuldig gemaakt aan het strafbare feit dat het openbaar ministerie vordert, en wat een passende straf is. Indien de strafrechter tot een veroordeling komt, weegt hij de persoonlijke omstandigheden van de verdachte en eventueel uitgebrachte adviezen (zoals van de Reclassering) mee. De strafrechter beslist ook of en zo ja, welke bijzondere voorwaarden worden opgelegd en kan bepalen dat de Reclassering wordt belast met het toezicht op de naleving en de begeleiding van de veroordeelde.

Reclassering

Begeleiden en toezicht houden om de kans op recidive te verkleinen

De Reclassering begeleidt en houdt toezicht op de veroordeelde in het gedwongen kader vanuit een tweeledig perspectief: het beschermen van de samenleving (door het voorkomen van nieuwe slachtoffers) en het begeleiden van de dader naar een gedragsverandering.⁵⁵ Haar taak is niet die van opsporing en het spreken van recht, maar vermindering van de kans op recidive door middel van gedragsbeïnvloeding. Dat doet de Reclassering op basis van wetenschappelijke inzichten.⁵⁶ Deze taak vervult de Reclassering op basis van een opgelegde strafrechtelijke interventie. Van deze interventie gaat dwang uit, waardoor het toezicht en de begeleiding ‘niet onderhandelbare’ elementen bevat.⁵⁷

Tegelijkertijd is binnen het gedwongen kader ruimte nodig om de begeleiding zo vorm te geven dat cliënten succesvol kunnen worden geholpen, met het oog op verandering van gedrag of omstandigheden, re-integratie en herstel. De mate van dwang en de ruimte om binnen de begeleiding te oefenen, leren, ontdekken en terug te vallen moeten voldoende in balans met elkaar zijn. Hoe dat vorm krijgt, wordt afgestemd op het individuele niveau, gelet op de waarden van de benodigde zorg, de veiligheid van de maatschappij en de autonomie van de cliënt/veroordeelde.⁵⁸

De combinatie van toezicht en begeleiding wordt aangeduid als ‘hybride werken’, waarbij de reclasseringsmedewerker de cliënt ‘controlerend begeleidt’, en ‘begeleidend controleert’.⁵⁹ Het interactieve proces tussen de reclasseringsmedewerker en de cliënt is voor een succesvol traject zeer van belang. De ‘werkalliantie’ verwijst naar de mate waarin het interactieve proces tussen cliënt en reclasseringsmedewerker zo verloopt, dat de cliënt in staat is het kader voldoende te accepteren, dat na verloop van tijd een voldoende werkbare samenwerking wordt bereikt bij het werken aan doelen en taken en dat de cliënt en reclasseringsmedewerker binding en voldoende vertrouwen in elkaars inzet ontwikkelen om vooraf gestelde doelen te realiseren.⁶⁰ De dynamiek in samenwerking tussen reclasseringsmedewerker en cliënt wordt beïnvloed door drie positieve kenmerken en een negatief kenmerk:⁶¹

- Richting en kader: de cliënt heeft voldoende duidelijkheid over de doelen van het traject (richting) en het juridisch kader (kader). De cliënt denkt dat reclasseringsmedewerker en hij het daarover eens zijn. De reclasseringsmedewerker schat in dat de doelen en het kader voldoende duidelijk zijn en dat zij het hierover voldoende eens zijn;

⁵⁵J. Bosker & A. Menger, *Werken in gedwongen kader*, Amsterdam: 2024, p. 28. De taken van de Reclassering zijn wettelijk vastgelegd in de Reclasseringsregeling 1995, zie artikel 8.

⁵⁶In het Nederlandse strafrecht, is naast vergelding een belangrijk doel die van de speciale preventie, ook wel het verminderen van recidive. De Reclassering heeft een taak voor dit doel van speciale preventie. J. Bosker & A. Menger, *Werken in gedwongen kader*, Amsterdam: 2024, p. 19.

⁵⁷Bosker & Menger, 2024, p. 23.

⁵⁸Bosker & Menger, 2024, p. 23-25, 42-43.

⁵⁹J. Bosker, J. Monnee-van Doornmalen, R. Henskens, D. van der Plaats, *Effectieve werkwijzen in het reclasseringstoezicht. Een systematisch literatuuroverzicht*. KFZ 2020, p. 18-19.

⁶⁰Bosker & Menger, 2024, p. 231-232.

⁶¹Bosker & Menger 2024, p. 231-232.

- Binding: de cliënt voelt zich voldoende gebonden en geëngageerd aan het traject en voelt zich gerespecteerd en ondersteund. De reclasseringsmedewerker schat in dat de cliënt zich gebonden voelt en dat deze gerespecteerd wordt en zich gesteund voelt. De reclasseringsmedewerker vindt zelf dat hij voldoende luistert en ondersteunend is;
- Vertrouwen: de cliënt ervaart dat hij zich genoeg kan uiten in het contact met de reclasseringsmedewerker, heeft voldoende vertrouwen in diens inzet en ervaart dat reclasseringsmedewerker hem voldoende vertrouwt. De reclasseringsmedewerker schat in dat de cliënt zich vrij genoeg durft te uiten en hem voldoende vertrouwt. De reclasseringsmedewerker denkt dat hij de cliënt voldoende kan vertrouwen;
- Stroefheid: de cliënt beleeft de interactie als negatief en vertoont veel tekenen van *reactance*.⁶² De reclasseringsmedewerker schat in dat de cliënt de interactie als negatief ervaart en ziet signalen van *reactance*. De reclasseringsmedewerker ervaart regie- en energieverlies bij zichzelf (*contra-reactance*).⁶³

Adviseren over passende bijzondere voorwaarden

Als expert in delictgedrag, de op- en afbouw van criminele carrières en de kans op recidive te verminderen, adviseert de Reclassering in het strafproces over passende bijzondere voorwaarden om iemand uit de criminaliteit te houden.⁶⁴ Dit doet de Reclassering op basis van *structured professional judgement*, door middel van een wetenschappelijk gevalideerd risicotaxatie-instrument, RISc.⁶⁵ Op basis hiervan worden de criminogene factoren, de beschermende factoren en de ondersteunende factoren gescoord, waarna de reclasseringsmedewerker op basis van zijn eigen kennis en ervaring deze factoren weegt, interpreteert, integreert en combineert tot een eindoordeel voor een schriftelijk advies aan bijvoorbeeld de rechter.⁶⁶ Daarnaast neemt de reclasseringsmedewerker in het advies een plan op om deze risico's op korte en lange termijn te beperken (risicomanagement). Hij spreekt hierover met de cliënt en beoordeelt of deze bereid is mee te werken aan de voorgestelde bijzondere voorwaarden, en of de voorwaarden passend (proportioneel) en uitvoerbaar zijn.

Een van de belangrijke modellen die ten grondslag ligt aan risicoanalyse en begeleiding in het gedwongen kader is die van de *Risk-Need-Responsivity*.⁶⁷ Dit model schrijft voor dat de aard van het recidiverisico en de intensiteit van de behandeling op elkaar moeten zijn afgestemd. De interventie moet zijn gericht op dynamische veranderbare criminogene factoren en moet worden afgestemd op specifieke kenmerken van cliënten, zoals motivatie, leerstijl en intellectuele mogelijkheden.⁶⁸

De risicotaxatie wordt voortdurend herijkt. In het risicomanagement is de reclasseringsmedewerker alert op signalen van oplopend risico op herhaald delictgedrag (hierna: *risicovol gedrag*).⁶⁹ Daarvoor moet de reclasseringsmedewerker weten welke signalen bij een cliënt wijzen op een verhoogd risico. Voor meer specifiek inzicht kunnen een delictscenario of een signaleringsplan worden gemaakt.⁷⁰ Voorbeelden van signalen van risicovol gedrag zijn: onderlinge afspraken of gedragsregels worden niet nageleefd, uit de gesprekken blijkt dat het niet goed gaat en de cliënt

⁶²Met *reactance* wordt bedoeld: weerstand tegen verandering in het gedwongen kader. Zie Bosker & Menger 2024, p. 223.

⁶³Bosker & Menger 2024, p. 231-232.

⁶⁴<https://werkenbij.reclassering.nl/over-ons/>; Zie artikel 8, eerste lid, onderdeel a, Reclasseringsregeling 1995.

⁶⁵ <https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc> Voor zedendelinquenten wordt hierbij voor betere uitkomsten een geïntegreerde verdiepende module gebruikt, de SSA. Bosker & Menger, 2024, p. 138-140.

⁶⁶ Bosker & Menger 2024, p. 138.

⁶⁷ Andrews, D. A., Zinger, I., Hoge, R. D., Bonta, J., Gendreau, P., Cullen, F. T., et al. 'Does correctional treatment work? A clinically relevant and psychologically informed meta-analysis.' *Criminology* 1990, 28, p. 369-404.

⁶⁸ Bosker & Menger 2024, p. 88-94; D.A. Andrews, J. Bonta, & R.D Hoge, Classification for effective rehabilitation: Rediscovering psychology. *Criminal Justice and Behavior* 1990, 17, 19-52.

⁶⁹ Bosker & Menger 2024, p. 158.

⁷⁰ Bosker & Menger 2024, p. 158.

weer richting het delictgedrag gaat of er wordt een bijzondere voorwaarde overtreden. Controle geeft de reclasseringsmedewerker zicht op risicovol gedrag en op de vraag of de voorwaarden worden nageleefd. Vormen van controle zijn bijvoorbeeld de gesprekken met de cliënt, middelencontrole en de controle van digitale gegevensdragers. Op die manier kan de begeleiding en het toezicht waar mogelijk bijgesteld worden ten behoeve van het risicomangement en de beoogde gedragsverandering.

De betrokkene: verdachte/dader/veroordeelde/cliënt

De persoon die centraal staat in het strafrechtelijke onderzoek, in de strafzaak en bij de ten uitvoerlegging van de straf, wordt aangeduid met verschillende termen. Degene die wordt verdacht van het downloaden of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen is een verdachte. Er wordt onderscheid gemaakt in type verdachte afhankelijk van de ernst van het delict. Als het tot een veroordeling komt wordt de verdachte dader of veroordeelde. Komt hij onder het toezicht van de Reclassering te staan, dan wordt hij door Reclassering aangeduid als cliënt.

Uit interviews met experts en ervaringen met betrokkenen uit de praktijk is gebleken dat de daders van delicten op het gebied van het downloaden of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen verschillende achtergronden kunnen hebben, en dat het in het merendeel van de gevallen om mannen gaat. Wetenschappelijk onderzoek bevestigt dat het een heterogene groep betreft met verschillende motivaties, gedrag en psychologische karakteristieken.⁷¹ Hierna volgen enkele beschrijvingen van de mogelijke typen daders die in de praktijk herkend worden. Het gaat hierbij niet om daderprofielen, omdat deze beschrijvingen onvoldoende wetenschappelijk gevalideerd zijn. Deze beschrijvingen zijn opgehaald bij een expert van de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen en komen voort uit de forensische zorg.

Het eerste type betreft een groep die overwegend in een sociaal isolement leeft, vaak moeite heeft met het aangaan en onderhouden van sociale relaties en op latere leeftijd nog alleenstaand is. Het tweede type betreft daders die een gezin, baan en huis hebben, waarvan men het in eerste instantie niet verwacht. Dit type heeft veel te verliezen bij een vervolging. Het derde type betreft daders die niet alleen dit delict plegen, maar ook soortgelijke delicten, zoals het vergaren van ander extreem beeldmateriaal. Het kan ook gaan om het plegen van geheel andere delicten, zoals gewelds- of vermogensdelicten. Ten slotte is er een vierde dadertype met een pedoseksuele geaardheid, met een drang om naar dergelijk materiaal te kijken.

Wat de eerste drie dadertypen met elkaar gemeen hebben, is dat zij zich over het algemeen niet herkennen in de pedoseksuele geaardheid. Zij hebben andere redenen om het materiaal te downloaden, al kan er wel een bepaalde seksuele motivatie achter zitten. Kenmerkend voor een deel van deze daders, zeker de daders uit de eerste twee beschrijvingen, is dat zij zich schamen voor het gedrag, het gedrag doorgaans afkeuren en gemotiveerd zijn om dit gedrag te veranderen. Daardoor zijn zij bijvoorbeeld ook geneigd snel akkoord te gaan met de bijzondere voorwaarden die hen worden opgelegd.

Ten slotte is er een deel van het type met een pedoseksuele geaardheid dat geen berouw heeft of dat hun delictgedrag ontkent of bagatelliseert. Dat is een type waarvan het gedrag lastig is te beïnvloeden en dat sneller terugvalt in het strafbare gedrag dan de andere typen. Een deel van het type met een pedoseksuele geaardheid heeft wel motivatie om zich te onthouden van het gedrag en is bereidwillig om mee te werken aan de bijzondere voorwaarden.

⁷¹ H. Bale, *Online Child Sexual Offending: Psychological Characteristics of Offenders and the Process of Exploitation*, University of Edinburgh: 2017.

Wat betreft de technische kennis en online competenties van de daders, weten de daders volgens de politie bovengemiddeld veel, maar het merendeel is niet bekwaam en gebruikt geen hoogwaardige technieken om het materiaal af te schermen. Een kleinere groep is technisch wel bekwaam, en is in staat het materiaal met behulp van techniek goed te verbergen. Wel blijft dat continu discipline en motivatie vergen, wat niet iedereen kan opbrengen. Daardoor kan ook deze groep tegen de lamp lopen. Of er een verband is tussen technische kennis en de beschreven typeringen van daders, is onduidelijk.

5.3 Ontstaan van de controle: INDIGO-afdoening van zedenzaken

De bestrijding van het downloaden of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen en kinderseksuïerisme is sinds 2012 een van de speerpunten van de Nationale Politie en is een van de vijf korpsprioriteiten in de gemeenschappelijke Veiligheidsagenda.⁷² Vanwege de ontwikkeling in technologie en internet nam het aanbod van materiaal van seksuele uitbuiting van kinderen in die periode enorm toe. In 2011 ontwikkelde het openbaar ministerie in Rotterdam in samenwerking met de politie, de Reclassering en een forensisch behandelinstituut een nieuwe afdoeningsmethode: Niets Doen Is Geen Optie (INDIGO).

Deze aanpak, waarbij de controle van digitale gegevensdragers een onderdeel is van een bredere gedragsbeïnvloedende interventie, is gericht op een alternatieve, maar bovenal snellere afdoening van deze zaken. De controle van digitale gegevensdragers stond dus nooit op zichzelf, maar vormde altijd onderdeel van een interventie die erop gericht is het gedrag van de betrokkene te beïnvloeden, bijvoorbeeld door behandeling. INDIGO betrof een nieuwe, lokale aanpak en werd na positieve ervaringen landelijk uitgerold. De methode werd sinds 2012 mogelijk als een voorwaarde bij het voorwaardelijk sepot op het gebied van zaken waarbij sprake was van het downloaden of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen. In 2013 werden werkafspraken tussen politie, OM en Reclassering vastgelegd in een stroomschema.⁷³

De aanleidingen voor de start van de INDIGO-afdoening waren de forse werkvoorraden bij de eenheden, het feit dat zaken te lang bleven liggen en dat deze veel onderzoekscapaciteit vergden. Door middel van INDIGO kan snel een hulpverleningstraject worden ingezet (wat vaak ook de uitkomst van een rechtszaak zou zijn). Dit kostte de politie veel minder tijd en de overheid gaf hiermee bovendien een signaal af dat ook zogenoemde simpele downloadzaken werden opgepakt.⁷⁴

Het doorzoeken van digitale gegevensdragers was voor 2012 overigens ook al mogelijk, maar dan uitsluitend in het kader van de opsporing en uitgevoerd door de politie. Met de introductie van INDIGO werd het doorzoeken van digitale gegevensdragers ook toegepast in het kader van het reclasseringstoezicht.

De officier van justitie kan onder bepaalde voorwaarden besluiten tot een INDIGO-afdoening. Juridisch gezien is dit een voorwaardelijk sepot; dat houdt in dat de politie geen verder onderzoek meer uitvoert. Het doel van INDIGO is tweeledig: 1) het voorkomen van recidive en 2) meer efficiëntie: het besparen van kostbare opsporingscapaciteit en een snelle afdoening van de zaak. Voorwaarden om in aanmerking te komen voor een INDIGO-afdoening zijn dat de verdachte een *first offender* is en dat sprake is van slechts een beperkte mate van bezit of verspreiding van materiaal van seksuele uitbuiting van kinderen. Wanneer de zaak via INDIGO wordt afgedaan

⁷² Veiligheidsagenda politie 2015-2018.

⁷³ Werkproces Indigo Den Haag (politie, OM, Reclassering, Waag, cq andere GGZ instelling) d.d. 20 augustus 2013.

⁷⁴ A. van Wijk e.a. Niet meer doen. Een onderzoek naar de INDIGO-afdoening, Den Haag, 2019.

ontloopt de verdachte strafvervolging, maar komt deze wel verplicht onder toezicht van de Reclassering. Indien uit een controle blijkt dat de betrokkene de fout in is gegaan, dan wordt het INDIGO-traject stopgezet.⁷⁵

In de evaluatie van het INDIGO-traject in 2019 wordt positief geoordeeld over de werkwijze. Met name omdat het om een doelgroep gaat die vooral gebaat is bij hulpverlening en niet of minder bij een strafrechtelijk onderzoek en de gevolgen van een rechtszaak.⁷⁶

5.4 Uitbreiding naar andere strafrechtelijke titels

Nadat de nodige ervaring was opgedaan met de INDIGO-afdoening ontstond bij zowel het openbaar ministerie als de Reclassering de wens om de controle van digitale gegevensdragers ook bij andere titels te kunnen toepassen. Het was immers niet logisch dat de controle wel werd ingezet bij een voorwaardelijk sepot, maar niet bij afdoeningen van ernstiger feiten. Juist in die gevallen is het belangrijk om te controleren, zoals bij een tbs'er met proefverlof. Uit gesprekken met de Reclassering blijkt dat om die reden na de evaluatie van het INDIGO-project werd besloten om controle van digitale gegevensdragers voortaan ook bij andere titels in te zetten, waaronder de voorwaardelijke veroordeling en de tbs onder voorwaarden. Dit onderzoek richt zich, zoals gezegd, op de voorwaardelijke veroordeling en de mogelijkheid om daaraan bijzondere voorwaarden te verbinden.

5.5 Afspraken over de uitvoering van de controle

De controle van digitale gegevensdragers is een technische aangelegenheid waarvoor specifieke kennis vereist is. Reclasseringsmedewerkers bleken doorgaans niet over de kennis te beschikken om deze controles uit te voeren. Hiervoor dient men om te kunnen gaan met de software, maar ook te weten hoe digitale gegevensdragers werken en hoe de resultaten van het softwareprogramma geïnterpreteerd moeten worden. Volgens de politie is voor de technische uitvoering minimaal een HBO ICT-opleiding nodig.

Uit de gesprekken blijkt dat het openbaar ministerie, de politie en de Reclassering afspraken hebben gemaakt waarin zij regelden hoe de controles in de praktijk zouden worden uitgevoerd. In de afspraken over de controle werd de technische uitvoering als taak bij de politie neergelegd; de controles zouden op aanvraag van de Reclassering worden uitgevoerd door digitaal specialisten van de politie. De politie zou jaarlijks maximaal vijftig controles uitvoeren, gelijkelijk verdeeld over de regionale politie-eenheden.

5.6 Nieuwe afspraken over de uitvoering van de controle

De Hoge Raad gaf in zijn arrest uit 2016 richtlijnen over de wijze van controle en aan welke voorwaarden de controle zou moeten voldoen (zie daarover paragraaf 3.3). Omdat de vigerende werkwijze daarmee niet in overeenstemming was, is in 2017 een nieuwe werkwijze vastgesteld conform het arrest van de Hoge Raad. Door dit arrest moet in de rechterlijke uitspraak – en dus ook

⁷⁵ A. van Wijk e.a. Niet meer doen. Een onderzoek naar de INDIGO-afdoening, Den Haag, 2019.

⁷⁶ A. van Wijk e.a. Niet meer doen. Een onderzoek naar de INDIGO-afdoening, Den Haag, 2019.

in het reclasseringsadvies – onder andere zo precies mogelijk worden geformuleerd aan welke gedragsvoorwaarde(-n) de veroordeelde zich moet houden, wat de frequentie van de controle is en hoe de controle dient uitgevoerd te worden.⁷⁷ De voorwaarde moet bijdragen aan het voorkomen van onwenselijke of aan strafbaarheid grenzende gedragingen.

In het interne handelingskader van de Reclassering uit 2017 is wederom bepaald dat de controles op aanvraag van de Reclassering worden uitgevoerd door digitaal specialisten van de politie. Indien uit die controle een verdenking van een strafbaar feit voortvloeit, meldt de Reclassering dit direct aan het openbaar ministerie. Uit het handelingskader volgt dat de politie en de Reclassering samen bepalen wanneer de controle van de digitale gegevensdragers plaatsvindt. Wanneer de toezichthouder daartoe aanleiding ziet, kan controle worden voorgesteld en wordt samen met de politie bepaald of deze zal worden uitgevoerd. Dit kan zijn in geval van een onderbouwde zorg om mogelijke recidive, bijvoorbeeld gebaseerd op concrete signalen, risicofactoren of om indrukken.

Volgens de werkwijze brengen de politie en de Reclassering gezamenlijk een onaangekondigd huisbezoek. Indien tijdens de controle strafbaar materiaal wordt aangetroffen, verleent de politie de cautie en zet hij opsporingsbevoegdheden in om de digitale gegevensdrager(s) in beslag te nemen. Nadere controle van de gegevensdrager vindt vervolgens plaats indien het openbaar ministerie een opsporingsonderzoek start.⁷⁸

5.7 Controle van digitale gegevensdragers als bijzondere voorwaarde

Wanneer het openbaar ministerie besluit tot vervolging over te gaan, hebben de officier van justitie en de rechter verschillende mogelijkheden om een combinatie van bijzondere voorwaarden te vorderen respectievelijk op te leggen die het best passen bij het risicoprofiel van een zedendelinquent. Dat proces is als volgt vormgegeven.

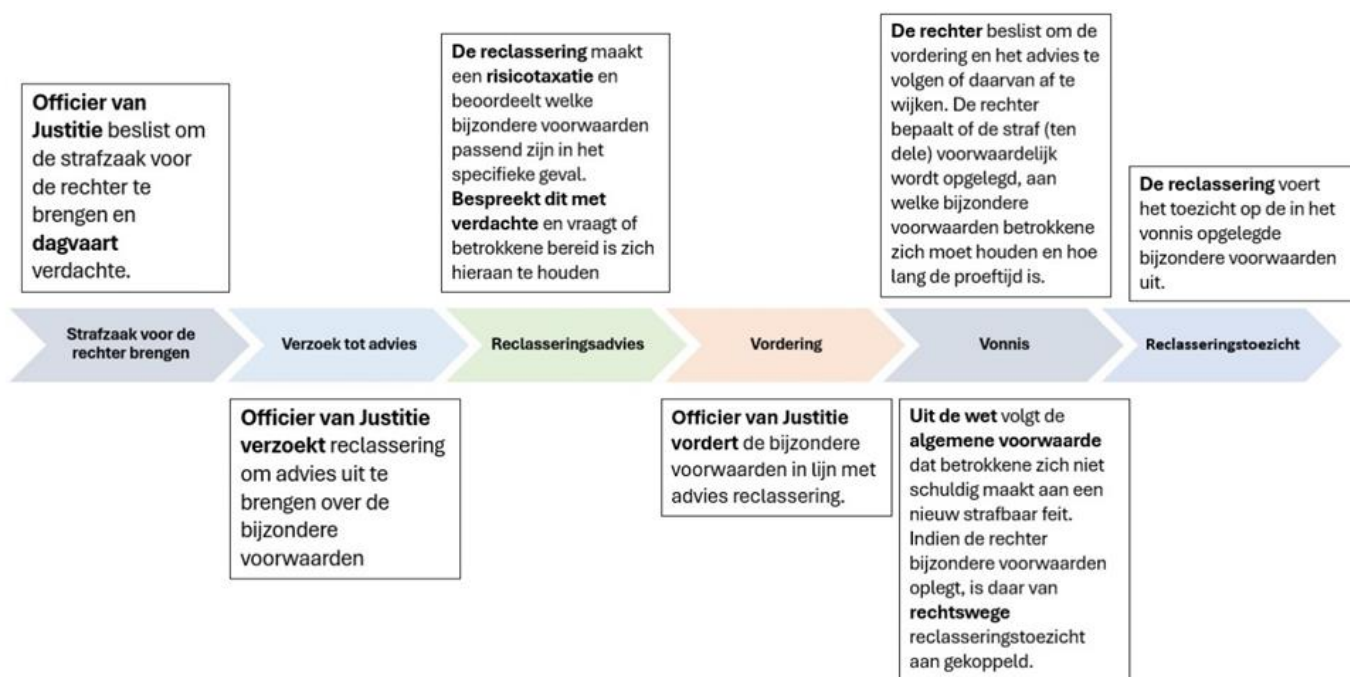
De officier van justitie beslist de strafzaak voor de rechter te brengen en dagvaardt de verdachte. Vervolgens verzoekt hij de Reclassering om advies uit te brengen over eventueel op te leggen bijzondere voorwaarden. De Reclassering maakt een taxatie van het recidiverisico door middel van RISC,⁷⁹ onderzoekt welke bijzondere voorwaarden in het concrete geval ondersteunend zijn om het risico op recidive terug te brengen, of deze bijzondere voorwaarden uitvoerbaar en haalbaar zijn en bespreekt in dat kader met de verdachte of hij bereid is zich hieraan te houden. Vervolgens brengt de Reclassering advies uit.

De officier van justitie bepaalt zelf of de voorwaarde wordt gevorderd, maar vordert de bijzondere voorwaarde doorgaans in lijn met het advies van de Reclassering. De rechter beslist uiteindelijk de vordering van de officier en het reclasseringsadvies te volgen of daarvan af te wijken. De rechter maakt een afweging en kan vervolgens in zijn vonnis de bijzondere voorwaarde opleggen. De Reclassering voert het toezicht uit op de naleving van de door de rechter opgelegde bijzondere voorwaarde en begeleidt de veroordeelde. Dit proces ziet er als volgt uit:

⁷⁷ Zie voor een uitgebreide beschrijving van het juridisch kader hoofdstuk 3.

⁷⁸ Werkafspraken bijzondere voorwaarden in zedenzaken Controle van digitale gegevensdragers, versie juni 2017.

⁷⁹ Zie hiervoor. <https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc>



Figuur 4. procesbeschrijving oplegging bijzondere voorwaarde⁸⁰

5.8 De praktijk

In de interviews met ketenpartners is de praktijk van de uitvoering van de controle in beeld gebracht. Daarbij moet worden opgemerkt dat de controle in de praktijk verschilde, vanwege bijvoorbeeld verschillen in de formulering van de bijzondere voorwaarde, de bereidheid en beschikbaarheid van de politie om de controle uit te voeren, de intensiteit van het toezicht en de werkwijze van de individuele reclasseringsmedewerker. Wel is uit de gesprekken een algemene lijn te halen, die hieronder is beschreven.

Vanwege de veiligheid van de reclasseringsmedewerker werd in de meeste gevallen de controle vooraf aangekondigd aan de betrokkene, terwijl in sommige vonnissen werd aangegeven dat dit onaangekondigd moest. Aangekondigde controle gebeurde zodanig dat de betrokkene niet het precieze moment van de controle wist: hij kreeg het bericht dat hij op korte termijn een huisbezoek kon verwachten waarbij tevens een controle zou kunnen plaatsvinden. De tijdens het huisbezoek door de cliënt overhandigde digitale gegevensdragers werden gecontroleerd. Van een doorzoeking tijdens het huisbezoek was geen sprake; de bijzondere voorwaarde scheidt namelijk geen bevoegdheid om de woning te doorzoeken. Tijdens eerdere toezichtgesprekken tussen Reclassering en de veroordeelde werd gevraagd welke gegevensdragers de betrokkene in bezit had zodat daarop gelet kon worden als er een controle zou gaan plaatsvinden. Ook als eerdere huisbezoeken plaatsvonden, werd gekeken welke gegevensdragers zichtbaar waren. Mochten bepaalde digitale gegevensdragers, die wel eerder waren gezien of waarover men had gehoord, niet worden overhandigd, dan kon daarnaar worden gevraagd.

⁸⁰ Het schema gaat over een voorwaardelijke veroordeling. De schorsing, proefverlof, een voorwaardelijke invrijheidstelling kennen een andere routing.

De Reclassering mag niet zonder toestemming de woning van de cliënt binnentreden. Medewerking van de betrokkene was dus noodzakelijk om de controle uit te kunnen voeren. Hiervoor werd zijn toestemming gevraagd. Indien de cliënt zijn medewerking weigerde, vond er geen controle plaats en leverde dit een schending van de bijzondere voorwaarde op waar in beginsel terugkoppeling aan het openbaar ministerie over plaatsvond.

Indien de veroordeelde medewerking verleende door zijn geautomatiseerde werk zelf te ontgrendelen of door het wachtwoord te geven, kon de digitaal specialist van de politie de feitelijke controle aan de digitale gegevensdrager uitvoeren. Daarbij werd gebruik gemaakt van een USB-stick met een geautomatiseerd softwareprogramma in de vorm van een 'hit/no-hit systeem', dat in staat was om de bestanden op een gegevensdrager te vergelijken met een database van uit eerder politieonderzoek bekende versleutelde bestanden van seksuele uitbuiting van kinderen. Ook werd met behulp van een woordenlijst gezocht naar bepaald woordgebruik op de gegevensdrager. Met de software kon zowel risicovol gedrag als strafbaar gedrag gedetecteerd worden.

De software toont zaken als afbeeldingen op de gegevensdrager die mogelijk seksuele uitbuiting van kinderen inhouden, de mappenstructuur, browsergeschiedenis (waaronder een zwarte lijst van websites waarop wordt gescand), lokale archieven, de aanwezigheid van versleutelingssoftware, het gebruik van een VPN (gebruikt om het IP-adres te verhullen), het gebruik van bijvoorbeeld een TOR-browser waarmee internetverkeer niet meer te traceren is (een onder meer door plegers van online zedendelicten veelgebruikte browser) en de aanwezigheid van bepaalde applicaties. De tool bevat een lijst van applicaties waarvan aanwezigheid op de digitale gegevensdrager interessant kan zijn, omdat deze applicaties mogelijk aanwijzingen geven dat de cliënt risicovol gedrag vertoont. De software toont dus uitsluitend informatie die in het licht van de controle en het risicovolle of strafbare gedrag dat kenmerkend is voor dit delict relevant kan zijn. Overige niet-relevante (persoonlijke) informatie wordt niet getoond. Het softwareprogramma verwerkt hierbij (bijzondere) persoonsgegevens, maar slaat enkel items op die hits opleveren. Het softwareprogramma kent bepaalde beperkingen. Zo werkt dit niet voor alle typen besturingssystemen.

Ten slotte was er een mogelijkheid dat de digitaal specialist handmatig in de gegevensdrager van de veroordeelde keek. Uit de gesprekken met de politie is gebleken dat soms handmatige controles hebben plaatsgevonden, maar gelet op het uitgangspunt van de werkwijze dat de controle geautomatiseerd wordt uitgevoerd, zal het aantal handmatige controles beperkt zijn geweest.

Uit de gesprekken blijkt dat voor de uitvoering van de controle door de Reclassering en politie het vonnis leidend was, tenzij dit in de praktijk onuitvoerbaar bleek te zijn. De Reclassering hield daarbij vast aan de standaard controlemethodiek van de politie via de software op de USB-stick, die bepaalde zoekmodaliteiten mogelijk maakte. Wat de uitvoering van de controle complex maakte is dat de rechter in zijn vonnis vaak andere formuleringen hanteerde dan de Reclassering in haar adviezen. Dat kon de toezichthouder van de Reclassering in een lastige positie brengen vanwege de soms praktische onuitvoerbaarheid van hetgeen de Reclassering werd opgedragen door de rechter. Het uitgangspunt was desalniettemin om de controle op zodanige wijze uit te voeren dat deze zoveel mogelijk in overeenstemming was met wat de rechter in het vonnis had bepaald.

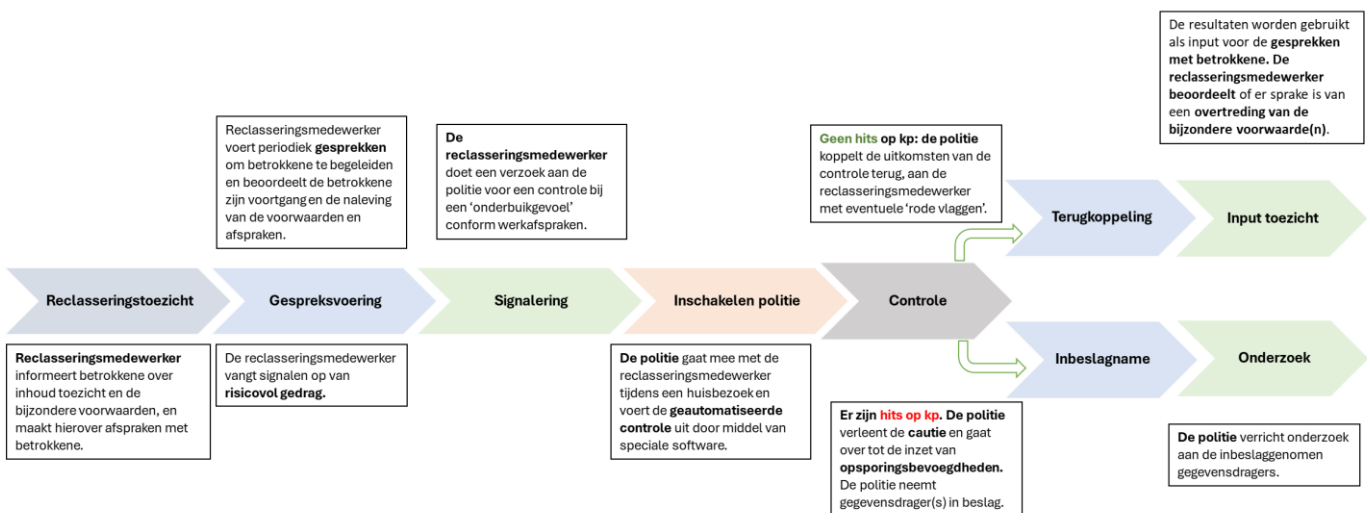
Het Kenniscentrum Cybercrime van het Gerechtshof Den Haag heeft voor de rechterlijke macht een modelformulering op zijn kennisbank gepubliceerd die gebaseerd is op de formulering van de voorwaarde die de toets van de Hoge Raad heeft doorstaan. Per onderdeel is een toelichting gegeven waarom bepaalde afwegingen zijn gemaakt. Het doel daarvan is om rechters op weg te

helpen met de formulering van de bijzondere voorwaarde, en te verduidelijken waarom bepaalde elementen opgenomen dienen te worden. De Reclassering en het openbaar ministerie hebben laten weten dat ook deze modelformulering volgens hen niet de oplossing is voor de ervaren uitvoeringsproblemen. Het openbaar ministerie en de Reclassering ontwikkelden nu zelf een bouwsteen voor de formulering van de bijzondere voorwaarde en het toezicht daarop.

5.9 Opvolging uitkomsten controle

Wanneer tijdens de controle geen strafbaar materiaal werd aangetroffen, koppelde de politie de uitkomsten van de controle terug aan de reclasseringsmedewerker met eventuele aandachtspunten of 'rode vlaggen' of signalen waarbij alertheid geboden was. De resultaten van de controle dienden vervolgens als input voor de periodieke gesprekken tussen de reclasseringsmedewerker en de betrokkene in het kader van het toezicht.

Indien wel strafbaar materiaal werd aangetroffen tijdens de controle verleende de politie de cautie, werd overgegaan tot de inzet van opsporingsbevoegdheden en werd de gegevensdrager in beslag genomen, waarop de politie nader onderzoek verrichtte. Het proces tot en met de uitvoering van de controle aan de digitale gegevensdragers zoals dat in de praktijk werd gevolgd, is hieronder weergegeven:



Figuur 5. Stroomschema uitvoering van de controle en opvolging

In het geval strafbaar materiaal werd aangetroffen tijdens de controle meldde de Reclassering aan het Centraal Justitieel Incassobureau (CJIB) dat de bijzondere voorwaarde niet was nageleefd en bracht de Reclassering advies uit over de wenselijke vervolgstappen aan het openbaar ministerie. In de praktijk had de Reclassering ook meestal direct contact met het openbaar ministerie. De politie meldde aan de officier van justitie dat een nieuw strafbaar feit was gepleegd. De officier van justitie

maakte op basis van de meldingen een afweging en besliste over de vervolgstappen. Dit kon leiden tot:

1. Het vervolgen voor een nieuw strafbaar feit;
2. Het vorderen van de tenuitvoerlegging van de voorwaardelijke straf of de wijziging van de bijzondere voorwaarde(n);
3. Vervolgen + vorderen tenuitvoerlegging;
4. Voorwaardelijk strafdeel ongewijzigd voortzetten.

5.10 Effectiviteit van de controle

Voor de vraag in hoeverre de controle van gegevensdragers effectief is, is het precieze doel dat wordt nagestreefd met de controle van belang. Uit hoofdstuk 3. volgt dat het doel van de bijzondere voorwaarde is om strafbaar gedrag te voorkomen door het goede levensgedrag van de veroordeelde te bevorderen. Met de controle kan toezicht worden gehouden op dit gedrag, zodat dit waar nodig kan worden bijgestuurd. Vanuit dat gezichtspunt bekijken we de effectiviteit.

Opgemerkt moet worden dat door een gebrek aan cijfers en wetenschappelijk onderzoek naar deze specifieke interventie geen harde uitspraken kunnen worden gedaan over de effectiviteit. Deze beperkingen worden hieronder toegelicht.

Ontbreken van of gebrek aan inzicht cijfers

Voor zover bekend is niet bijgehouden wat de precieze uitkomsten van de controles waren (dus in hoeveel gevallen risicovol gedrag of strafbaar gedrag werd geconstateerd) en wat vervolgstapen waren. Om hierover iets te kunnen zeggen, kunnen wij ons enkel baseren op ervaringen van de gesprekspartners.

Ontbreken wetenschappelijk onderzoek

Er is vooralsnog geen wetenschappelijk onderzoek gedaan naar de effectiviteit van de controles. In de interviews is aangegeven dat onderzoek naar effectieve manieren om recidive te verminderen in zijn algemeenheid een uitdaging is.⁸¹ Daarnaast is uit de interviews gebleken dat het erg lastig is om effecten toe te schrijven aan een specifieke interventie als deze onderdeel is van een breder palet aan maatregelen. De bijzondere voorwaarde (en de dreiging die hiervan uitgaat vanwege een mogelijke controle) en de daadwerkelijke controle zijn altijd onderdeel van zo'n breder palet. Ook behandeling, begeleiding en training, gericht op gedragsbeïnvloeding kunnen hiervan deel uitmaken.

Daarom kan de effectiviteit slechts op algemene wetenschappelijke inzichten en op de opgehaalde inzichten en ervaringen van de gesprekspartners worden gebaseerd. Er is voor gekozen om op basis hiervan een aantal kenmerken te beschrijven die van invloed zijn op de effectiviteit van de controle.

Risk-Need-Responsivity

Bij de risicotaxatie en het advies over passende bijzondere voorwaarden sluit de Reclassering aan bij de beschikbare wetenschappelijke inzichten. Vanuit wetenschappelijk onderzoek zijn er wel algemene inzichten beschikbaar over de inzet van gedragsmaatregelen om recidive te voorkomen die bruikbaar zijn voor de inzet van de controle van digitale gegevensdragers. Een voorbeeld is het

⁸¹Zie voor een algemene bespreking over de effectiviteit van behandelingen onder andere: E. Post, *De kunst van het straffen? Forensische zorg als premisse*, diss. Vrije Universiteit 2023, p. 316-326.

Risk-Need-Responsivity model – beschreven in paragraaf 5.2 – dat aangeeft dat de intensiteit van behandeling moet zijn afgestemd op het risico. Als sprake is van een lage recidivekans, is het niet wenselijk is om in te zetten op een hoge controle-intensiteit, omdat dit averechts kan werken. De Reclassering speelt hierop in, door in het reclasseringsadvies deze afweging te maken en daarop de voorgestelde maatregelen af te stemmen.

Dreiging van controle

Verondersteld wordt dat van het opleggen van de bijzondere voorwaarde en de dreiging dat de betrokkene gecontroleerd wordt, een gewenst effect uitgaat, namelijk dat het de betrokkene weerhoudt van een terugval in het oude gedrag. De dreiging moet wel voldoende reëel zijn. Het feit dat slechts een beperkte groep daadwerkelijk gecontroleerd werd, doet afbreuk aan deze dreiging en daarmee de effectiviteit.

Type dader

Uit de gesprekken met betrokkenen is gebleken dat de effectiviteit mede afhangt van het type dader. Geïnterviewde gesprekspartners gaven aan dat bekend is uit de praktijk er een doelgroep is die stelt gebaat te zijn bij oplegging van de bijzondere voorwaarde en bij de controles. Het gaat om de groep die zou willen dat ze geen drang hebben om het gedrag te vertonen en daarom graag zelf via (de mogelijkheid van) controle een stok achter de deur willen hebben om dat gedrag na te laten. Voor die groep kan de controle heel effectief zijn, op voorwaarde dat zij ervan uit kunnen gaan dat de controle ook daadwerkelijk bij hen wordt uitgevoerd. Aan de andere kant van het spectrum zit een dadergroep die moeilijker te controleren is, doordat deze groep gemotiveerd is het online gedrag te verhullen. Toch is de ervaring dat ook deze groep op den duur tegen de lamp kan lopen, doordat het verhullen constante motivatie vergt en omdat het een doelgroep betreft die door een vorm van dwangmatigheid opnieuw het gedrag vertoont.

Intensiteit van de zoekslag

Verondersteld wordt dat naarmate de intensiteit van de zoekslag toeneemt, er meer risicovol gedrag en/of strafbaar materiaal kan worden aangetroffen. De intensiteit is afhankelijk van de vraag hoeveel gegevensdragers gecontroleerd worden en hoe de controle wordt uitgevoerd: wat kan de software wel en niet detecteren? Of gebeurt de controle handmatig, en hoe intensief is de zoekslag van de controleur in dat geval?

Bij het uitvoeren van de controle werden uitsluitend die gegevensdragers gecontroleerd die de betrokkene aandroeg of die door de toezichthouder werden waargenomen. Het was, zo lijkt het, op het eerste gezicht dus heel eenvoudig voor de betrokkene om andere gegevensdragers te verbergen voor de controle. In gesprekken met de Reclassering wordt erkend dat die mogelijkheid bestaat en dat die zich in de praktijk ongetwijfeld zal voordoen. Toch worden de controles zinvol geacht, gelet op de bovengenoemde kenmerken van de typen daders en de dwangmatigheid in het gedrag.

Bovendien is een waterdichte controle volgens gesprekspartners niet noodzakelijk om effectief te kunnen zijn. De huidige software die wordt gebruikt voor de controles levert in voldoende mate bruikbare aanknopingspunten voor het gesprek en voor eventuele vervolgstappen. Voorbeelden zijn het zoeken op bepaalde trefwoorden, het bezoeken van bepaalde websites of het gebruiken van bepaalde applicaties. Het omzeilen van het softwareprogramma is mogelijk, maar het geeft wel indicaties dat een cliënt dit heeft geprobeerd, bijvoorbeeld door de aanwijzing dat er iets gewist is. Het softwareprogramma kan niet achterhalen welke inhoud gewist is. Een beperking van de software die meer impact heeft op effectiviteit en toepassingsbereik is dat deze niet werkt voor alle beschikbare besturingssystemen.

Inzicht in de digitale modus operandi

Uit de gesprekken is het belang naar voren gekomen van inzicht in de handelwijze van betrokkene voor een effectieve controle van diens digitale gegevensdragers. Elke zedendelinquent kent immers zijn eigen online zoekmethoden, voorkeursapplicaties en digitale gedragspatronen. Wanneer uit het dossier van de cliënt blijkt dat hij het strafbare materiaal altijd via bepaalde Telegram-kanalen verzamelde en tijdens de controle blijkt dat hij opnieuw actief is geweest op Telegram, kan dit een signaal zijn van risicovol gedrag.

Voor een andere cliënt kan diezelfde constatering juist helemaal niet van belang zijn, omdat bekend is dat hij hele andere zoekmethoden of digitale gedragspatronen hanteert. Kortom, inzicht in de modus operandi van de betrokkene kan van grote meerwaarde zijn bij de beoordeling en interpretatie van de bevindingen bij de controle en de effectiviteit ervan vergroten. Uit de gesprekken blijkt echter dat het inzicht in de handelwijze van de cliënt niet (altijd) bekend was bij degene die de controle uitvoerde. Dat kan ertoe hebben geleid dat bepaalde bevindingen van risicovol gedrag uit de controle niet op waarde zijn geschat.

5.11 Knelpunten in de praktijk

Naar aanleiding van de evaluatie van de INDIGO-afdoening zijn medio 2022 de strafrechtelijke titels waarvoor de controle kon worden opgelegd uitgebreid. Dit leidde tot een onvoorziene en zeer flinke toename van het aantal uit te voeren controles. Werden volgens gesprekspartners medio 2012 circa 20 keer bijzondere voorwaarden opgelegd, medio 2022 waren dit er circa 300 en eind 2023 meer dan 460.

Deze toename knelde met de beperkte capaciteit die de politie hiervoor beschikbaar kon stellen. De Reclassering en de politie waren overeengekomen dat de politie bij vijftig controles ondersteuning kon bieden.

Dit leidde tot noodgedwongen risicoselectie: de bijzondere voorwaarde werd uiteindelijk jaarlijks honderden keren opgelegd, terwijl er maar ruimte was voor vijftig controles. Gezien de beperkte capaciteit bij de politie werden de controles op hun verzoek alleen uitgevoerd bij degenen bij wie (sterke) signalen bestonden van overtreding van de voorwaarden. Deze signalen konden bijvoorbeeld voortkomen uit de contacten van de reclasseringswerker met de veroordeelde of uit diens directe omgeving.

Ervaren knelpunten bij de politie

De politie heeft zich in de Veiligheidsagenda's van 2019-2022 en 2023-2026 ten doel gesteld om bij de aanpak van online seksueel misbruik in te zetten op een zo groot mogelijk (maatschappelijk) effect en om de interventies zoveel mogelijk te richten op vervaardigers en verspreiders van materiaal van seksuele uitbuiting van kinderen, misbruikers, *keyplayers* en (internationale) netwerken. Controle van gegevensdragers bij cliënten zonder dat er (sterke) signalen zijn die wijzen op aanwezigheid van verboden beeldmateriaal verhoudt zich slecht met deze doelstelling. Om bij alle toezichtopdrachten jaarlijks controles uit te voeren, zou een forse uitbreiding van de controlecapaciteit nodig zijn. De politie heeft aangegeven hier onvoldoende capaciteit voor vrij te kunnen maken.

Daarnaast bleken er voor de politie verschillende juridische bezwaren te bestaan, omdat de controle op de naleving van door de officier van justitie of rechter opgelegde bijzondere voorwaarden in principe een taak van de Reclassering is. De Reclassering heeft andere taken en bevoegdheden dan de politie. Wanneer de politie (opsporingsambtenaar) ter technische ondersteuning van de

Reclassering meeding, kon de focus van de controle komen te liggen op het al dan niet vaststellen van de aanwezigheid van strafbaar materiaal. Het risico hierbij was dat de toezichts- en opsporingstaken door elkaar gingen lopen. De prioritering van de politie, het gebrek aan capaciteit en de onwenselijke vermenging tussen reclasseringstoezicht en opsporing heeft ertoe geleid dat politie medio juli 2023 weinig tot geen ruimte meer zag om te ondersteunen bij de controles.⁸²

Ervaren knelpunten bij de Reclassering

Uit gesprekken blijkt dat de Reclassering zich (evenals de politie) niet meer comfortabel voelde bij de wijze waarop de uitvoering van de controle was geregeld en hoe deze werd uitgevoerd. De Reclassering stelde zich op het standpunt dat de controle op gespannen voet kwam te staan met haar taak en met de kern van het werken in gedwongen kader. Het primaire doel van de Reclassering is immers gedragsbeïnvloeding en terugdringen van recidive. Dit doet de Reclassering door toezicht te houden op de gedragsvoorwaarden. De werkalliantie tussen de reclasseringsmedewerker en de betrokkene berust op onderling vertrouwen, binding, en het gezamenlijk werken aan doelen. De taak van de Reclassering is niet het opsporen van strafbaar materiaal, terwijl in de praktijk de focus van de controle daarop kwam te liggen. Dat kwam volgens de Reclassering omdat alleen diegenen werden gecontroleerd waarbij sterke vermoedens bestonden dat strafbaar materiaal zou worden aangetroffen en vanwege de aard van de controle (namelijk de controle of strafbaar materiaal op zijn digitale gegevensdrager stond). Deze voorwaarde stelde de politie om mee te werken aan de controles.

De eerdergenoemde noodgedwongen risicoselectie wrong, omdat vanuit Reclasserings- en toezichtperspectief geldt dat wanneer de bijzondere voorwaarde met controle wordt geadviseerd en opgelegd, deze uitgevoerd *moet* worden. Als dat niet gebeurt, ondermijnt dat de effectiviteit van het toezicht. De oude methode van de controle staat volgens Reclassering op gespannen voet met de waarden van de Reclassering, de werkalliantie en de plichten van reclasseringsmedewerkers (zoals het beroepsgeheim, het borgen van de vertrouwensrelatie) en de rechten van de betrokkenen.

Er ontstonden ook regionale verschillen. In een aantal politieregio's waar de bijzondere voorwaarde werd opgelegd, werd de controle voor zover mogelijk conform het vonnis uitgevoerd, terwijl in weer andere politieregio's de controles op den duur uitbleven. Zo waren er regio's waar de politie helemaal geen ondersteuning meer bood, in andere regio's gebeurde dit alleen bij concrete signalen die duiden op aanwezigheid van verboden materiaal en in weer andere regio's werd de Reclassering verzocht eerst zelf te controleren. Van een uniforme uitvoeringspraktijk was geen sprake meer.

Kortom, de politie werkte mee aan de controles vanwege een dubbele doelstelling om als technisch expert de toezichtstaak van de Reclassering te ondersteunen en om de maatschappij te beschermen door strafbaar materiaal op te sporen, terwijl de Reclassering de controle als instrument zag binnen het bredere palet aan maatregelen om het gedrag van de betrokkene te beïnvloeden en de recidive terug te dringen. Twee doelstellingen die zich niet goed met elkaar verhouden.

Ervaren knelpunten openbaar ministerie

Dat technisch specialisten van de politie de reclassering ondersteunden bij de controles en dat dit spanning opleverde, onderkent ook het openbaar ministerie. Ook zij geven aan dat het feit dat politieagenten die in hun dagelijkse werk bezig waren met opsporing van materiaal van seksuele uitbuiting van kinderen, ook in de sfeer van reclasseringstoezicht opereerden, leidde tot vervaging van de grens tussen opsporing en toezicht. Een ander knelpunt dat door het openbaar ministerie

⁸² Kamerstukken II 29270, nr. 156, p. 2.

wordt gesignaleerd is het vraagstuk van het op juridisch houdbare wijze formuleren van de vordering van de bijzondere voorwaarde. Bij deze afweging staat centraal de verhouding tussen enerzijds een effectieve en werkbare wijze van controle en anderzijds het in acht nemen van het recht op privacy van de betrokkene. Idealiter zouden datgene wat de reclassering adviseert, het openbaar ministerie vordert en de rechtbank oplegt eensluidend moeten zijn. Om de effectiviteit van de controle op het voorkomen van recidive goed te kunnen bepalen, zou het wenselijk zijn dat de reclassering bij alle opgelegde bijzondere voorwaarden de controle zou kunnen uitvoeren.

Ervaren knelpunten rechtspraak

Het Kenniscentrum cybercrime, dat onderdeel uitmaakt van de rechtspraak, signaleert ook de variëteit in formuleringwijzen van de bijzondere voorwaarde in vonnissen. Het kenniscentrum publiceert over dit thema en biedt handreikingen aan rechters en ondersteuners om tot meer werkbare en juridisch houdbare formuleringen van de bijzondere voorwaarde te komen, maar ziet dat deze maar weinig benut worden. Een andere verklaring die het kenniscentrum ziet voor de variëteit in formuleringen in vonnissen is dat doorgaans de meeste aandacht bij het schrijven van het vonnis gaat naar de bewezenverklaring en de persoonlijke omstandigheden en in mindere mate naar de formulering van de bijzondere voorwaarde.

5.12 Stopzetting controle

Medio 2023 is de controle van digitale gegevensdragers niet meer uitgevoerd. De Minister voor Rechtsbescherming heeft dit gemeld aan de Tweede Kamer en aangegeven dat er een doorontwikkeling van de controle zou plaatsvinden in de vorm van een tijdelijke voorziening.⁸³

5.13 Tijdelijke voorziening

Sinds de controles vanaf juli 2023 niet meer worden uitgevoerd, wordt gewerkt aan een oplossing om de controle van gegevensdragers door de Reclassering zelf binnen de toezichthoudende taak te laten uitvoeren. Het primaire doel dat de Reclassering met deze tijdelijke voorziening beoogt, is het signaleren van risicovol online gedrag van de betrokkene en het op basis daarvan kunnen inschatten of de bijzondere voorwaarden zijn overtreden. De Reclassering is medio september 2024 nog aan het definiëren wat online risicovol gedrag precies inhoudt.

Door het ontwerpen en uitvoeren van een tijdelijke werkwijze (tijdelijke voorziening) kan de Reclassering vanaf het derde kwartaal van 2024 op beperkte schaal een controle uitvoeren op risicovol online gedrag. De ervaringen hiermee kunnen worden benut voor het bijstellen van de werkwijze. De Reclassering streeft ernaar om in 2024 in ieder geval vijftig controles te kunnen uitvoeren.⁸⁴ Naast de tijdelijke voorziening loopt er een project 'toekomstbestendige controle', dat als doel heeft de technische en organisatorische randvoorwaarden van de controle te formuleren. Het is medio september 2024 voor de Reclassering nog niet duidelijk welke precieze organisatorische en technische randvoorwaarden de toekomstige werkwijze met zich zal brengen, omdat dit afhankelijk is van de uitvoering van de tijdelijke voorziening en van de vraag of de controle juridisch is toegestaan en technisch haalbaar en uitvoerbaar is binnen de wettelijke taak van de Reclassering.

⁸³ Kamerstukken II, 2023/2024, 29270, nr. 156.

⁸⁴ Beslisnota Directoraat-Generaal Straffen en Beschermen, Directie Sanctie- en Slachtofferbeleid van 9 februari 2024.

5.14 Conclusie

In 2012 is het INDIGO-project ontwikkeld. Dit was een lokaal initiatief dat later landelijk zou worden ingevoerd met als doel om snel een hulpverleningstraject op te kunnen zetten voor verdachten van een licht zedenvergriep. Met een INDIGO-afdoening stemde de verdachte in om mee te werken aan een controle van zijn digitale gegevensdragers op aan seksuele kinderoitbuiting gerelateerd strafbaar materiaal. Met een INDIGO-afdoening bleef strafrechtelijke vervolging achterwege; de politie bespaarde daarmee capaciteit en de overheid gaf het signaal af aan de maatschappij dat zogenoemde simpele downloadzaken werden opgepakt. Na een evaluatie van het project werd besloten om de controle ook in te gaan zetten bij andere titels.

Nadat de nodige ervaring was opgedaan met de INDIGO-afdoening ontstond bij zowel het openbaar ministerie als de Reclassering de wens om dit ook bij andere zaken te kunnen toepassen, als onderdeel van een interventie die gericht is op beïnvloeding van het gedrag van de betrokkene. Het was immers niet logisch dat de controle wel werd ingezet bij een voorwaardelijk sepot, maar niet bij andere afdoeningen waar het gaat om ernstiger feiten. Juist in die gevallen is het belangrijk om gegevensdragers van de veroordeelde te controleren. De controle van gegevensdragers had primair tot doel om recidive van de veroordeelde te voorkomen.

Er werden werkafspraken vastgelegd en de politie en Reclassering kwamen overeen dat de politie technische bijstand zou verlenen aan de Reclassering bij de controles van gegevensdragers. Deze ondersteuning zou maximaal vijftig keer per jaar worden verleend. Dat aantal leek toentertijd toereikend, maar vanaf medio 2012 nam het aantal bijzondere voorwaarden waarbij de controle van digitale gegevensdragers werd opgelegd, explosief toe. Dit leidde ertoe dat in een minderheid van de gevallen de controle ook daadwerkelijk werd uitgevoerd. De politie stelde de voorwaarde dat hij alleen nog wilde controleren als er signalen waren dat de veroordeelde opnieuw materiaal van seksuele uitbuiting van kinderen bekeek of in bezit was van dergelijk strafbaar materiaal.

Als tijdens de controle strafbaar materiaal werd aangetroffen vormde dit aanleiding om een nieuw opsporingsonderzoek te starten. Dit begon te knellen, voor zowel de Reclassering als de politie, omdat door de toegepaste risicoselectie, opsporing en Reclasseringstoezicht door elkaar gingen lopen. Een ander belangrijk knelpunt vormde de wijze waarop rechters de bijzondere voorwaarde in hun vonnissen formuleerde. Deze formuleringen sloten vaak niet aan bij de formuleringen die de Reclassering hanteerde in haar advies aan het openbaar ministerie. Dit kon in veel gevallen leiden tot praktische onuitvoerbaarheid van het vonnis. Dat dwong de Reclassering ertoe een balans te vinden tussen enerzijds een zinvolle controle en anderzijds recht doen aan hetgeen de rechter in zijn vonnis had bepaald.

In 2021 liet de Reclassering het Ministerie van JenV weten dat de controles voor uitvoeringsproblemen zorgden en dat er bepaalde juridische bezwaren kleefden aan de aanpak, gelet op de arresten van de Hoge Raad. Medio 2023 is de oude controle niet meer uitgevoerd en sindsdien wordt gewerkt aan een tijdelijke voorziening waarmee op kleine schaal door de Reclassering ervaring kan worden opgedaan. Doel is te komen tot een nieuwe wijze van controleren die recht doet aan de bedoeling van de bijzondere voorwaarde en die past binnen de doelstelling van het toezicht op de veroordeelde waarmee de Reclassering belast is.

6. Grondrechten

6.1 Inleiding

Als een veroordeelde moet meewerken aan een controle van zijn digitale gegevensdragers, heeft dit impact op zijn persoonlijke levenssfeer. Uit hoofdstuk 5 is gebleken dat de inhoud van zijn telefoon of computer wordt gescand. Door de belangrijke rol die deze apparaten en de online wereld spelen in het dagelijks leven, bevatten telefoons en computers in de meeste gevallen veel (gevoelige) persoonlijke informatie. Bijvoorbeeld over iemands voorkeuren, persoonlijke opvattingen en de communicatie met zijn sociale contacten. In dit hoofdstuk wordt onderzocht welke inbreuk de controle maakt op de persoonlijke levenssfeer, bedoeld in artikel 8 EVRM. Daarnaast kan de controle uitwijzen dat de veroordeelde opnieuw een strafbaar feit heeft begaan. Daarmee is het mogelijk dat het recht om niet mee te werken aan een nieuwe veroordeling een rol speelt bij de controle. Dit recht is neergelegd in artikel 6 EVRM en wordt aangeduid als het nemo tenetur-beginsel. In dit hoofdstuk wordt onderzocht of dit recht van toepassing is en zo ja, of de controle dit beginsel mogelijk schendt.

In dit hoofdstuk wordt het laatste deel van onderzoeksvraag 1 beantwoord, en wordt onderzoeksvraag 6 beantwoord. De beantwoording van onderzoeksvraag 6 is nodig om onderzoeksvraag 1 te beantwoorden wat betreft 8 EVRM.

1. Wat zijn, mede gelet op recente jurisprudentie, de juridische kaders waaraan controles van online gedrag betreffende seksueel kindermisbruik moeten voldoen?

6. Welke waarborgen worden getroffen om de inbreuk op de persoonlijke levenssfeer van de onder toezicht gestelde zoveel mogelijk te beperken?

Deze informatie zal vervolgens in hoofdstuk 8 als onderdeel van het juridisch kader worden gebruikt om de werkwijze te evalueren en advies te kunnen geven over de doorontwikkeling van de controle. Dit hoofdstuk is als volgt opgebouwd. Eerst behandelen we het nemo tenetur-beginsel en dan volgt een bespreking van het recht op de eerbiediging van de persoonlijke levenssfeer. Per grondrecht wordt toegelicht wat de betekenis ervan is en op welke wijze wordt getoetst of sprake is van een inbreuk en zo ja, of dit een gerechtvaardigde inbreuk is. Vervolgens wordt per grondrecht getoetst of dit van toepassing is op de controle, en zo ja, hoe het grondrecht zich verhoudt tot de oude werkwijze die werd gehanteerd voor de controle van gegevensdragers. Daarna staan we stil bij de bescherming van persoonsgegevens en gaan we in op de toepasselijkheid van de AVG, de Wpg en de Wjsg tijdens de uitvoering van de controle.

6.2 Artikel 6 EVRM: het nemo tenetur-beginsel

In deze paragraaf staat het toetsingskader centraal voor de beoordeling of het nemo tenetur-beginsel van toepassing is en of zich een eventuele schending daarvan voordoet. Dit beginsel kan een rol spelen wanneer de Reclassering tijdens de controle van gegevensdragers strafbaar materiaal aantreft en de politie aan de hand van die informatie tot een strafrechtelijk onderzoek overgaat. Om zo dicht mogelijk te blijven bij de uitleg die het Europese Hof voor de Rechten van de Mens (EHRM) geeft aan het nemo tenetur-beginsel en bij de invulling die het EHRM aan het toetsingskader geeft,

zijn de overwegingen van het EHRM in het Engels weergegeven en niet naar het Nederlands vertaald.

6.2.1 Definitie nemo tenetur-beginsel

Het nemo tenetur-beginsel⁸⁵ houdt in dat iemand niet hoeft mee te werken aan diens eigen veroordeling. Het beginsel ligt besloten in artikel 6 van het EVRM, de artikelen 47 en 48 van het Handvest van de grondrechten van de Europese Unie en artikel 29 Sv. Het beginsel is verder opgenomen in artikel 14, derde lid, onderdeel g, van het Internationaal Verdrag inzake burgerrechten en politieke rechten en artikel 7, tweede lid, van Richtlijn- (EU) 2016/343, inzake de versterking van het vermoeden van onschuld.⁸⁶

In het Nederlandse recht is geen onvoorwaardelijk recht of beginsel verankerd dat een verdachte op geen enkele wijze kan worden verplicht tot het verlenen van medewerking aan het verkrijgen van voor hem mogelijk bezwarend bewijsmateriaal. Wel brengt het aan artikel 29 Sv ten grondslag liggende beginsel mee dat een verdachte niet kan worden verplicht tot het afleggen van een verklaring omtrent zijn betrokkenheid bij een strafbaar feit, waarvan niet kan worden gezegd dat deze in vrijheid is afgelegd. Ook ligt in artikel 6 EVRM besloten dat, indien ten aanzien van een verdachte sprake is van een *criminal charge* in de zin van die bepaling, deze het recht heeft om te zwijgen en zichzelf niet te incrimineren.⁸⁷

6.2.2 Ratio nemo tenetur-beginsel

Volgens vaste rechtspraak van het EHRM ligt de ratio van het zwijgrecht en het nemo tenetur-beginsel onder meer in het tegengaan van ongeoorloofde dwang, en daarmee het tegengaan van rechterlijke dwalingen, en aan het realiseren van de doelen van artikel 6 van het EVRM. In verband met die grondgedachte strekt het nemo tenetur-beginsel tot het respecteren van de wil van de verdachte te zwijgen. Het EHRM verwoordt dit als volgt:

‘Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6 (art. 6) (...). The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused. In this sense the right is closely linked to the presumption of innocence contained in Article 6 para. 2 of the Convention’.⁸⁸

⁸⁵ Nemo tenetur se ipsum accusare.

⁸⁶ Richtlijn (EU) 2016/343 van het Europees Parlement en de Raad van 9 maart 2016 betreffende de versterking van bepaalde aspecten van het vermoeden van onschuld en van het recht om in strafprocedures bij de terechtzitting aanwezig te zijn (*PbEU* 2016, L65).

⁸⁷ Zie bijvoorbeeld HR 20 april 2021, ECLI:NL:HR:2021:515, r.o. 3.3 en HR 19 september 2006, ECLI:NL:HR:2006:AV1141, r.o. 6.5.1

⁸⁸ Zie bijvoorbeeld EHRM, 4 oktober 2022, nr. 58342/15 (*De Legé* tegen *Nederland*), par. 63, 67, EHRM, 13 september 2016, nrs. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim en anderen* tegen *het Verenigd Koninkrijk*), par. 266; EHRM, 17 december 1996, nr. 19187/91 (*Saunders* tegen *het Verenigd Koninkrijk*); EHRM 8 februari 1996, nr. 18731/91 (*Murray* tegen *het Verenigd Koninkrijk*), par. 45.) en EHRM, 25 februari 1993, nr. 10828/84 (*Funké* tegen *Frankrijk*).

Naast deze twee onderling verbonden ratio's die door het EHRM expliciet zijn erkend, wordt in de literatuur een derde, impliciete ratio onderkend, namelijk de procesautonomie.⁸⁹ De procesautonomie houdt in dat de verdachte volledig vrij is in het bepalen van de eigen procespositie.⁹⁰ Deze ratio raakt tevens aan de menselijke waardigheid en vloeit voort uit het respect dat voor de verdachte moet worden opgebracht. Daarnaast raakt dit aan de gedachte dat het wreed is of zelfs onmenselijk zou zijn verdachten te confronteren met het dilemma – ook wel *cruel dilemma* genoemd – om jezelf te beschuldigen door de waarheid te spreken of gestraft te worden vanwege niet-meewerken.^{91 92}

De toetsing aan het nemo tenetur-beginsel moet telkens in samenhang met de verschillende ratio's van dit beginsel worden gezien.

6.2.3 Toetsing aan het nemo tenetur-beginsel

In het arrest *De Legé tegen Nederland* zet het EHRM het toetsingskader uiteen om te bepalen of het nemo tenetur-beginsel geldt en te beoordelen of sprake is van een schending daarvan.⁹³

Allereerst moet zijn voldaan aan de twee hierna door het EHRM geformuleerde randvoorwaarden.⁹⁴

- 1) In order for an issue to arise from the perspective of the privilege against self-incrimination, there must be some form of coercion or compulsion exerted on the person concerned;
- 2) It is furthermore required that either that person is subject to existing or anticipated criminal proceedings – (...) a 'criminal charge' (...)—, or incriminating information compulsorily obtained outside the context of criminal proceedings is used in a subsequent criminal prosecution (...).

Als aan deze twee randvoorwaarden is voldaan, wordt beoordeeld of het gebruik van het aan de hand van een uitgeoefende vorm van dwang verkregen bewijsmateriaal niettemin moet worden beschouwd als vallend buiten de reikwijdte van de bescherming van het nemo tenetur-beginsel.

- 3) The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect

⁸⁹ Dissenting opinion Martens and Kuris bij EHRM 17 December 1996, nr. 19187/91 (*Saunders tegen het Verenigd Koninkrijk*), par. 9: 'respect for human dignity and autonomy requires that every suspect should be completely free to decide which attitude he will adopt with respect to the criminal charges against him. On this view it would be improper, because incompatible with such respect, to compel an accused to cooperate in whatever way in bringing about his own conviction.'

⁹⁰ Zie onder meer J.S. Nan, 'Een probleem rondom het nemo tenetur-beginsel?', *Bsb* 2021, afl. 4; D.A.G van Toor, , *Het schuldige geheugen?* (diss. Nijmegen), Deventer: Wolters Kluwer 2017, p. 391-409; S.Ligthart, *Coercive brain-reading in criminal justice: An analysis of European human rights law* Cambridge University Press: 2022. <https://doi.org/10.1017/9781009252447>, p. 156, 6; Concl. A-G F.W. Bleichrodt voor HR 13 oktober 2020, *NJ* 2021/120, m.nt. J.M. Reijntjes, onder 31.

⁹¹ Zie onder meer Van Toor 2017, p. 379, 382-384. Martens en Kuris zijn kritisch over een dergelijke cruel choice-rationale: 'Such "rationales" cannot justify the immunities under discussion since they obviously presuppose that the suspect is guilty, for an innocent suspect would not be subjected to such choices nor bring about his own ruin by answering questions truthfully! Innocent suspects are, therefore, not treated cruelly or unethically, whilst guilty suspects should not complain that society does not allow them to escape conviction by refusing to answer questions or otherwise hiding evidence.' (dissenting opinion rechters Martens en Kuris in *Saunders tegen het Verenigd Koninkrijk*, onder 9, voetnoot 11)

⁹² Een andere ratio die in de literatuur wordt genoemd is privacy van de verdachte als voorwaarde voor een eerlijke proces. Zie in dat kader D.A.G. van Toor, 'Het nemo-teneturbeginsel bij digitale opsporingsbevoegdheden: oproep tot discussie over fundamentele bezinning van de normering van het opsporingsonderzoek in een digitale context', *TBS&H* 2021, nr. 2, p. 89-100, en A. Pivaty, P. ter Vrugt & D. de Vocht, *EmpRISe Netherlands: Policy Report*, 2021 (www.empriseproject.org/policy-briefs/), p. 1, 3-4.

⁹³ De Hoge Raad lijkt dit toetsingskader eveneens te hanteren. Zie HR 19 november 2023, *AA* 2024/0155 mnt. J.S. Nan.

⁹⁴ EHRM, 4 oktober 2022, nr. 58342/15 (*De Legé tegen Nederland*), par. 65, 74.

such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing (par. 67).

- 4) Where the use of documentary evidence obtained under threat of penalties in the context of financial law matters is concerned, it may further be deduced from the Court's case-law, that such use does not fall within the scope of protection of the privilege against self-incrimination where the authorities are able to show that the compulsion is aimed at obtaining specific pre-existing documents — thus, documents that have not been created as a result of the very compulsion for the purpose of the criminal proceedings — which documents are relevant for the investigation in question and of whose existence those authorities are aware. That situation is to be distinguished from the situation where the authorities attempt to compel an individual to provide the evidence of offences he or she has allegedly committed by forcing him or her to supply documents which they believe must exist, although they are not certain of it. The latter situation the Court has described as 'fishing expeditions' (par. 76.)
- 5) Regardless of whether or not the authorities are aware of the existence of documentary or other material evidence, if it has been obtained by a measure which breaches Article 3,⁹⁵ the privilege against self-incrimination remains applicable (par. 77).

Wordt voldaan aan de voorwaarden voor de toepasselijkheid van het nemo tenetur-beginsel en valt het gebruik van door dwang verkregen bewijsmateriaal binnen de reikwijdte daarvan, dan moet worden onderzocht of in de procedure de *kern* van het beginsel voldoende is geëerbiedigd. Daarmee wordt gewogen op welke manier het beginsel invloed heeft gehad op de *algehele eerlijkheid* van de procedure. Het EHRM betreft daarbij in het bijzonder:

- 6) a. the nature and degree of the compulsion, b. the existence of any relevant safeguards in the procedure and, crucially, c. the use to which any material so obtained is put (par. 68).⁹⁶
- ⁹⁷

Stappen 1 en 2: dwang en criminal charge

Het nemo tenetur-beginsel komt aan de orde als er een vorm van dwang wordt uitgeoefend op de betrokkene én de betrokkene onderwerp is van een bestaande of verwachte strafvervolgning of als de door middel van dwang verkregen belastende informatie wordt gebruikt in een latere strafrechtelijke vervolging.

Het nemo tenetur-beginsel is dan ook alleen van toepassing in relatie tot een *criminal charge* als bedoeld in artikel 6 van het EVRM. Dat is volgens het EHRM het geval vanaf het moment dat:

⁹⁵ Artikel 3 van het EVRM bepaalt dat niemand mag worden onderworpen aan folteringen of aan onmenselijke of vernederende behandelingen of bestraffingen. Dit betreft een absoluut recht.

⁹⁶ In *Jalloh tegen Duitsland* noemde het EHRM nog een vierde factor, nl. 'the weight of the public interest in the investigation and punishment of the offence in issue. In navolgende zaken komt de factor *public interest* niet meer terug.

⁹⁷ Van Toor betoogt dat de focus op de aard en mate van dwang als centraal criterium bij de beoordeling van nemo-teneturklachten moet plaatsmaken voor een meer op de informatie gebaseerd toetsingskader. Niet het ingezette middel, de handeling van de autoriteiten – daar gaat het om bij het criterium de aard en mate van dwang –, maar het doel – de verzameling informatie – moet bepalend zijn. Dit vanwege de grote hoeveel data die met slechts een lichte vorm van dwang – het begrenzen van de beweeglijkheid van de pols en de hand en het vervolgens scannen van de vingerafdruk – kan worden vergaard. D.A.G. van Toor, 'Het nemo tenetur-beginsel bij digitale opsporingsbevoegdheden', *TBS&H* 2021, afl. 2

an individual is officially notified by the competent authority of an allegation that he has committed a criminal offence, or from the point at which his situation has been substantially affected by actions taken by the authorities as a result of a suspicion against him.⁹⁸

Hiervan is bijvoorbeeld sprake als iemand herhaaldelijk door de politie wordt ondervraagd over een bepaald misdrijf, de politie gebruikt maakt van de hem toekomende bevoegdheden om iemand door middel van dwang informatie te laten verstrekken over iemands betrokkenheid bij een misdaad dan wel wanneer een persoon wordt gearresteerd op verdenking van het plegen van een misdrijf.

Zodra een zaak onherroepelijk is geworden en tot de tenuitvoerlegging van de straf wordt overgegaan, is artikel 6 van het EVRM en het daaraan verbonden nemo tenetur-beginsel niet meer van toepassing, omdat van een *criminal charge* op dat moment geen sprake meer is. Wanneer bijvoorbeeld de Reclasering een controle van de voorwaarden van een voorwaardelijke straf uitvoert, is op die controle als zodanig het nemo tenetur-beginsel dan ook niet van toepassing. Echter, als deze controle ertoe leidt dat een verdenking ontstaat, op basis waarvan opsporingsbevoegdheden worden ingezet, is wel sprake van een *criminal charge* en speelt het beginsel wel een rol.⁹⁹

Stappen 3 + 5 Ongeoorloofde dwang (improper compulsion)

In de zaak *Saunders* tegen het *Verenigd Koninkrijk* heeft het EHRM een uitzondering geformuleerd op de toepasselijkheid van het nemo tenetur-beginsel:

The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. (...) it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing.¹⁰⁰

Waar het EHRM in deze zaak nog geen duidelijkheid over bood, is of het nemo tenetur-beginsel bescherming biedt tegen *ongeoorloofde* dwang om bewijs te verkrijgen en daarmee de verdachte beschermt tegen het gebruik van ongeoorloofde middelen (*means-based*; 'through the use of compulsory powers') of tegen het ongeoorloofd verkrijgen van bepaalde type bewijs (*material based*; 'material that has an existence independent of the will'). In de literatuur wordt uit latere jurisprudentie van het EHRM afgeleid dat het een *means based* nemo tenetur-beginsel hanteert.¹⁰¹ De aard van het materiaal speelt daarmee geen (doorslaggevende) betekenis. Het nemo tenetur-beginsel biedt de verdachte dus een uniek beschermingsbereik dat los staat van het zwijgrecht, waarbij de aard en mate van dwang ter verkrijging van het materiaal centraal staan.¹⁰²

⁹⁸ EHRM, 12 mei 2017, nr. 21980/04 (*Simeonovi* tegen *Bulgarije*), par. 110; EHRM, 13 september 2016, nrs. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim en anderen* tegen *het Verenigd Koninkrijk*), par. 249; EHRM, 10 september 2010, nr. 31333/06 (*McFarlane* tegen *Ierland*) par. 143, en EHRM; 27 februari 1980, nr. 6903/75 (*Deweert* tegen *België*) par. 44.

⁹⁹ Ligthart 2022, p. 175-176.

¹⁰⁰ EHRM, 17 december 1996, nr. 19187/91 (*Saunders* tegen *het Verenigd Koninkrijk*), par. 69.

¹⁰¹ EHRM, 4 oktober 2022, nr. 58342/15 (*De Legé* tegen *Nederland*); EHRM 5 april 2012, nr. 11663/04 (*Chambaz* tegen *Zwitserland*); EHRM 11 juli 2006, nr. 54810/00 (*Jalloh* tegen *Duitsland*); EHRM 3 mei 2001, nr. 31827/96 (*J.B.* tegen *Zwitserland*); EHRM 29 juni 2007, nr. 15809/02, nr. 25624/02 (*O'Halloran & Francis* tegen *het Verenigd Koninkrijk*). Zie onder meer ook Ligthart 2022; D.A.G. van Toor 'Het gedwongen ontgrendelen van een smartphone in het licht van het nemo tenetur-beginsel', *NJ* 2019/06, p. 406; Van Toor 2017, p. 398-403.

¹⁰² D.A.G. van Toor 'Het gedwongen ontgrendelen van een smartphone in het licht van het nemo tenetur-beginsel', *NJ* 2019/06, p. 406.

Waar de Hoge Raad voorheen uitging van een *material based* benadering,¹⁰³ lijkt deze, onder verwijzing naar de in de zaak *De Legé tegen Nederland* aangehaalde jurisprudentie van het EHRM, nu ook een *means based* benadering te hanteren.¹⁰⁴

Stappen 3 en 5: Wils(on)afhankelijk materiaal

Op basis van de hiervoor aangehaalde arresten van het EHRM levert het afdwingen en het gebruik van bewijs dat onafhankelijk van de wil *bestaat*¹⁰⁵ (*wilsonafhankelijk materiaal*) – zoals DNA, bloed, urine, bolletjes drugs, documenten – in beginsel geen strijdigheid op met het nemo tenetur-beginsel.

Het afdwingen van verklaringen binnen een strafrechtelijke procedure en het gebruik van buiten het strafproces afgedwongen verklaringen zijn in beginsel wel in strijd met nemo tenetur-beginsel. Het gaat daarbij immers over materiaal dat niet zonder volledige medewerking van de verdachte kan worden vergaard. Het materiaal is daarmee niet onafhankelijk van de wil van de verdachte *verkregen* (*wilsafhankelijk materiaal*).

Wanneer op het eerste gezicht wilsonafhankelijk materiaal toch afhankelijk van de wil van de verdachte wordt verkregen, is er alsnog sprake van wilsafhankelijk materiaal. Een dergelijke situatie doet zich bijvoorbeeld voor als de autoriteiten een (nog niet) verdachte met forse dwangsommen dwingen tot het verstrekken van bankafschriften op een wijze die van de verdachte een inspanning vraagt die neerkomt op het leveren van bewijs van vermeende overtredingen door hem of haar te dwingen documenten te verstrekken waarvan zij geloven dat deze moeten bestaan, hoewel ze daar niet zeker van zijn (dit staat bekend als een *fishing expedition*), of op het zodanig ordenen van informatie dat daar het belastende verhaal mee wordt weggegeven.¹⁰⁶ In zo'n geval komt het gedwongen verstrekken van de in beginsel wilsonafhankelijke informatie in wezen neer op het geven van een verklaring die wilsafhankelijk is.

Informatie die al is opgeslagen op een gegevensdrager en onafhankelijk van de wil van de verdachte bestaat, betreft wilsonafhankelijk materiaal wanneer deze informatie vrij toegankelijk is. In het geval deze informatie slechts toegankelijk is door middel van een vergrendelde smartphone of laptop kan het verkrijgen van *toegang* tot het materiaal afhankelijk worden van de wil van de verdachte.

Daarvan is *geen* sprake wanneer om een smartphone of laptop biometrisch te ontgrendelen de verdachte tegen zijn wil is geboeid en zijn duim op een vingerafdrukscanner is geplaatst. Op deze wijze is de vingerafdruk van verdachte gebruikt om gegevens die op dat moment al in smartphone of laptop waren vastgelegd als bewijs van het strafbare feit, waarvan hij werd verdacht, veilig te stellen.¹⁰⁷ Er wordt namelijk geen nieuw materiaal geproduceerd: de vingertop en de huid bestaan en kunnen, zonder schending van het nemo tenetur-beginsel, van de verdachte worden 'verkregen'. Dit is eventueel anders voor wachtwoorden: als het wachtwoord wordt verkregen doordat de verdachte wordt gedwongen het uit te spreken. De verdachte produceert dan immers materiaal dat afhankelijk is van de wil van de verdachte. Als de autoriteiten het wachtwoord op een andere manier verkrijgen, bijvoorbeeld door een vordering gegevens aan een telecommunicatiedienst of door een stuk papier waarop het wachtwoord is opgeschreven in beslag te nemen, is geen sprake

¹⁰³ Zie onder meer HR 24 april 2015, ECLI:NL:HR:2015:1130, r.o. 4.4.2; HR 12 juli 2013, ECLI:NL:HR:2013:BZ3640, r.o. 3.6; HR 21 december 2010, ECLI:NL:HR:2010:BL0666, r.o. 4.3.

¹⁰⁴ HR 14 november 2023, ECLI:NL:HR:2023:1562, r.o. 3.5.1 tot en met 3.5.3.

¹⁰⁵ Er is geen wilsbepaling of spierbeweging noodzakelijk om het materiaal te creëren.

¹⁰⁶ Onderdeel 38 van de conclusie van A-G mr. F.W. Bleichrodt voorafgaand aan HR 9 februari 2021, ECLI:NL:HR:2021:202.

¹⁰⁷ In lijn met HR 9 februari 2021, ECLI:NL:HR:2021:202, r.o. 7.3.

van materiaal dat afhankelijk is van de wil van de verdachte.¹⁰⁸

Tussenstap 4: strafzaken in de financiële context

Hoewel het arrest *De Legé tegen Nederland* aanwijzingen bevat dat de onder 4 geformuleerde regel ten aanzien van *documentary evidence* ook buiten de fiscale context kan gelden, dient daarbij paragraaf 62 van het arrest in aanmerking te worden genomen. Het EHRM overweegt daarin dat het algemene uitgangspunt kan worden gehanteerd dat:

cases concerning tax surcharges or tax fines differ from the hard core of criminal law for the purpose of the Convention, and that, consequently, the guarantees of Article 6 under its criminal head will not necessarily apply with their full stringency.

Dat zou erop duiden dat wanneer de waarborgen van artikel 6 in volle omvang gelden, aan het nemo tenetur-beginsel in de regel meer gevolgen zijn verbonden,¹⁰⁹ namelijk dat medewerking van de verdachte eigenlijk niet kan worden afgedwongen.¹¹⁰

Stap 6: de algehele eerlijkheid (fairness) van de procedure

Een inbreuk op nemo tenetur-beginsel leidt in beginsel tot het uitsluiten van onrechtmatig verkregen bewijsmateriaal en kan in uitzonderlijke gevallen zelfs de gehele strafvordering doen vervallen. Deze gevolgen zijn echter niet absoluut. Het EHRM bestraft schending van het nemo tenetur-beginsel alleen met uitsluiting als het gaat om een schending in de kern. Wanneer daar volgens het EHRM sprake van is, wordt hierna nader toegelicht.

a. de aard en mate van dwang (the nature and degree of the compulsion)

Welke dwang ongeoorloofd is, lijkt van het concrete geval af te hangen. Een vrijheidsbenemende straf is (vrijwel) altijd ontoelaatbaar, maar een bescheiden geldboete kan door het EHRM nog wel eens gebillijkt worden. Uiteindelijk gaat het erom dat het weigeren om mee te werken nog een reële optie voor de betrokkene moet zijn. Bij een aanzienlijke boete of vrijheidsbeneming zal dat in beginsel niet langer het geval zijn.¹¹¹

Het EHRM identificeert op basis van zijn jurisprudentie in ieder geval drie situaties, die aanleiding geven tot zorg voor een met artikel 6 van het EVRM ongeoorloofde dwang,¹¹² namelijk:

- 1) where a suspect is obliged to testify under threat of sanctions and either testifies in consequence or is sanctioned for refusing to testify;
- 2) where physical or psychological pressure, often in the form of treatment which breaches Article 3 of the Convention, is applied to obtain real evidence or statements;
- 3) where the authorities use subterfuge to elicit information that they were unable to obtain during questioning.

¹⁰⁸ D.A.G. van Toor, 'Het nemo tenetur-beginsel bij digitale opsporingsbevoegdheden', *TBS&H* 2021, afl. 2, p. 96-97.

¹⁰⁹ PHR 11 juli 2023, ECLI:NL:PHR:2023:676, nrs 33-37.

¹¹⁰ Onderdeel 4 van de annotatie van J.S. Nan bij HR 19 november 2023; AA 2024/0155

¹¹¹ J.S. Nan, 'Een probleem rondom het nemo tenetur-beginsel?', *BSb* 2021 nr. 4, p. 118.

¹¹² EHRM, 13 september 2016, nrs. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim en anderen tegen het Verenigd Koninkrijk*) par. 267.

b. het bestaan van enige relevante procedurele waarborgen (the existence of any relevant safeguards in the procedure)

Gedragingen die mogelijk geoorloofd zijn, kunnen door afwezigheid van relevante waarborgen toch als ongeoorloofd worden bestempeld. Het gaat dan om procedurele waarborgen die effectief en voldoende de mate van dwang reduceren.¹¹³ Zo kan in dat kader onder meer worden gewezen op procedurele waarborgen in het geval de verdachte de informatie niet heeft of zou kunnen hebben die de autoriteiten proberen te verkrijgen.¹¹⁴

c. de manier waarop enig aldus verkregen materiaal wordt gebruikt (the use to which any material so obtained is put)

Zoals reeds hiervoor is vastgesteld, valt de controle van gegevensdragers door de Reclassering (al dan niet met tussenkomst van de politie) ten behoeve van het toezicht op de naleving van de voorwaardelijke straf als zodanig niet onder de reikwijdte van het nemo tenetur-beginsel. Wel speelt dit beginsel een rol wanneer de controle ertoe leidt dat een verdenking ontstaat op basis waarvan opsporingsbevoegdheden worden ingezet. Het gaat dan met name over de manier waarop het tijdens de controle verkregen materiaal wordt gebruikt in de strafrechtelijke procedure.

Als de verkregen informatie niet wordt gebruikt in het kader van het vaststellen van een *criminal charge* wordt het nemo tenetur-beginsel niet geschonden.¹¹⁵ In de EHRM-zaak *Gäfgen* tegen *Duitsland* was sprake van een bekentenis die was afgedwongen in strijd met artikel 3 EVRM. Deze verklaring werd echter als bewijs uitgesloten in de strafzaak die in het geding was. Het Hof oordeelde: ‘no causal chain existed leading from the prohibited methods of investigation to the applicant’s conviction and sentence’.¹¹⁶ Dit is anders wanneer het bewijs zou zijn toegestaan in de procedure. Tegelijkertijd zal het uitsluiten of eenvoudig niet gebruiken van onder dwang verkregen bewijs niet altijd een schending van het nemo tenetur-beginsel kunnen voorkomen. Uiteindelijk zal dit afhangen van de algehele *fairness* van de procedure.¹¹⁷

Het Hof lijkt bij de beoordeling ook in aanmerking te nemen in welke mate de informatie een rol heeft gespeeld in de veroordeling van de verdachte. Wanneer de onder dwang verkregen verklaringen een grote rol spelen in de veroordeling, zal dit eerder leiden tot een schending van het nemo tenetur-beginsel, dan wanneer het bewijsmateriaal slechts een (mineur) element is in het vaststellen van de overtreding.¹¹⁸

Los van de hiervoor beschreven situaties rijst de vraag in hoeverre onder dwang verkregen informatie gedurende een controle kan worden gebruikt als startinformatie voor een strafrechtelijk onderzoek. De schaarse jurisprudentie lijkt te suggereren dat het nemo tenetur-beginsel de toelating van bewijs dat voortkomt uit onder dwang verkregen verklaringen niet per definitie uitsluit; onder dwang verkregen bekentenissen kunnen worden gebruikt tijdens het strafrechtelijk onderzoek, maar niet tijdens de terechtzitting.¹¹⁹ Hieruit lijkt te volgen dat tijdens de controle onder dwang verkregen informatie als startpunt kan worden gebruikt voor een strafrechtelijk onderzoek.

¹¹³ Van Toor 2017, p. 403.

¹¹⁴ Zie bijvoorbeeld EHRM, 29 juni 2007, nrs. 15809/02 and 25624/02 (*O’Halloran and Francis* tegen *het Verenigd Koninkrijk*), par. 59. Zie ook Lighthart 2022, p. 171-172.

¹¹⁵ Bijvoorbeeld EHRM, 16 juni 2015, nr. 784/14 (*Van Weerelt* tegen *Nederland*), par. 60–64; EHRM 8 April 2004, nr. 38544/97 (*Weh* tegen *Oostenrijk*), par 54.

¹¹⁶ EHRM, 1 juni 2010, nr. 22978/05 (*Gäfgen* tegen *Duitsland*), par. 186.

¹¹⁷ Lighthart 2022, p. 172.

¹¹⁸ EHRM, 17 december 1996, nr. 19187/91 (*Saunders* tegen *het Verenigd Koninkrijk*), par. 71; EHRM, 29 juni 2007, nrs. 15809/02 and 25624/02 (*O’Halloran and Francis* tegen *het Verenigd Koninkrijk*), par. 60.

¹¹⁹ EHRM, 1 juni 2010, nr. 22978/05 (*Gäfgen* tegen *Duitsland*), par. 186; EHRM, 17 december 1996, nr. 19187/91 (*Saunders* tegen *het Verenigd Koninkrijk*), par. 67. Zie uitgebreider Lighthart 2022, p. 173-174.

6.2.4 Nemo tenetur-beginsel en de controle van digitale gegevensdragers

In deze paragraaf wordt het beschreven toetsingskader voor het nemo tenetur-beginsel toegepast op de controle van digitale gegevensdragers.

Op grond van de door de rechter opgelegde bijzondere voorwaarde is de betrokkene verplicht om mee te werken aan de controle van digitale gegevensdragers door de Reclassering. Hiermee wordt een zekere vorm van dwang op de betrokkene uitgeoefend.

Zoals hiervoor is besproken, valt de controle van gegevensdragers *als zodanig* niet onder de reikwijdte van het nemo tenetur-beginsel. Er is immers in die situatie geen sprake van een *criminal charge*. Echter, wanneer tijdens de controle beeldmateriaal wordt aangetroffen dat leidt tot een verdenking dat een strafbaar feit is gepleegd op basis waarvan opsporingsbevoegdheden worden ingezet, speelt het beginsel wel een rol.

Ten behoeve van de controle van gegevensdragers gebruikt de Reclassering een softwareprogramma van de politie. De Reclassering werd – in de oude situatie – bij het uitvoeren van de controle van gegevensdragers ook bijgestaan door (digitaal) specialisten van de politie. Het gaat om een geautomatiseerd softwareprogramma in de vorm van een ‘hit/no-hit systeem’. Dit softwareprogramma bevat een mogelijkheid om afbeeldingen op gegevensdragers te vergelijken met een database van uit eerder politieonderzoek bekende versleutelde bestanden van seksuele uitbuiting. Het softwareprogramma slaat alleen afbeeldingen op die hits opleveren. Deze afbeeldingen worden in de applicatie getoond. De software toont *uitsluitend* informatie en gegevens die in het licht van de controle relevant zijn. Overige niet-relevante (persoonlijke) informatie wordt niet getoond. De software geeft daarnaast inzicht in de mappenstructuur, browsergeschiedenis (waaronder een zwarte lijst met websites), de aanwezigheid van versleutelingssoftware, de aanwezigheid van bepaalde applicaties, het gebruik van een VPN (waardoor het IP-adres verborgen blijft) en het gebruik van bijvoorbeeld een TOR-browser waarmee internetverkeer niet meer te traceren is (een onder meer door online zedendelinquenten veelgebruikte browser).

Tot medio 2023 maakte de Reclassering bij de controle van gegevensdragers gebruik van de beschreven software, die het ook mogelijk maakte om gevonden afbeeldingen te vergelijken met bekende versleutelde bestanden van seksuele uitbuiting. Het was dus mogelijk om met deze applicatie naast risicovol gedrag ook strafbare feiten te detecteren. De Werkafspraken bijzondere voorwaarden in zedenzaken, controle digitale gegevensdragers tussen politie, openbare ministerie en Reclassering Nederland uit 2017, geven aan dat de controle slechts een indicatief karakter had, waarbij de aanwezigheid van materiaal van seksuele uitbuiting van kinderen, gezien de hiervoor beschreven werking van de software, op basis van een eerste scan niet kon worden uitgesloten.¹²⁰

Wanneer tijdens de controle sprake was van een *hit* en daardoor een nieuwe verdenking ontstond, werd door de politie een nieuw opsporingsonderzoek gestart. Daarbij werden onderzoeksbevoegdheden ingezet,¹²¹ zodat sprake was van een *criminal charge*. In zoverre speelde het nemo tenetur-beginsel bij het doen van de controle een rol.

Nu aan beide voorwaarden wordt voldaan, moet worden beoordeeld of door de hiervoor beschreven dwang verkregen bewijsmateriaal redelijkerwijs buiten de reikwijdte van de

¹²⁰ Werkafspraken bijzondere voorwaarden in zedenzaken; controle digitale gegevensdragers tussen politie, openbaar ministerie en Reclassering Nederland, juni 2017, p. 5

¹²¹ Werkafspraken bijzondere voorwaarden in zedenzaken; controle digitale gegevensdragers tussen politie, openbaar ministerie en Reclassering Nederland, juni 2017, p. 6

bescherming van het nemo tenetur-beginsel valt. Dit beginsel biedt de verdachte bescherming tegen ongeoorloofde dwang(middelen) om bewijs te verkrijgen.

Materiaal van seksuele uitbuiting van kinderen dat reeds is opgeslagen op een gegevensdrager bestaat op die gegevensdrager onafhankelijk van de wil van de cliënt. De verplichting van de cliënt om mee te werken en het gebruik voor het bewijs van dit materiaal levert in beginsel geen strijd op met het nemo tenetur-beginsel. Wanneer echter de toegang tot deze informatie afhankelijk is van het verstrekken van een wachtwoord of pincode door de cliënt, wordt het verkrijgen van het materiaal afhankelijk van de wil van de cliënt. Die informatie kan slechts met een intellectuele inspanning van de verdachte worden verkregen.

Om dit type informatie te verkrijgen, is de wil van de cliënt een noodzakelijke schakel. Als de betrokkene weigert dergelijke informatie te verstrekken, ligt een schending van het nemo tenetur-beginsel op de loer in het geval door dwang of druk zijn wil om niet mee te werken wordt doorbroken. Het nemo tenetur-beginsel is ook van toepassing als de betrokkene niet bezwijkt onder de dwang of druk een wachtwoord of pincode te verschaffen, maar daarom wel wordt bestraft. Door te straffen wordt de wil van de betrokkene om de desbetreffende informatie niet te verschaffen immers niet gerespecteerd.

De Reclassering beschikt bij de uitvoering van uit de uitspraak voortvloeiende opdracht om controles uit te oefenen niet over bevoegdheden om een cliënt tot medewerking te dwingen. De Reclassering vraagt toestemming aan de cliënt om de woning te betreden en vraagt medewerking van de cliënt om het geautomatiseerd werk te ontgrendelen. De cliënt kan de medewerking aan de controle dan ook weigeren. Het gevolg daarvan is dat geen controle plaatsvindt.

Indien de cliënt medewerking verleent aan de controle en de Reclassering en de politie toegang verschaft tot zijn geautomatiseerde werk, bijvoorbeeld door het geven van zijn wachtwoord of pincode, kan de feitelijke controle van de gegevensdrager met gebruikmaking van het geautomatiseerd softwareprogramma plaatsvinden.

Centraal staat de vraag of de consequentie van het niet verlenen van medewerking door de cliënt leidt tot dwang of druk, waarmee de wil om niet mee te werken – in casu het geven van een wachtwoord of pincode – niet wordt gerespecteerd.

Het niet verschaffen van toegang tot een geautomatiseerd werk, kan leiden tot het schenden van de bijzondere voorwaarde. In dat geval meldt de Reclassering de overtreding van de bijzondere voorwaarden aan de officier van justitie.¹²² Een reële kans bestaat voor de cliënt dat de opgelegde straf alsnog ten uitvoer wordt gelegd. Het alsnog ten uitvoer leggen van de straf betreft geen sanctie gericht op het breken van de wil van de betrokkene. Immers, het betreft een reeds door de rechter aan de cliënt opgelegde voorwaardelijk straf die vanwege de schending van de bijzondere voorwaarde alsnog geheel of gedeeltelijk onvoorwaardelijk wordt.

Als de cliënt een drang voelt om een wachtwoord of pincode aan de Reclassering te verschaffen, dan komt die drang voort uit het niet willen schenden van de bijzondere voorwaarde. Die omstandigheid kan de cliënt ertoe brengen de voor de controle benodigde informatie te verschaffen. Dit betreft echter in het licht van *Ibrahim en anderen tegen het Verenigd Koninkrijk* geen ongeoorloofde dwang, omdat deze dwang uitgaat van de door de rechter opgelegde bijzondere voorwaarden en de daaruit voortvloeiende opdracht om controles uit te voeren. Mede gezien de destijds in de praktijk gehanteerde werkafspraken is ook in zoverre geen sprake van een schending van het nemo tenetur-beginsel.

¹²² Werkafspraken bijzondere voorwaarden in zedenzaken; controle digitale gegevensdragers tussen politie, openbaar ministerie en Reclassering Nederland, juni 2017, p. 6.

Van een schending van het nemo tenetur-beginsel is dan ook geen sprake.¹²³ Sinds medio mei 2023 heeft de Reclassering ervoor gekozen om te stoppen met de tot dan toe gehanteerde werkwijze bij de controle van gegevensdragers. Hoe de controle is aangepast en welke gevolgen dat heeft voor de rol van het nemo tenetur-beginsel bij de controle wordt nader toegelicht in paragraaf 8.3.

6.3 Artikel 8 EVRM

Artikel 8 EVRM ziet op de bescherming van de persoonlijke levenssfeer. Dit omvat het recht op de eerbiediging van het privéleven, het familie- en gezinsleven, de woning en correspondentie. Het begrip privéleven moet ruim worden opgevat. Het betreft onder andere de fysiologische en psychologische integriteit van een individu. Artikel 8 EVRM omvat ook het recht op bescherming van persoonsgegevens.¹²⁴

6.3.1 Verhouding EVRM, EU-Handvest en de Grondwet

Uit de preambule van het EU Handvest volgt dat dit Handvest de rechten bevestigt die (onder meer) voortvloeien uit het EVRM en de rechtspraak van het EHRM. Artikel 7 EU-Handvest (recht op eerbiediging van het privéleven en van het familie- en gezinsleven) correspondeert met de rechten die artikel 8 EVRM waarborgt en heeft ook dezelfde reikwijdte en inhoud als dat artikel. In artikel 8 EU-Handvest staat specifiek het recht op bescherming van persoonsgegevens, ook dat artikel is gebaseerd op artikel 8 EVRM.¹²⁵

De Algemene verordening gegevensbescherming (AVG) van de EU (en de nationale Uitvoeringswet AVG (UAVG)) en de EU-Richtlijn gegevensbescherming politie en justitie¹²⁶ (in Nederland geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg), zie paragraaf 6.4) vormen – wat betreft de bescherming van persoonsgegevens – een nadere en gedetailleerde invulling van artikel 8 van het EU-Handvest en in algemene zin van de fundamentele rechten zoals neergelegd in artikel 8 van het EVRM en artikel 7 van het EU-Handvest. Die samenhang blijkt ook uit de AVG en de Richtlijn gegevensbescherming politie en justitie zelf, waarin is bepaald dat deze de grondrechten en fundamentele vrijheden van burgers en met name hun recht op bescherming van persoonsgegevens beschermen.¹²⁷

Als gevolg van de komst van deze Europese wetgeving is sprake van een verschuiving in de bevoegdheidsverdeling tussen de lidstaten en de Europese Unie; de bescherming van het grondrecht *op bescherming van persoonsgegevens* wordt hoofdzakelijk geregeld en bepaald op EU-niveau. De bewegingsruimte van de lidstaten wordt hierdoor beperkt. Deze beperking heeft ook constitutionele implicaties. De door artikel 10 Grondwet voorziene rol van de nationale wetgever bij het stellen van regels over (beperking van) de eerbiediging persoonlijke levenssfeer is minder groot geworden. De reikwijdte van het recht op de eerbiediging van de persoonlijke levenssfeer wordt

¹²³ Zie onder meer ook de uitspraak van de rechtbank Noord-Nederland van 27 oktober 2022, ECLI:NL:RBNHO:2022:9501 die in r.o. 3.3.1, zij het zeer summier onderbouwd, tot eenzelfde conclusie kwam.

¹²⁴ Dit blijkt uit het arrest van het EHRM van 27 juni 2017, nr. 931/12 (*Satakunnan Markkinapörssi Oy en Satamedia Oy tegen Finland*), par. 137.

¹²⁵ Toelichtingen bij het Handvest van de grondrechten (2007/C 303/02), Toelichting ad artikel 7, artikel 8 en artikel 52.

¹²⁶ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (*PbEU* 2016, L119).

¹²⁷ Artikel 1, tweede lid, AVG en artikel 1, tweede lid, onderdeel a, Richtlijn gegevensbescherming politie en justitie.

bovendien in grote mate bepaald door artikel 8 EVRM en de jurisprudentie van het EHRM.¹²⁸ Toch is artikel 10 van de Grondwet niet zonder betekenis.

Artikel 8, tweede lid, EVRM bepaalt namelijk dat een inmenging ‘bij wet’ moet zijn voorzien. Dit vereiste is door het EHRM zodanig uitgelegd dat een inmenging een basis moet hebben in wetgeving, niet per se een wet in formele zin. Elk algemeen verbindend voorschrift of onder omstandigheden zelfs rechtersrecht kan een voldoende rechtsbasis zijn voor een inmenging. Artikel 10, eerste lid, van de Grondwet bepaalt echter dat het moet gaan om ‘bij of krachtens de wet te stellen beperkingen’ en vereist een wet in formele zin.¹²⁹ De Grondwet is dus strenger op dat punt. De Afdeling advisering van de Raad van State merkt hierover op dat de wetgever die bevoegdheid wel kan delegeren naar lagere regelgeving, maar dat dit geen *carte blanche* mag zijn. De beperkingen van het grondrecht moeten op het niveau van de formele wet worden gespecificeerd en er dient, in elk geval op hoofdlijnen, een belangenafweging plaats te vinden in het licht van artikel 10 van de Grondwet. De Grondwet geeft daarmee aan de wetgever een belangrijke verantwoordelijkheid: deze moet beoordelen of de beperking van fundamentele rechten van burgers blijft binnen de grenzen die de Grondwet stelt en voldoet aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Aan deze verantwoordelijkheid wordt volgens de Afdeling advisering van de Raad van State geen recht gedaan als de concrete invulling vrijwel geheel wordt overgelaten aan de algemene maatregel van bestuur (AMvB). De hoofdelementen die in algemene zin in ieder geval in de formele wet moeten worden neergelegd zijn de reikwijdte en de structurele elementen van een regeling. Een nadere uitwerking van de beperking kan plaatsvinden bij AMvB, indien een wet in formele zin hiervoor de delegatiegrondslag biedt. Een ministeriële regeling leent zich enkel voor technische voorschriften of voorschriften die met spoed gewijzigd moeten kunnen worden.¹³⁰

6.3.2 Toetsing aan artikel 8 EVRM

In deze paragraaf wordt de controle van gegevensdragers getoetst aan de eisen van artikel 8 EVRM.

Inmenging privéleven?

De controle vindt plaats aan voor de controleurs zichtbare gegevensdragers van de cliënt. Met de voor de controle gebruikte software worden grote hoeveelheden persoonlijke informatie ‘gescand’, om vervolgens volgens het principe ‘hit/no-hit’ relevante resultaten weer te geven. Dit principe wordt niet toegepast voor afbeeldingen die mogelijk seksuele uitbuiting van kinderen bevatten. Deze zijn wel zichtbaar voor de controleur. Hoewel de controleur dus geen inzage heeft in alle op de gegevensdragers aanwezige informatie, wordt deze informatie bij het gebruik van de software wel verwerkt. Bovendien worden de uitkomsten van de controle opgeslagen en kunnen de uitkomsten iets zeggen over het seksueel en mogelijk strafbaar gedrag van de veroordeelde. Dit heeft in potentie ingrijpende gevolgen voor de veroordeelde. Het voorgaande in ogeschouw genomen, kan worden geconcludeerd dat de controle van gegevensdragers een zware inmenging vormt in het privéleven van de cliënt.

¹²⁸ *Kamerstukken II* 2017/18, 34851, nr. 4, Advies Afdeling Advisering Raad van State, p. 6; Tekst & Commentaar privacy- en gegevensbeschermingsrecht, artikel 10 Grondwet, aant. 1.

¹²⁹ H.R. Kranenburg & L.F.M. Verhey, *De Algemene verordening gegevensbescherming in Europees en Nederlands perspectief*, Tweede druk, Deventer: Wolters Kluwer 2024, p. 43. Zie ook: HR 24 februari 2017 ECLI:NL:HR:2017:288, r.o. 2.3.2, (vgl. HR 19 december 1995, *NJ* 1996/249, r.o. 6.4.2); HR 10 april 2020, ECLI:NL:HR:2020:639, r.o. 2.5.2.

¹³⁰ *Kamerstukken II* 2019/20, 35447, nr. 4, Advies Afdeling advisering Raad van State en nader rapport Wet gegevensverwerking door samenwerkingsverbanden, p. 26 ; *Kamerstukken II* 2023/24, 36455 (R2188), nr. 4, Advies Afdeling advisering Raad van State bij Goedkeuring wijziging van verdrag over bescherming persoonsgegevens, p. 5.

Vervolgens moet worden getoetst of deze inmenging gerechtvaardigd is. Deze toets wordt hieronder uitgewerkt. Daarbij wordt uitgegaan van het toetsingskader dat artikel 8, tweede lid, EVRM biedt. Volgens dit artikel dient de inmenging:

1. te zijn voorzien bij wet,
2. noodzakelijk zijn in een democratische samenleving.

Voor zover de AVG (niet van toepassing op het binnentreden van de woning, wel van toepassing op de daadwerkelijke controle van de gegevensdragers)¹³¹ en artikel 10 Grondwet meer specifieke of aanvullende eisen stellen aan deze inmenging, wordt dat hierna expliciet aangegeven.

Bij wet voorzien?

Ingevolge artikel 8 EVRM moet de wettelijke regeling zodanig helder zijn omschreven dat burgers kunnen voorzien onder welke omstandigheden en voorwaarden de autoriteiten een inbreuk kunnen maken op het recht. De discretionaire ruimte die bevoegde autoriteiten hebben en de wijze waarop van deze ruimte gebruik mag worden gemaakt, moeten voldoende duidelijk in de wet zijn omschreven. De eisen die het EHRM stelt aan de grondslag hangen samen met de zwaarte van de inbreuk. In de regel geldt: hoe zwaarder de inbreuk is, hoe preciezer de wettelijke grondslag moet zijn en hoe gedetailleerder moet zijn voorzien in waarborgen (daarbij moet het geheel van in de wet aanwezige garanties in aanmerking worden genomen).¹³² Ingevolge artikel 10 Grondwet vereist een inbreuk op de eerbiediging van de persoonlijke levenssfeer een wet in formele zin waarin de beperking op dit grondrecht voldoende wordt gespecificeerd. Bij de controle van gegevensdragers is ook een verwerking van persoonsgegevens aan de orde, waarop de AVG van toepassing is.

Hiervoor is al geconstateerd dat de controle van digitale gegevensdragers een zware inmenging in het privéleven betreft. Daarvoor is onder meer volgens de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 3 april 2024 een vrij precieze wettelijke grondslag met de vereiste waarborgen nodig.¹³³ De hiervoor genoemde huidige wettelijke grondslagen (artikel 14c, tweede lid, aanhef en onderdeel 14° Sr – soms in samenhang gezien met artikel 14c, zesde lid, Sr (voor de aanwijzing van het toezicht)) – bieden een vrij algemene grondslag. Deze sluit onvoldoende aan bij de eisen die artikel 8 EVRM hieraan stelt, bij de daarmee corresponderende rechten ex artikel 7 en 8 EU Handvest in samenhang gezien met artikel 10, eerste lid, Grondwet, en bij de vereisten ex artikel 5, eerste lid, onderdeel b, AVG. Het verdient dan ook de voorkeur om de controle van gegevensdragers bij wet in formele zin van een specifieke rechtsgrondslag te voorzien.

Noodzakelijk in een democratische samenleving?

De inmenging moet noodzakelijk zijn in een democratische samenleving voor één van de in artikel 8, tweede lid, EVRM opgesomde doelen. Deze doelen betreffen de nationale veiligheid, de openbare

¹³¹ De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2, eerste lid, AVG).

¹³² Kranenborg & Verhey 2024, p. 44-45.

¹³³ Vgl. de beoordeling van de ABRvS in haar uitspraak van 3 april 2024, ECLI:NL:RVS:2024:1387, r.o. 8-9, over de rechtmatigheid van het onderzoeken van een telefoon op de mogelijke aanwezigheid van een identiteitsbewijs van een vreemdeling. Met name overweging 9.3 is relevant: "De staatssecretaris heeft bevestigd dat er geen nader regelgevend kader is aan de hand waarvan ambtenaren hun beslissing om een mobiele telefoon te onderzoeken nemen. De Afdeling leidt hieruit af dat artikel 59, achtste lid, van de Vw 2000, bij de beslissing om een telefoon al dan niet te onderzoeken, onvoldoende bescherming biedt tegen willekeurig optreden. Deze bepaling noch enige andere materieelwettelijke regeling schrijft voor in welke omstandigheden en onder welke voorwaarden een mobiele telefoon mag worden onderzocht, zodat die beslissing volledig wordt overgelaten aan de beoordeling van individuele ambtenaren van de AVIM en de KMar. Als grondslag voor het zonder toestemming onderzoeken van mobiele telefoons is de toepassing van deze bepaling daarom onvoldoende voorspelbaar. Deze bepaling voldoet dus niet aan de vereisten van duidelijkheid en nauwkeurigheid die de AVG en de rechtspraak van het EHRM stellen aan een grondslag voor de vergaande gegevensverwerking die die praktijk meebrengt." In deze zaak ging het om het "doorzoeken" van de telefoon, dus een gerichte "quickcheck". Die verwerking van (persoons)gegevens is vergelijkbaar met de in par. 5.8 van dit rapport beschreven controle aan gegevensdragers.

veiligheid, het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid en goede zeden of de bescherming van rechten en vrijheden van anderen. Daarbij moet sprake zijn van een dringende maatschappelijke behoefte (*pressing social need*), moet de maatregel proportioneel zijn om het beoogde doel te bereiken en moeten de rechtvaardigingsgronden aangedragen door de nationale autoriteiten relevant en voldoende zijn.¹³⁴

Uitgangspunt is dat de beperking in beginsel niet rechtmatig is als het daarmee beoogde doel ook kan worden bereikt op een wijze die het grondrecht niet of in minder mate beperkt. Laatstgenoemd criterium, ook wel aangeduid als het subsidiariteitsbeginsel, kan worden geacht deel uit te maken van de proportionaliteitstoets. Uit de jurisprudentie van het EHRM blijkt dat veel elementen in de proportionaliteitstoets relevant kunnen zijn. Zo spelen de aard van de gegevens en de reikwijdte van de aangevochten maatregel een rol. Verder kijkt het EHRM, zoals geschreven, naar de waarborgen waarmee de maatregel was omkleed, zoals de aanwezigheid van effectief onafhankelijk toezicht.¹³⁵

Omdat de controle van gegevensdragers ertoe dient om recidive tegen te gaan en daardoor strafbare feiten – met name (gerelateerd aan) online seksueel misbruik/uitbuiting – te voorkomen (een van de in artikel 8, tweede lid, EVRM genoemde doelen), mag worden aangenomen dat de controle van gegevensdragers een legitiem doel dient en voorziet in een dringende maatschappelijke behoefte. Wat betreft de proportionaliteit en subsidiariteit van de controle van digitale gegevensdragers bij veroordeelden voor het bezitten of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen, zijn de volgende punten van belang:

- De aard van de gegevens bij een *hit* kan zeer gevoelig zijn. Eventueel gevonden afbeeldingen van seksuele kinderausluiting maken een zeer grote inbreuk op de persoonlijke levenssfeer van de desbetreffende kinderen en de afbeeldingen geven het seksuele gedrag of seksuele gerichtheid van de veroordeelde zelf prijs. Het gaat dus om een bijzondere categorie van persoonsgegevens die extra bescherming behoeft. Als geen afbeeldingen worden gevonden, maar er wel andere *hits* zijn, dan geldt dat deze indirect kunnen wijzen op risicovol gedrag van de veroordeelde persoon, waarmee eventueel de bijzondere voorwaarde wordt overtreden. Volgens het EHRM heeft de gevoeligheid van de gegevens niet noodzakelijkerwijs betrekking op de inhoud daarvan.¹³⁶ In hoeverre gegevens gevoelig van aard zijn, is bovendien contextafhankelijk. Een gegeven op zichzelf hoeft niet gevoelig te zijn, maar kan dat worden door de wijze waarop en de context waarin het gegeven wordt gebruikt. Een voorbeeld daarvan is de EHRM-zaak *Benedik tegen Slovenië*,¹³⁷ waarin het ging om inzage door de politie in het IP-adres (geen op zichzelf gevoelig gegeven) om te achterhalen of dat mogelijk gebruikt was om materiaal van seksuele uitbuiting van kinderen

¹³⁴ EHRM 22 oktober 1981, nr. 7525/76 (*Dudgeon tegen Verenigd Koninkrijk*), par. 51. Zie ook: EHRM 22 juni 2023, 10794/12 (*Giuliano Germano tegen Italië*), par. 96 en EHRM 20 juni 2023, 36705/16 (*Margari tegen Griekenland*), par. 53.

De grondbeginselen van deze toets vinden hun oorsprong in oudere rechtspraak. Zie EHRM 7 december 1976, nr. 5493/72 r.o. 48 (*Handyside tegen Verenigd Koninkrijk*) NJ 1978/236 en EHRM 26 april 1979, A-30 (*Sunday Times tegen Verenigd Koninkrijk*), par. 59, NJ 1980/146 Deze zijn daarna leidraad gebleven en toegepast in vele arresten.

¹³⁵ Kranenborg & Verhey, 2024, p. 48-54.

¹³⁶ Kranenborg & Verhey, 2024, p. 49 Daarbij wordt verwezen naar EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. tegen Verenigd Koninkrijk*), par. 342, 363-364 en 416 e.v., JBP 2021/63, m.nt. E. Moyakine. In dit arrest gaf het EHRM aan dat ook verkeersgegevens veel persoonlijke informatie kunnen bevatten en, mede gelet op de moderne technologieën die daarop kunnen worden toegepast, een intiem beeld kunnen geven van een bepaald persoon. Daarbij gaat het om het blootleggen van sociale netwerken, communicatiepatronen,

fysieke plaatsbepalingen en zoekgedrag op het internet. In verband daarmee dienen verkeersgegevens gelijkwaardige (niet noodzakelijkerwijs identieke) bescherming te krijgen als de inhoud van de betreffende communicatie. Deze redenering kan min of meer gelijkmatig worden toegepast op het 'hit-no-hit'-systeem dat voor de controle van gegevensdragers wordt gebruikt, hoewel daarbij moet worden opgemerkt dat het in de Big Brother-zaak ging om bulkinterceptie en de inbreuk dus veel grootschaliger was.

¹³⁷ EHRM 24 april 2018, nr. 62357/14 (*Benedik tegen Slovenië*) par. 109, NJB 2018/1427.

te delen. Dit betrof volgens het EHRM gevoelige informatie. Eenzelfde redenering kan worden aangehouden ten aanzien van de software die wordt gebruikt bij de controles en werkt volgens het principe 'hit/no hit'. Bovendien: ook als geen *hits* uit de controle naar voren komen, dan geldt dat de digitale gegevensdrager van de veroordeelde wel volledig is gescand op informatie die tot een *hit* zou kunnen leiden. Dit kan betekenen dat bij het uitvoeren van de scan alsnog gevoelige of bijzondere categorieën van persoonsgegevens worden verwerkt, zonder dat dit een zichtbaar resultaat voor de controleur oplevert.

- Het EHRM toetst soms strenger aan de proportionaliteitseis, omdat moderne technologische middelen het gemakkelijker maken om dieper in te grijpen in de persoonlijke levenssfeer van burgers. Naarmate de verwerking zich meer toespitst op individuele personen, zijn sterkere waarborgen noodzakelijk.¹³⁸ Met de gebruikte software wordt tijdens de controle een grote hoeveelheid gegevens van een individu verwerkt. De reikwijdte van de inbreuk op de persoonlijke levenssfeer is dus groot. Wel moet daarbij worden opgemerkt dat als waarborg geldt dat alleen de *hits* en afbeeldingen die mogelijk seksuele uitbuiting van kinderen bevatten uit de controle naar voren komen, alleen potentieel relevante informatie zal zichtbaar worden voor de controleur. Ook wordt geen excessieve hoeveelheid gegevens opgeslagen, omdat alleen aangetroffen afbeeldingen worden bewaard. De aanwezigheid van effectief onafhankelijk toezicht lijkt voor het EHRM vooral een belangrijke rol te spelen in zaken waarin sprake is van heimelijke maatregelen die het privéleven binnendringen.¹³⁹ Daarvan is geen sprake bij de controle van gegevensdragers van veroordeelden voor het bezitten, vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen. Voor zover dit toezichtcriterium wel een rol zou spelen, kan worden geconstateerd dat een onafhankelijke rechter de bijzondere voorwaarde oplegt op basis waarvan de controle van digitale gegevensdragers plaatsvindt, zij het dat de kaders waarbinnen die controle moet plaatsvinden niet altijd even uitvoerig in rechterlijke uitspraken worden gegeven.
- Voor wat betreft de subsidiariteit van de controle van gegevensdragers wordt – in bredere zin – opgemerkt dat het gedragsvoorschrift (dat de reden vormt voor de uitvoering van de controle) slechts één van de instrumenten is die kunnen bijdragen aan het beoogde doel van – samengevat – het tegengaan van recidive. In dat licht bezien is de controle van gegevensdragers minder ingrijpend voor het privéleven van de veroordeelde dan bijvoorbeeld verblijf in de gevangenis of opname in een tbs-kliniek. In de engere zin kan worden bekeken hoe de controle van de gegevensdragers is vormgegeven. Momenteel wordt gebruik gemaakt van software die weliswaar veel gegevens verwerkt (*scant*), maar waarmee gericht wordt gezocht op potentieel risicovol materiaal (afbeeldingen) of indirecte aanwijzingen die kunnen duiden op risicovol gedrag (de andere *hits*). De controleur krijgt daarmee niet meer inzage dan noodzakelijk is voor het effectief uitoefenen van de controle.

6.3.3 Reflectie

De controle van digitale gegevensdragers dient ertoe om de kans op recidive van online seksueel misbruik/uitbuiting te verkleinen en daarmee strafbare feiten te voorkomen. De uitvoering van de controle dient dan ook een groot maatschappelijk belang. Hoewel de huidige software met het 'hit/no hit'-systeem een filter bevat waardoor de inbreuk wordt geminimaliseerd, kan worden gesteld dat de controle alsnog een ingrijpende maatregel is voor het privéleven van de voor de

¹³⁸ Kranenborg & Verhey, 2024, p. 51.

¹³⁹ Kranenborg & Verhey, 2024, p. 53-54.

veroordeelde persoon. Immers ook als geen ‘hits’ uit de controle naar voren komen, dan geldt dat de digitale gegevensdrager van de veroordeelde wel volledig is gescand op informatie die tot een ‘hit’ zou kunnen leiden. Dit kan betekenen dat bij het uitvoeren van de scan alsnog gevoelige of bijzondere categorieën van persoonsgegevens worden verwerkt, zonder dat dit een zichtbaar resultaat voor de controleur oplevert. Gelet op het voorgaande lijkt meer specifieke wetgeving – inclusief waarborgen – aangewezen voor de bijzondere voorwaarde van controle van digitale gegevensdragers.

Dit sluit aan bij de eerder aangehaalde adviezen van de Afdeling advisering van de Raad van State en de uitspraak van 3 april 2024 van de Afdeling bestuursrechtspraak van de Raad van State en is ook in lijn met de benadering van de Hoge Raad (zie par. 3.3, HR 29 november 2022, ECLI: NL:HR: 2022: 1763). De Hoge Raad heeft weliswaar bepaald dat het ontbreken van een specifieke wettelijke regeling voor toezicht op de naleving van bepaalde gedragsvoorwaarden er niet aan in de weg hoeft te staan dat de rechter invulling geeft aan de wijze waarop het toezicht kan plaatsvinden, maar wijst er wel op dat bij het geven van een toezichtopdracht door de rechter moet zijn gewaarborgd dat het toezicht niet leidt tot een meer dan beperkte inbreuk op de persoonlijke levenssfeer van de veroordeelde.

Deze conclusie is tevens in lijn met het advies van Procureur-Generaal Bleichrodt aan de Hoge Raad uit 2022. Bleichrodt besteedde hierin ook aandacht aan de rol van de wetgever bij normering van de reikwijdte van het reclasseringstoezicht, in het bijzonder ten aanzien van digitale gegevensdragers (zie ook paragraaf 3.3).¹⁴⁰ Hij schreef: “Gelet op de inbreuk op de persoonlijke levenssfeer die het onderzoek van gegevensdragers kan meebrengen, verdient het de voorkeur dat de wetgever bij de normering het voortouw neemt.”

Wel merken we op dat de wetgever bij normering van het toezicht ruimte zou moeten laten aan de rechter om een afweging te maken of een bijzondere voorwaarde moet worden opgelegd en wat deze in een bepaalde casus concreet zou moeten inhouden. Voor de Reclassering is het op haar beurt belangrijk dat de wetgeving en de rechter ruimte laten om het reclasseringstoezicht af te stemmen op het individuele geval, gelet op de waarden van de benodigde zorg, de veiligheid en de autonomie van de cliënt (zie paragraaf 5.2).

6.4 Toepasselijkheid AVG en Wjsg

De Reclassering verwerkt persoonsgegevens bij de controle van de digitale gegevensdragers. Het is daarbij de vraag of de AVG of de Wjsg van toepassing is.

De Wjsg ziet op de zorgvuldige omgang met de persoonsgegevens die door de rechterlijke macht en het openbaar ministerie worden verwerkt ten behoeve van strafrechtelijke procedures. De Wjsg onderscheidt verschillende typen gegevens.

In de eerste plaats gaat het om justitiële gegevens (persoonsgegevens over de toepassing van het strafrecht of strafvordering op een bepaald persoon) en om strafvorderlijke gegevens. Dat zijn de persoonsgegevens die in het kader van een strafvorderlijk onderzoek (strafdossier) worden verwerkt. Daarnaast gaat het om tenuitvoerleggingsgegevens, de persoonsgegevens die worden verwerkt ten behoeve van de tenuitvoerlegging van een opgelegde straf. Persoonsdossiers bevatten een verzameling van de uitgebrachte rapporten over het gedrag en de levensomstandigheden van een persoon in verband met een aanhangige strafzaak of de tenuitvoerlegging van een straf. Ten

¹⁴⁰ Par. 4.4 gaat over een conclusie van Procureur-Generaal Bleichrodt: PHR 22 februari 2022, ECLI:PHR:2022:170.

slotte worden gerechtelijke strafgegevens onderscheiden: dat zijn gegevens die zijn verkregen in het kader van de behandeling en beslissing in Nederlandse strafzaken.

Alle verschillende typen gegevens hebben onder de Wjsg hun eigen regime; die regimes worden in het Besluit justitiële en strafvorderlijke gegevens nader uitgewerkt. Onder andere wordt voorgeschreven wie de verwerkingsverantwoordelijke is, met welke actoren de gegevens gedeeld mogen worden, hoe lang de gegevens bewaard mogen worden en welke maatregelen moeten worden genomen om de gegevens te beschermen. Het regime van de Wjsg bepaalt voor welke doeleinden het verwerken van de verschillende typen gegevens noodzakelijk is.

De vraag is of de uitvoering van het toezicht op de bijzondere voorwaarde door de Reclassering (in samenwerking met de politie) valt onder het toepassingsbereik van de Wjsg. Uit de memorie van toelichting bij de Wjsg blijkt dat resocialisatie door instanties als de Reclassering¹⁴¹ niet onder het toepassingsbereik van de Wjsg valt, maar onder de AVG.¹⁴² Hierbij worden de voorbeelden van controle op de naleving van de voorwaarden bij vrijlating en taakstraffen gegeven. Het toezicht op de bijzondere voorwaarde bij een voorwaardelijke veroordeling kan ook worden gezien als resocialisatie door de Reclassering. Dit leidt tot de conclusie dat persoonsgegevens die de Reclassering in dit kader verwerkt, onder de bescherming van de AVG valt en niet onder de Wjsg.

De AVG bevat beginselen die bij de verwerking van persoonsgegevens in acht moeten worden genomen. Samengevat gaat het om: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, vertrouwelijkheid en integriteit van de verwerking. In het bijzonder moet rekening worden gehouden met het verwerkingsverbod van artikel 9 AVG, dat geldt voor de verwerking van bijzondere categorieën van persoonsgegevens (zoals gezondheidsgegevens of gegevens over seksuele aard of politieke voorkeur). De verwerking daarvan is enkel toegestaan als een van de uitzonderingen op het verwerkingsverbod (opgenomen in artikel 9, tweede lid, AVG) van toepassing is.

Zodra de Reclassering overgaat tot het verstrekken van persoonsgegevens aan een autoriteit die onder de werkingssfeer van de Wjsg valt – zoals het openbaar ministerie of de rechterlijke macht – in het kader van een doel dat verband houdt met de Wjsg, zal die wet van toepassing worden. Een voorbeeld is dat de Reclassering persoonsgegevens over het niet naleven van de bijzondere voorwaarde deelt met het openbaar ministerie, zodat het openbaar ministerie kan beoordelen of het voorwaardelijke deel van de straf ten uitvoer moet worden gelegd. In dit geval transformeren de persoonsgegevens tot tenuitvoerleggingsgegevens.

6.4.1 Toepasselijkheid AVG en Wet politiegegevens bij inzet van de politie

Vóór juli 2023 werd de politie door de Reclassering ingezet ten behoeve van de controle van gegevensdragers. Bij het uitlezen van de gegevensdragers worden persoonsgegevens verwerkt. De vraag die zich in die situatie voordeed was welk regime geldt voor de verwerking van de gegevens voor deze controle door de politie. Valt deze verwerking onder het toepassingsbereik van de AVG of de Wpg?

De Wpg is van toepassing indien de persoonsgegevens worden verwerkt in verband met de politietaak, bedoeld in artikel 3 en 4 van de Politiewet 2012. In het kader van dit onderzoek is artikel 3 van de Politiewet 2012 relevant. Volgens dit artikel heeft de politie de taak "(...) te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze

¹⁴¹ Alle persoonsgegevens die worden verwerkt door een autoriteit die niet onder de werkingssfeer valt van Richtlijn (EU) 2016/680, zoals de Reclassering, vallen onder de AVG.

¹⁴² *Kamerstukken II*, 2017/2018, 34889, nr. 3, p. 9-10, 13.

behoeven.” Wat betreft de strafrechtelijke handhaving valt hieronder ook de uitvoering van beslissingen van de rechter of het openbaar ministerie in strafzaken.¹⁴³

Het toezicht op de naleving van de bijzondere voorwaarde strekt niet tot strafrechtelijke handhaving of de tenuitvoerlegging van een straf, maar als doel heeft recidive te voorkomen. De politie bood de Reclassering destijds ondersteuning bij de uitvoering van diens taken. Gelet op deze omstandigheden lijkt het destijds door de politie ten behoeve van de Reclassering uitgevoerde toezicht niet onder de strafrechtelijke handhavingstaak en daarmee de politietaak te vallen. Hierdoor was niet de Wpg, maar de AVG van toepassing op de verwerking van persoonsgegevens door de politie in het kader van controle van gegevensdragers. Dit betekent bijvoorbeeld dat het verwerkingsverbod op bijzondere categorieën van persoonsgegevens op artikel 9 AVG op deze situatie van toepassing was.

Zodra de politie, na constatering van een strafbaar feit overging tot opsporing, werd de Wpg van toepassing op de persoonsgegevens die op dat moment werden verwerkt. De opsporing van strafbare feiten valt namelijk wel onder de politietaak, genoemd in artikel 3 van de Politiewet.

6.5 Conclusie

In dit hoofdstuk is onder meer aan de hand van jurisprudentie- en literatuuronderzoek getoetst hoe artikel 6 EVRM en het daarin besloten liggende *nemo tenetur*-beginsel, en de in artikel 8 EVRM opgenomen bescherming van de persoonlijke levenssfeer, als onderdelen van het van toepassing zijnde juridisch kader zich verhouden tot de tot medio 2023 uitgevoerde controle van gegevensdragers door de Reclassering, met bijstand van de politie.

Artikel 6 EVRM: nemo tenetur-beginsel

Wanneer de Reclassering een controle van digitale gegevensdragers uitvoert, valt die controle als zodanig niet onder de reikwijdte van het *nemo tenetur*-beginsel. Dit is echter anders in het geval de controle ertoe leidt dat een verdenking ontstaat op basis waarvan opsporingsbevoegdheden worden ingezet. Dan is namelijk sprake van een *criminal charge* als bedoeld in artikel 6 EVRM.

Bij het uitvoeren van de controle werd destijds een softwareprogramma van de politie ingezet. De (digitaal) specialisten van de politie verleenden de Reclassering technische bijstand en voerden de controles uit door het toepassen van deze software. Deze software bood de mogelijkheid om naast risicovol gedrag ook strafbare feiten te detecteren. Wanneer tijdens de controle sprake was van een *hit* en een nieuwe verdenking ontstond, werd door de politie een nieuw opsporingsonderzoek gestart, waarbij onderzoeksbevoegdheden werden ingezet, zodat sprake was van een *criminal charge*.

Het *nemo tenetur*-beginsel speelde daarmee bij het uitvoeren van de controle een rol van betekenis. Dit bracht met zich dat het in het arrest *De Legé tegen Nederland* door het EHRM uiteengezette toetsingskader in acht genomen moest worden. Op basis hiervan concluderen wij dat de aard en mate van de tijdens de controle uitgeoefende dwang ter verkrijging van het materiaal niet leidt tot een schending van het *nemo tenetur*-beginsel. Wij hebben daarbij het volgende in aanmerking genomen.

Materiaal van seksuele uitbuiting van kinderen dat al is opgeslagen op een gegevensdrager bestaat op die gegevensdrager onafhankelijk van de wil van de cliënt. De verplichting van de cliënt om mee te werken en het gebruik voor het bewijs van dit materiaal levert in beginsel geen strijd op met het

¹⁴³ Kamerstukken II 1985/1986, 19535, nr. 3, p. 6

nemo tenetur-beginsel. Dit is anders wanneer de toegang tot deze informatie afhankelijk is van het verstrekken van een wachtwoord of pincode door de cliënt. Die informatie kan slechts met een intellectuele inspanning van de verdachte worden verkregen. In dat geval wordt het verkrijgen van het materiaal afhankelijk van de wil van de cliënt; zijn wil is een noodzakelijke schakel.

De Reclassering beschikt bij de uitvoering van uit de uitspraak voortvloeiende opdracht om controles uit te oefenen niet over bevoegdheden om een cliënt tot medewerking te dwingen. De Reclassering hanteerde op grond van de Werkafspraken bijzondere voorwaarden in zedenzaken; controle digitale gegevensdragers tussen politie, openbaar ministerie en Reclassering Nederland, juni 2017, de werkwijze dat toestemming werd gevraagd aan de cliënt om de woning te betreden en dat medewerking van de cliënt werd gevraagd om het geautomatiseerd werk te ontgrendelen. De cliënt kon ook geen toestemming verlenen en de medewerking aan de controle weigeren. Het gevolg daarvan was dat geen controle plaatsvond.

Het niet verschaffen van toegang tot een geautomatiseerd werk kan leiden tot het schenden van de bijzondere voorwaarde. De consequentie daarvan kan mogelijk zijn dat de officier van justitie vordert dat de straf geheel of gedeeltelijk alsnog ten uitvoer wordt gelegd vanwege niet naleven van de bijzondere voorwaarde. Het alsnog ten uitvoer leggen van de straf betreft geen sanctie gericht op het breken van de wil van de betrokkene. Immers, het betreft een reeds door de rechter aan de cliënt opgelegde voorwaardelijke straf die vanwege de schending van de bijzondere voorwaarde alsnog geheel of gedeeltelijk onvoorwaardelijk wordt.

Als de cliënt een drang voelt om een wachtwoord of pincode aan de Reclassering te verschaffen, dan komt die drang voort uit het niet willen schenden van de bijzondere voorwaarde. Die omstandigheid kan de cliënt ertoe brengen de voor de controle benodigde informatie te verschaffen. Dit betreft echter in het licht van *Ibrahim en anderen tegen het Verenigd Koninkrijk* geen ongeoorloofde dwang, omdat deze dwang uitgaat van de door de rechter opgelegde bijzondere voorwaarde en de daaruit voortvloeiende opdracht om controles uit te voeren. Mede gezien de destijds gehanteerde werkafspraken is ook in dit geval geen sprake van een schending van het nemo tenetur-beginsel.

Artikel 8 EVRM: bescherming persoonlijke levenssfeer

Het recht op eerbiediging van het privéleven is nauw gerelateerd aan de bescherming van persoonsgegevens. Een verwerking van persoonsgegevens valt binnen de reikwijdte van artikel 8 EVRM wanneer deze een inmenging in het privéleven oplevert.

De controle vindt plaats aan voor de controleurs zichtbare gegevensdragers van de cliënt. Met de voor de controle gebruikte software worden grote hoeveelheden persoonlijke informatie ‘gescand’, om vervolgens volgens het principe ‘hit-or-no-hit’ relevante resultaten weer te geven. Dit principe wordt niet toegepast voor afbeeldingen die mogelijk seksuele uitbuiting van kinderen bevatten. Deze zijn wel zichtbaar voor de controleur. Hoewel de controleur dus geen inzage heeft in alle op de gegevensdragers aanwezige informatie zelf, wordt deze informatie wel bij het gebruik van de software verwerkt. Bovendien worden de uitkomsten van de controle opgeslagen en kunnen de uitkomsten iets zeggen over het seksueel en mogelijk strafbaar gedrag van de veroordeelde. Dit heeft in potentie ingrijpende gevolgen voor de veroordeelde. Dit maakt dat de controle van gegevensdragers een zware inmenging vormt in het privéleven van de cliënt.

Vervolgens is aan de hand van de criteria uit artikel 8, tweede lid, EVRM beoordeeld of deze inmenging gerechtvaardigd is. Daarvan is sprake wanneer:

1. de inmenging bij wet is voorzien; en
2. in een democratische samenleving noodzakelijk is om een van de in het tweede lid opgesomde legitieme doelen te bereiken.

Bij de beoordeling of de *inmenging bij wet is voorzien*, wordt getoetst of de wettelijke regeling zodanig helder is omschreven dat burgers kunnen voorzien onder welke omstandigheden en voorwaarden de autoriteiten een inbreuk kunnen maken op het recht. De discretionaire ruimte die bevoegde autoriteiten hebben en de wijze waarop van deze ruimte gebruik mag worden gemaakt, moeten voldoende duidelijk in de wet zijn omschreven. Voorts vereist artikel 10, eerste lid, Grondwet dat de beperkingen op het grondrecht op het niveau van een wet in formele zin worden gespecificeerd. De Grondwet geeft daarmee aan de wetgever een belangrijke verantwoordelijkheid: deze moet beoordelen of de beperking van fundamentele rechten van burgers blijft binnen de grenzen die de Grondwet stelt en daarbij voldoet aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.

De huidige wettelijke grondslagen (artikel 14c, tweede lid, aanhef en onderdeel 14°, Sr – soms in samenhang gezien met artikel 14c, zesde lid, Sr (voor de aanwijzing van het toezicht) – bieden een vrij algemene grondslag voor het controleren van digitale gegevensdragers. Ze sluiten daarmee niet aan bij eisen waaraan wetgeving in dit kader dient te voldoen. In lijn met de adviezen van de Afdeling advisering van de Raad van State, de aangehaalde jurisprudentie van de Hoge Raad en het advies van Procureur-Generaal Bleichrodt aan de Hoge Raad uit 2022, en de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 3 april 2024 verdient het, gelet op de inbreuk op de persoonlijke levenssfeer die de controle van gegevensdragers kan meebrengen, de voorkeur om deze controle bij wet in formele zin van een specifieke rechtsgrondslag te voorzien.

Omdat de controle van gegevensdragers ertoe dient om recidive tegen te gaan en met name aan online seksueel misbruik/uitbuiting gerelateerde strafbare feiten te voorkomen (een van de in artikel 8, lid, EVRM genoemde doeleinden), mag worden aangenomen dat de controle van gegevensdragers *een legitiem doel* dient en voorziet in een *dringende maatschappelijke behoefte*. Wij achten de beperking van de persoonlijke levenssfeer van de cliënt *noodzakelijk*, waarbij we het volgende in aanmerking hebben genomen. De controle is slechts één van de instrumenten die kunnen bijdragen aan het beoogde doel van – samengevat – het tegengaan van recidive. In dat licht bezien is de controle van gegevensdragers als zodanig minder ingrijpend voor het privéleven van de veroordeelde dan bijvoorbeeld het verblijf in een gevangenis of de opname in een tbs-kliniek.

Bij het uitvoeren van de controle van gegevensdragers kan de aard van de gegevens bij een *hit* zeer gevoelig zijn. Eventueel gevonden afbeeldingen van seksuele uitbuiting van kinderen maken een zeer grote inbreuk op de persoonlijke levenssfeer van de desbetreffende kinderen en de afbeeldingen geven het seksuele gedrag of seksuele gerichtheid van de cliënt zelf prijs. Het gaat dus om een bijzondere categorie van persoonsgegevens die extra bescherming behoeft. Als geen afbeeldingen worden gevonden, maar er wel andere *hits* zijn, dan geldt dat deze indirect kunnen wijzen op risicovol gedrag van de veroordeelde persoon waarmee eventueel de bijzondere voorwaarde wordt overtreden. Ook als het resultaat is dat er geen *hits* zijn, worden bij het uitvoeren van de scan alsnog gevoelige of bijzondere categorieën van persoonsgegevens verwerkt, zonder dat dit een zichtbaar resultaat voor de controleur oplevert. De reikwijdte van de inbreuk op de persoonlijke levenssfeer is dus groot. Daar staat tegenover dat als waarborg geldt dat alleen de *hits* en afbeeldingen die mogelijk seksuele uitbuiting van kinderen bevatten uit de controle naar voren komen, dus alleen potentieel relevante informatie zal zichtbaar worden voor de controleur. Ook wordt geen excessieve hoeveelheid gegevens opgeslagen, nu alleen aangetroffen afbeeldingen worden bewaard. Deze waarborgen zorgen daarmee voor een balans tussen de beperking van het grondrecht op eerbiediging van persoonlijke levenssfeer, waaronder de bescherming van persoonsgegevens, en het beoogde doel.

7. Verkenning uitbreiding controle naar andere delicten

7.1 Inleiding

De online wereld speelt een steeds belangrijkere rol in het leven van mensen, zo ook in de criminaliteit. Zo zijn er nieuwe delicten ontstaan die voor de uitvinding van de computer niet bestonden. Denk aan het *hacken* van een computer. Daarnaast zijn er tal delicten die voor het bestaan van het internet en de computer al wel bestonden, maar zich door digitalisering hebben aangepast of zich nu deels online afspelen. Het verplaatsen van delicten naar de online wereld stelt de organisaties binnen de strafrechtketen voor een grote uitdaging, onder meer omdat zij hier nog niet altijd op zijn ingericht. Het wel of niet (kunnen) verkrijgen van inzicht in wat zich afspeelt in de online wereld is hierbij een belangrijk aspect. Dat inzicht is van grote meerwaarde om criminaliteit effectief tegen te gaan. Een voorbeeld daarvan is de *hack* van de cryptocommunicatiedienst EncroChat, een berichtendienst waar veel criminele organisaties gebruik van maken. Wereldwijd volgden op basis van inzicht in de berichten van deze dienst duizenden arrestaties.¹⁴⁴ De gehackte berichten speelden in Nederland een belangrijke rol bij de bewijsvoering in een aantal grote strafzaken, zoals het Marengoproces.¹⁴⁵

Los van de meerwaarde van inzicht in online gedrag voor de opsporing van delicten en de bewijsvoering in strafzaken, wordt ook verder in de strafrechtketen het nut van inzicht in online gedrag onderkend. Dat hebben we gezien in dit onderzoek, waarbij voor de Reclassering inzicht in (resultaten van) toezicht nuttig is in het kader van de gedragsverandering van veroordeelden. De controle van digitale gegevensdragers heeft in dat licht ook potentie voor het toezicht op naleving van de bijzondere voorwaarden bij veroordeelden van andere (online) delicten, zeker omdat steeds meer risicovol gedrag dat de Reclassering dient te controleren zich online afspeelt.

Om die reden is een verkenning uitgevoerd naar de vraag in hoeverre de controle van digitale gegevensdragers zich, in aangepaste vorm, leent voor andere typen delicten die zich ten dele of geheel online afspelen zoals online terrorisme, extremisme, radicalisering, cybercrime en andere online seksuele delicten. Het is de vraag of de controle ook haalbaar is voor deze andere typen delicten, gelet op de verschillende relevante gezichtspunten, zoals wat juridisch is toegestaan, de techniek, de aard van de dader, en de uitvoerbaarheid van de controle. Per delict gaan we in op de aard daarvan en op twee dadereigenschappen die van belang zijn voor de controle, namelijk de digitale expertise van de dadergroep en de bereidwilligheid om mee te werken. Daarna maken we een eerste inschatting of de huidige software, die wordt ingezet bij de controle van digitale gegevensdragers op materiaal van seksuele uitbuiting van kinderen zich kan lenen voor cliënten die zijn veroordeeld van de bovengenoemde type delicten of dat daarvoor andere software nodig is. Ten slotte benoemen we algemene randvoorwaarden die bij een uitbreiding in acht moeten worden genomen ten behoeve van de uitvoerbaarheid. De geschetste beelden betreffen een eerste verkenning, waarbij we hebben geput uit interviews met experts en ketenpartners uit de praktijk. Voor sluitende antwoorden zal nader verdiepend onderzoek per type delict en per type dader moeten worden verricht.

In dit hoofdstuk wordt de relevante informatie voor de beantwoording van onderzoeksvraag 11 verzameld. In hoofdstuk 8 volgt de definitieve beantwoording van onderzoeksvraag 11. In dit hoofdstuk wordt ook onderzoeksvraag 12 beantwoord.

¹⁴⁴ <https://nos.nl/artikel/2480473-ruim-6500-verdachten-opgepakt-na-hack-berichtendienst-encrochat>

¹⁴⁵ <https://nos.nl/op3/artikel/2347879-de-grootste-politievangst-ooit-martelkamers-drugs-en-spoorloze-criminelen>

11. Kan de nieuw voorgestelde controle-methodiek in aangepaste vorm worden toegepast bij andere soorten online delicten, zoals andere seksuele delicten, cybercrime en delicten op het terrein van terrorisme, extremisme en radicalisering?

12. In hoeverre zijn er verschillen tussen deze soorten delicten waarmee rekening moet worden gehouden?

7.2 Online terrorisme, extremisme en radicalisering

7.2.1 Aard van de delicten

Extremisme en radicalisering zijn pas strafbaar zodra deze overtuigingen of ideeën leiden tot het plegen van een of meer (terroristische) misdrijven

Het hebben van een extremistische overtuiging of het ontwikkelen van radicale ideeën is niet strafbaar. Dit verandert wanneer die overtuiging of ideeën worden omgezet in daden en leiden tot een misdrijf. Het kan in die gevallen gaan om misdrijven die met een terroristisch oogmerk worden gepleegd (zoals het plegen van een aanslag of het deelnemen aan een terroristische organisatie) of misdrijven ter voorbereiding of vergemakkelijking van een terroristisch misdrijf (zoals opruiing).¹⁴⁶ Een terroristisch oogmerk geldt daarnaast voor bepaalde delicten als strafverzwarende omstandigheid.¹⁴⁷ De woorden extremisme en radicalisering komen als zodanig niet voor in het Wetboek van Strafrecht.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid definieert terrorisme als “het uit ideologisch motieven dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij ontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politiek besluitvorming te beïnvloeden”. Extremisme wordt gedefinieerd als: “het fenomeen dat personen of groepen vanuit ideologische motief bereid zijn in ernstige mate de wet te overtreden of activiteiten te verrichten die de democratische rechtsorde ondermijnen”.¹⁴⁸ Volgens de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) kan extremisme in zijn uiterste vorm leiden tot terrorisme. Radicalisering lijkt weer een voorfase te zijn van extremisme.¹⁴⁹

Hoewel het in eerste instantie verdedigbaar lijkt dat een strafrechtelijke veroordeling voor terroristische misdrijven niet direct resulteert in een (deels) voorwaardelijke straf met bijzondere voorwaarden, blijkt uit de jurisprudentie dat dit wel voorkomt. Bijvoorbeeld bij een veroordeling wegens het voorbereiden van een terroristische aanslag of het aansluiten bij een terroristische organisatie. De bijzondere voorwaarde wordt dan bijvoorbeeld in combinatie met een gevangenisstraf of een taakstraf opgelegd waarbij gedragsvoorwaarden worden opgelegd zoals ‘de veroordeelde vermijdt in aanraking te komen met extremistisch materiaal’ of ‘veroordeelde onthoudt zich van het bezoeken van een digitale omgeving waarin materiaal met extremistische inhoud kan worden verkregen’.¹⁵⁰

¹⁴⁶ Deze delicten zijn genoemd in artikel 83 en 83b Sr. In artikel 83a Sr wordt de definitie van een terroristisch oogmerk gegeven.

¹⁴⁷ J. de Hullu, *Materieel strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht*, Wolters Kluwer 2021, p. 81.

¹⁴⁸ M. Ezinga & M. Boelens, *Onderzoek naar terrorisme, extremisme en contraterrorisme*, WODC 2019.

¹⁴⁹ <https://www.aivd.nl/onderwerpen/terrorisme>; <https://www.aivd.nl/onderwerpen/extremisme>

¹⁵⁰ Zie bijvoorbeeld Rechtbank Rotterdam 22 februari 2024 ECLI:NL:RBROT:2024:1290 en ECLI:NL:RBROT:2024:1291 en 2 december 2021 ECLI:NL:RBROT:2021:11857.

Het duiden en afbakenen van online risicovol gedrag bij online terrorisme kan een uitdaging zijn, maar is in ontwikkeling

Bij terroristische misdrijven gaat het om delicten die voor het computertijdperk al bestonden, maar zich door digitalisering ten dele hebben verplaatst naar de online wereld. Ook de daders hebben zich daarop aangepast. De computer kan worden gezien als een hulpmiddel, bijvoorbeeld voor het verspreiden van bepaald gedachtegoed en het aanzetten van anderen tot of het voorbereiden van een terroristische aanslag.

Bij het duiden van online risicovolle gedragingen die grenzen aan terrorisme is de nodige zorgvuldigheid geboden. Bij deze gedragingen is sprake van een glijdende schaal tussen niet-strafbaar, risicovol en mogelijk strafbaar gedrag, wat voor de nodige afgrenzingsproblemen kan zorgen en het moeilijk kan maken om vast te stellen wanneer iemand precies de grens over gaat. Gesprekspartners dachten verschillend over de vraag in hoeverre dit type gedrag voldoende precies is af te bakenen. De gesprekspartners van de rechtspraak voorzagen op dit punt de nodige uitdagingen, omdat bij het formuleren van het verboden gedrag een conflict van grondrechten, zoals de vrijheid van godsdienst en de vrijheid van meningsuiting, kan optreden.

De Reclassering heeft de laatste jaren met dit type zaken ervaring opgedaan in een daarvoor opgezet landelijk team en heeft op basis daarvan de formulering van het gedrag waar de betrokkene zich van moet onthouden ontwikkeld. Dit maakt dat de Reclassering mogelijkheden ziet om controleerbare gedragsvoorwaarden op te leggen. Daarnaast kunnen contactverboden worden opgelegd, die ook goed controleerbaar zijn. Kennis van het type online gedrag is hierbij belangrijk, zeker omdat het gedrag meerdere online verschijningsvormen kent. Voorbeelden zijn het plaatsen/verspreiden van opruiend beeldmateriaal of teksten op/via sociale media, in meer beslotenheid delen van bepaald gedachtegoed in Telegram groepen, of het consumeren (en eventueel reposten) van bepaald gedachtegoed. Daarmee verschilt het online gedrag per verdachte/dader. Een voordeel dat werd benoemd bij het controleren of de bijzondere voorwaarden worden nageleefd bij online-terroristisch gedrag is dat de risicovolle gedragingen die wijzen op een overtreding van de bijzondere voorwaarden in verhouding tot gedragingen die zien op het bezitten of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen, verder af liggen van het strafbare feit, waardoor minder snel spanning tussen toezicht en opsporing ontstaat. Bij materiaal van seksuele uitbuiting van kinderen is het vinden van dit materiaal op zichzelf een voldoende aanwijzing dat er een strafbaar feit is gepleegd en geeft ook het bezoeken van een website waar het materiaal te vinden is een aanwijzing dat er een strafbaar feit is gepleegd. Dat is bij deze delicten niet het geval, omdat het bezoeken of bekijken van materiaal nog geen nieuw strafbaar feit oplevert.

7.2.2 Dadereigenschappen

Daders van online terrorisme lijken goed in staat te zijn te misleiden, wat controle van deze groep bemoeilijkt

Volgens gesprekspartners is kenmerkend voor deze dadergroep dat er sprake is van een netwerkdelict, waarbij het collectief lerend vermogen hoog is. Dit maakt het aannemelijk dat – in verhouding met daders van een delict als bedoeld in artikel 252 Sr. waar in elk geval een deel van de daders in een meer sociaal isolement leeft – een groter deel van deze dadergroep in staat zal zijn om het online gedrag te verhullen door gebruik te maken van dit netwerk. Zo waarschuwen personen binnen het netwerk elkaar, brengen zij elkaar op de hoogte van werkwijzen van verschillende overheidsinstanties en geven zij elkaar bijvoorbeeld het advies een tweede telefoon te

hebben en content te wissen. Het kan een uitdaging zijn om daders te controleren, omdat actieve misleiding een rol kan spelen binnen de dadergroep.

Het kan moeilijk zijn om het gedrag van de dadergroepen te veranderen

Uit de interviews is gebleken dat het om dadergroepen gaat die veelal overtuigd blijven van het gedachtegoed, ondanks een veroordeling. In sommige gevallen stimuleert de omgeving dat, doordat bijvoorbeeld directe familie en vrienden het desbetreffende gedachtegoed delen. Ook speelt bij de verschillende vormen van extremisme, zoals politiek extremisme en de zogenoemde ‘autonomen’ een rol dat de dadergroep zich heeft afgekeerd van de overheid en het vertrouwen in de overheid laag is.¹⁵¹ Om die redenen is het moeilijk om het gedrag van de dadergroepen te veranderen door begeleiding en toezicht; ook hebben gesprekspartners de verwachting dat de doelgroepen minder bereid zijn mee te werken in vergelijking tot daders van een delict als bedoeld in artikel 252 Sr. Deze groep veroordeelden ervaren over het algemeen gevoelens van schaamte en negativiteit en zijn daardoor juist vaak gemotiveerd om hun gedrag te veranderen. Een andere ontwikkeling is dat daders steeds jonger zijn, waarbij de directe omgeving niet in de gaten heeft waar zij zich mee bezighouden. Dat komt doordat de wereld van jongeren zich met name online afspeelt en zij daar gerekruteerd en beïnvloed worden.¹⁵² Het gaat hierbij om een kwetsbare groep jongeren die vaak niet beseffen wat ze aanrichten in de samenleving en ook de gevolgen voor henzelf niet goed overzien. Het is van belang om rekening te houden met de kwetsbaarheid van deze jongeren, zeker omdat de informatie over het ouderschap en het stempel ‘terrorist’ iemand zijn leven lang kan achtervolgen en veel impact heeft.¹⁵³

Gesprekspartners van de Reclassering zien wel potentie in de controle voor hiervoor genoemde doelgroepen, omdat hiermee meer zicht wordt gekregen op het gedrag en daarover het gesprek met de betrokkenen kan worden gevoerd.

7.2.3 De techniek

Voor online terrorisme lijkt andere software vereist dan voor de controle van gegevensdragers van daders van een delict als bedoeld in 252 Sr

Voor controle bij dit type delict lijkt andere software vereist doordat het risicovolle gedrag bij zaken van online terrorisme verschillende online verschijningsvormen kent, die anders zijn dan de gedragingen bij zaken waar een delict als bedoeld in artikel 252 Sr is gepleegd. Ook het feit dat de daders beter in staat te zijn om hun gedrag te verhullen, waardoor mogelijk diepgravend online onderzoek nodig is om een goed beeld te krijgen van het risicovolle gedrag (zie paragraaf 7.2.2), speelt een rol. Het risico hiervan is dat de controle gaat raken aan opsporing. Bij doorontwikkeling zal moeten worden onderzocht of software beschikbaar is die in staat is een beeld te geven van het online gedrag, zonder dat het online onderzoek een te grote inbreuk maakt op de persoonlijke levenssfeer, en die past binnen de taak van de Reclassering. Daarbij is het krijgen van zicht op de digitale modus operandi van de veroordeelden behulpzaam, omdat op die manier sneller signalen van risicovol gedrag kunnen worden gedetecteerd, waardoor het onderzoek minder diepgaand hoeft te zijn. De software die wordt ingezet bij de controle van gegevensdragers van daders die

¹⁵¹AIVD, Nationale Politie & NCTV, *Met de rug naar de samenleving. Een analyse van de soevereinenbeweging in Nederland*, april 2024, p. 14.

¹⁵²C. Stoeldraaijers e.a., *Radicale reclame op sociale media: Een onderzoek naar online rekrutering door en voor extremistische groepen*, NSCR juni 2024.

¹⁵³<https://nos.nl/nieuwsuur/artikel/2536282-om-en-kinderbescherming-waarschuwen-voor-snelle-online-radicalisering-van-jongeren>.

veroordeeld zijn vanwege een delict als bedoeld in artikel 252 Sr is naar eerste inschatting in mindere mate geschikt voor dit type delict, omdat hiermee onvoldoende geautomatiseerd op de inhoud van de communicatie – zoals op chatgedrag en gedrag op sociale media – kan worden gescand. Wel kan met deze software gescand worden op het gebruik van bepaalde applicaties (zoals Telegram), wat ook voor terroristische delicten relevant is.

7.3 Cybercrime

7.3.1 Aard van de delicten

Cybercrime kent vele verschijningsvormen waardoor de aard van de delicten uiteenlopend is

Cybercrime is een verzamelnaam voor online criminaliteit. Hierbij wordt onderscheid gemaakt tussen delicten waarbij de computer als hulpmiddel wordt gebruikt en delicten die de computer als doelwit hebben. Delicten waarbij de computer een hulpmiddel is zijn bijvoorbeeld online oplichting (zoals bankhelpdeskfraude¹⁵⁴) of illegale handel op het *dark web* in wapens, drugs, persoonsgegevens, e.d. Delicten die de computer als doelwit hebben, zijn bijvoorbeeld door computers hacken of infecteren met ransomware, en Denial-of-Service (DDOS)-aanvallen.¹⁵⁵

Voor de eerste categorie delicten gaat het om delicten die zich voorheen afspeelden in de offline wereld en die nu (ten dele) verplaatst zijn naar de online wereld en waarbij de daders zich daarop hebben aangepast. Om de aard van deze delicten te doorgronden is het belangrijk te bekijken in hoeverre de computer het delict gedrag in algemene zin heeft veranderd en welke gedragingen juist hetzelfde zijn gebleven in vergelijking tot het traditionele delict. Vervolgens zal de specifieke wijze waarop de veroordeelde digitaal te werk gaat en het delict heeft gepleegd (de digitale modus operandi) van belang zijn om voldoende precies te kunnen formuleren wat de veroordeelde moet nalaten en om daarop te kunnen controleren.

De tweede categorie gaat om delicten die voor het digitale tijdperk niet bestonden. Mogelijk zijn de precieze risicovolle gedragingen die horen bij dit type delicten minder ver uitgekristalliseerd dan de meer traditionele ‘verplaatste’ delicten, omdat men niet kan terugvallen op het gebruik van bestaande inzichten over het gedrag van de ‘offline variant van het delict. Bij doorontwikkeling zal voor elk type cyberdelict bekeken moeten worden in hoeverre het online risicovol gedrag zodanig precies kan worden geformuleerd, zodat de bijzondere voorwaarde voldoende te controleren is. Dat vergt (technische) kennis over de digitale modus operandi bij deze verschillende soorten delicten.

7.3.2 Dadereigenschappen

Daders van cybercrime verschillen van elkaar in mate van professionaliteit

Uit onderzoek blijkt dat de diversiteit van het type cyberdaders groot is.¹⁵⁶ Dat betekent dat er ook verschillen bestaan in de mate van professionaliteit van daders.¹⁵⁷ De plegers van eenvoudiger online delicten, zoals online oplichtingspraktijken, hebben minder technische kennis nodig dan

¹⁵⁴ <https://www.consumentenbond.nl/veilig-internetten/bank-spoofing-oplichting-door-nepmedewerkers>

¹⁵⁵ Een DDOS-aanval is er op gericht een bepaalde online dienst of ondersteunende servers en netwerkapparatuur onbereikbaar te maken door enorm veel verzoeken tegelijkertijd, door middel van een botnet, op de server af te sturen. Het netwerkverkeer kan al deze verzoeken niet verwerken en komt tot stilstand; W. van der Wagen & J.J Oerlemans, *Basisboek cybercriminaliteit*, Den Haag: Boom 2024.

¹⁵⁶ W. van der Wagen e.a, *Cyberdaders: uniek profiel, unieke aanpak?* WODC 2019.

¹⁵⁷ W. van der Wagen e.a, *Cyberdaders: uniek profiel, unieke aanpak?* WODC 2019, p. 90.

daders die een online crimineel netwerk runnen, computers hacken of DDOS-aanvallen plegen. Aannemelijk is dat voor de categorie waarbij de computer als doelwit wordt gebruikt, de expertise van de daders over het algemeen hoger zal zijn, omdat technische kennis nodig is voor het plegen van dergelijke delicten. Deze laatste groep zal waarschijnlijk beter in staat zijn om de controle van digitale gegevensdragers door de Reclassering te omzeilen.

Bij een mogelijke doorontwikkeling van de controle op het gebied van cybercrime zal de Reclassering bedacht moeten zijn op deze verschillen in professionaliteit. Er zal een groep daders zijn met een hogere mate van professionaliteit, meer middelen en een breder crimineel netwerk, waardoor deze daders goed in staat zijn het gedrag af te schermen en de controle te omzeilen. Deze dadergroep lijkt zich niet te lenen voor het opleggen van een bijzondere voorwaarde in de vorm van een controle van digitale gegevensdragers; Door de hoge mate van professionaliteit zal de controle waarschijnlijk weinig effectief zijn. De dadergroep die minder technisch bekwaam is, leent zich beter voor controle. Aanbevolen wordt nader onderzoek te doen naar de typen daders van cybercrime (meer in het specifiek naar de relatie tussen het gepleegde cyberdelict en de technische expertise) om te bepalen welke typen cyberdelicten zich lenen voor controle.

Daders van cybercrime zijn geneigd het gedrag in stand te houden

Uit de interviews is gebleken dat deze dadergroep gemotiveerd is om het strafbare gedrag in stand te houden en af te schermen vanwege de positieve prikkels die aan het gedrag verbonden zijn. Met cybercrime kan met een relatief lage pakkans snel veel geld worden verdiend.¹⁵⁸ Daarnaast kan het een bepaald (gevoel van) status opleveren binnen een crimineel netwerk. Dit maakt het aannemelijk dat de dadergroep minder snel bereid is mee te werken in vergelijking tot daders van een delict als bedoeld in artikel 252 Sr. Zoals gezegd dragen bij die doelgroep juist vaak gevoelens van schaamte en negativiteit over het delict bij aan de bereidwilligheid om mee te werken. Het is van belang om onderzoek te doen naar de prikkels die kunnen bijdragen aan het positief beïnvloeden van het gedrag van de dadergroep van cybercrime en aan de bereidwilligheid om mee te werken aan controles. Ook onderzoek naar de wijze waarop deze effectief kunnen worden uitgevoerd, is van belang.

7.3.3 De techniek

Het is niet te verwachten dat voor alle varianten van online cybercrime dezelfde software kan worden gebruikt omdat, zoals hiervoor beschreven, de delicten qua aard verschillend zijn en ook de expertise om het gedrag te verhullen verschilt. Voor de meer professionele, georganiseerde online criminaliteit en de criminaliteit die de computer als doelwit heeft, is naar verwachting geavanceerde software nodig die diepgravend onderzoek kan verrichten om de modus operandi te herkennen, onder meer vanwege de expertise van de dadergroepen. Daarmee is er een gerede kans dat de controle het karakter van een opsporingsonderzoek krijgt.

Op basis van de gesprekken lijkt het niet onaannemelijk dat voor de minder geavanceerde online delicten, zoals verschillende vormen van online fraude, het gedrag makkelijker te detecteren is met een softwareprogramma. Dit omdat daders doorgaans minder geavanceerde technieken gebruiken om de delicten te plegen en mogelijk ook over minder kennis beschikken om het gedrag te verhullen. Als het risicovolle gedrag met name bestaat uit het bezoeken van bepaalde websites of het beschikken over bepaalde bestanden of programma's, dan kan de software die wordt gebruikt

¹⁵⁸ Zie over de pakkans bijvoorbeeld recent onderzoek waaruit blijkt dat online criminaliteit niet vaak leidt tot opsporing, vervolging en de berechting van daders. S. Ruijter e.a., *In- en doorstroom van online criminaliteit in de strafrechtssketen*, NCSR 2024.

voor de controle van digitale gegevensdragers op materiaal van seksuele uitbuiting van kinderen geschikt zijn voor dit type delicten. Is controle nodig die bijvoorbeeld gericht is op de inhoud van bepaalde online communicatie, dan zal andere software nodig zijn. Ook hierbij moet in het oog worden gehouden of het onderzoek niet een te grote inbreuk maakt op de persoonlijke levenssfeer van de betrokkene en of de controle past binnen de taak van de Reclassering.

7.4 Andere online seksuele delicten

7.4.1 Aard delicten

[Andere online seksuele delicten zijn qua aard meer vergelijkbaar met een delict als bedoeld in artikel 252 Sr](#)

Een deel van de daders van andere online seksuele delicten zullen vergelijkbaar online gedrag vertonen als de daders van een delict als bedoeld in artikel 252 Sr. Dat is bijvoorbeeld het geval bij seksueel getint chatten met minderjarigen en het bezitten of vervaardigen etc. van materiaal van seksuele uitbuiting van dieren. Doordat de online gedragingen meer op elkaar lijken en/of verband met elkaar kunnen houden, zeker in vergelijking tot de hiervoor besproken type delicten, is het mogelijk relatief eenvoudig om de controle van gegevensdragers voor deze delicten geschikt te maken.

Wel zal eerst per delict goed moeten worden onderzocht van welk risicovol online gedrag de veroordeelde zich precies moet onthouden en of dat gedrag goed controleerbaar is. Hierbij speelt mogelijk hetzelfde probleem als bij het bezitten of vervaardigen etc. van materiaal van seksuele uitbuiting van kinderen, namelijk dat het risicovolle gedrag dicht aan ligt tegen het strafbare gedrag. Het is dus belangrijk eerst te ondervinden of de (aangepaste) controle bij materiaal van seksuele uitbuiting van kinderen voldoende werkbaar is binnen de grenzen van wat is toegestaan.

7.4.2 Eigenschappen daders

[Een deel van de daders van andere online seksuele delicten zullen waarschijnlijk overeenkomsten vertonen met de daders van een delict als bedoeld in artikel 252 Sr](#)

Een deel van de daders van andere online seksuele delicten zullen naar verwachting meer overeenkomsten vertonen met daders van een delict als bedoeld in artikel 252 Sr in vergelijking met de hiervoor besproken typen daders. Dit beeld wordt bevestigd op basis van de gevoerde gesprekken. Dat is ook aannemelijk gelet op de jurisprudentie. Zo zijn er strafzaken waarin daders worden veroordeeld voor zowel het bezitten of vervaardigen van materiaal van seksuele uitbuiting van dieren als voor het bezitten of vervaardigen van materiaal van seksuele uitbuiting van kinderen.¹⁵⁹ Daarnaast wordt het daders van een delict als bedoeld in artikel 252 Sr in de bijzondere voorwaarde met regelmaat verboden om te chatten met minderjarigen.¹⁶⁰

Gelet op de mogelijke overeenkomsten tussen de daders is het aannemelijk dat een deel van deze daders bereidwillig is om mee te werken aan de controles vanwege gevoelens van schaamte en om

¹⁵⁹ Zie voor de samenloop bijvoorbeeld de volgende zaken: Rb Noord-Nederland 16 juli 2024, ECLI:NL:RBNNE:2024:2635; Gerechtshof Den Haag 26 augustus 2019, ECLI:NL:GHDHA:2019:2425; Rb Midden-Nederland 30 september 2021, ECLI:NL:RBMNE:2021:4785; Rb Limburg 18 april 2023, ECLI:NL:RBLIM:2023:2609.

¹⁶⁰ Dat beeld is naar voren gekomen op basis van de cijfermatige analyse van de jurisprudentie. Zie ter illustratie: Rb Rotterdam 1 februari 2022, ECLI:NL:RBROT:2022:1706; Rb Midden-Nederland 30 september 2021, ECLI:NL:RBMNE:2021:4785; Rb Noord-Nederland 15 mei 2019, ECLI:NL:2019:2253; Rb Noord-Holland, 7 september 2023, ECLI:NL:RBNHO:2023:8894; Rb Limburg 8 mei 2018, ECLI:NL:RBLIM:2018:4622; Rb Rotterdam 22 maart 2024, ECLI:NL:RBROT:2024:3580.

die reden ook gemotiveerd zijn hun gedrag te veranderen. Aanbevolen wordt om dit nader te onderzoeken, en om te bekijken of deze dadergroepen inderdaad overeenkomsten met elkaar vertonen of dat er toch belangrijke verschillen bestaan tussen de daders.

Indien er overeenkomsten bestaan tussen (een deel van de) daders van online zedendelicten, zal mogelijk de mate van technische kennis ook vergelijkbaar zijn met de daders van een delict als bedoeld in artikel 252 Sr. Een klein deel zal mogelijk over een geavanceerde technische kennis beschikken en in staat zijn hun online gedrag te verhullen. Dit zal echter niet voor de gehele dadergroep gelden. Aanbevolen wordt om ook wat betreft de technische kennis nader te onderzoeken of er overeenkomsten bestaan met daders van online zedendelicten, of dat er belangrijke verschillen zijn waar rekening mee gehouden dient te worden.

7.4.3 De techniek

Doordat er een zekere overlap bestaat tussen een delict als bedoeld in artikel 252 Sr en andere online zedendelicten, is de software die wordt ingezet voor de controle van digitale gegevensdragers op materiaal van seksuele uitbuiting van kinderen mogelijk ook geschikt of geschikt te maken voor andere online zedendelicten. Dat geldt in ieder geval voor materiaal van seksuele uitbuiting van dieren, omdat het daarbij ook zal gaan om het bezoeken van bepaalde websites en om het controleren op het gebruik van bepaalde zoektermen.

Voor het geautomatiseerd controleren op risicovolle gedragingen die verband houden met de inhoud van online communicatie, zoals chatgedrag met minderjarigen is naar verwachting andere software nodig. Bij het inzetten van nieuwe of doorontwikkelde software moet bekeken worden of het onderzoek niet een te grote inbreuk maakt op persoonlijke levenssfeer en of de controle past binnen de taak van de Reclassering.

7.5 Andere randvoorwaarden

Naast het onderzoeken en beoordelen of de delicten zich lenen voor een controle van digitale gegevensdragers van veroordeelde cliënten, is het voor succesvolle uitvoering van de controle noodzakelijk dat er bij de Reclassering voldoende capaciteit en deskundigheid aanwezig is om de controles te kunnen uitvoeren, de resultaten te kunnen interpreteren en om de gedragspatronen van de online gedragingen voldoende te kunnen herkennen en duiden. Deze deskundigheid is vooral van belang bij de meer geavanceerde vormen van cybercrime, omdat men de geavanceerde technieken die worden gebruikt moet kennen en moet weten hoe het gedrag wordt verhuld.

7.6 Conclusie

Als we kijken naar de aard van de delicten die centraal stonden in deze verkenning, kan geconcludeerd worden dat deze delicten over het algemeen qua aard niet overeenkomen met die van een delict als bedoeld in artikel 252 Sr, met uitzondering van de andere online zedendelicten. Dat geldt ook voor de typen daders. Dat maakt dat er bij doorontwikkeling voldoende aandacht moet zijn voor het precies omschrijven van de aard van het delict en het daarbij horende online gedrag waarop gecontroleerd kan worden. Daarnaast is het goed om oog te hebben of, gelet op de aard van het delict, niet te diepgravend onderzoek nodig is om het gedrag te detecteren, of de

typen daders in voldoende mate bereid zijn mee te werken en of een controle, gelet op de expertise van de daders, effectief kan zijn. In dit hoofdstuk hebben we dit per delict verkend.

Wat betreft online terrorisme, -extremisme en -radicalisering hebben we gezien dat het duiden en afbakenen van online risicovol gedrag bij online extremisme, -terrorisme en -radicalisering een uitdaging is, en nog in ontwikkeling. Wat betreft de dadereigenschappen, is uit interviews gebleken dat deze groepen beschikken over een groot collectief vermogen tot aanpassing en tot actieve misleiding. Het kan moeilijk zijn om het gedrag van deze dadergroepen te veranderen. Daarnaast is er een toename aan jonge daders waarneembaar.

Cybercrime is een verzamelterm voor verschillende delicten. Bij een deel daarvan wordt de computer als hulpmiddel gebruikt; het gaat dan om traditionele delicten die zich (ten dele) hebben verplaatst naar de online wereld. Bij andere vormen van cybercrime vormt de computer juist het doelwit, zoals een DDOS-aanval of een hack. Door de verscheidenheid aan delicten is er ook grote variatie in typen daders. Er zullen ook verschillen zijn in de mate van technische kennis van de dadergroepen en van hun professionaliteit. Doordat met cybercrime snel veel geld kan worden verdiend met een relatief lage pakkans, en dit een gevoel van status kan opleveren binnen een community, ervaren daders positieve prikkels om het gedrag in stand te houden.

Ten slotte geldt voor andere online zedendelicten dat deze naar hun aard meer vergelijkbaar zijn met een delict als bedoeld in artikel 252 Sr in vergelijking tot de voornoemde typen delicten. Uit deze eerste verkenning komt naar voren dat een deel van de daders qua eigenschappen naar verwachting meer overeenkomsten vertonen. Daardoor is er mogelijk bereidwilligheid mee te werken vanwege gevoelens van schaamte. De verwachting is dat ook het niveau van technische kennis vergelijkbaar is. Aanbevolen wordt de gelijkenissen en verschillen tussen dadergroepen van delicten als bedoeld in artikel 252 Sr en van andere online zedendelicten nader te onderzoeken.

Naar verwachting is de software die wordt gebruikt voor de controle van digitale gegevensdragers op materiaal van seksuele uitbuiting van kinderen in de meeste gevallen niet (direct) geschikt voor toepassing bij andere online delicten. Bij online terrorisme, -extremisme en -radicalisering is controle op de inhoud van communicatie op sociale media kanalen van belang, wat met de huidige software niet goed mogelijk is. Bij cybercrime zal het afhangen van de aard van de online gedragingen en de mate van technische complexiteit van het delict. Als het risicovolle gedrag zich met name richt op het zich begeven op bepaalde websites of het beschikken over bepaalde bestanden, dan is de software geschikt die wordt gebruikt voor de controle van digitale gegevensdragers op materiaal van seksuele uitbuiting van kinderen. Voor bepaalde andere online zedendelicten zoals dierenmisbruik leent de software zich naar waarschijnlijkheid ook. Zodra sprake is van online zedendelicten waarbij chatgedrag gecontroleerd moet worden zal andere software nodig zijn.

Ten slotte is het voor de uitvoerbaarheid van de controles bij alle beschreven delicten en dadergroepen noodzakelijk dat voldoende capaciteit en technische deskundigheid bij de Reclassering aanwezig is.

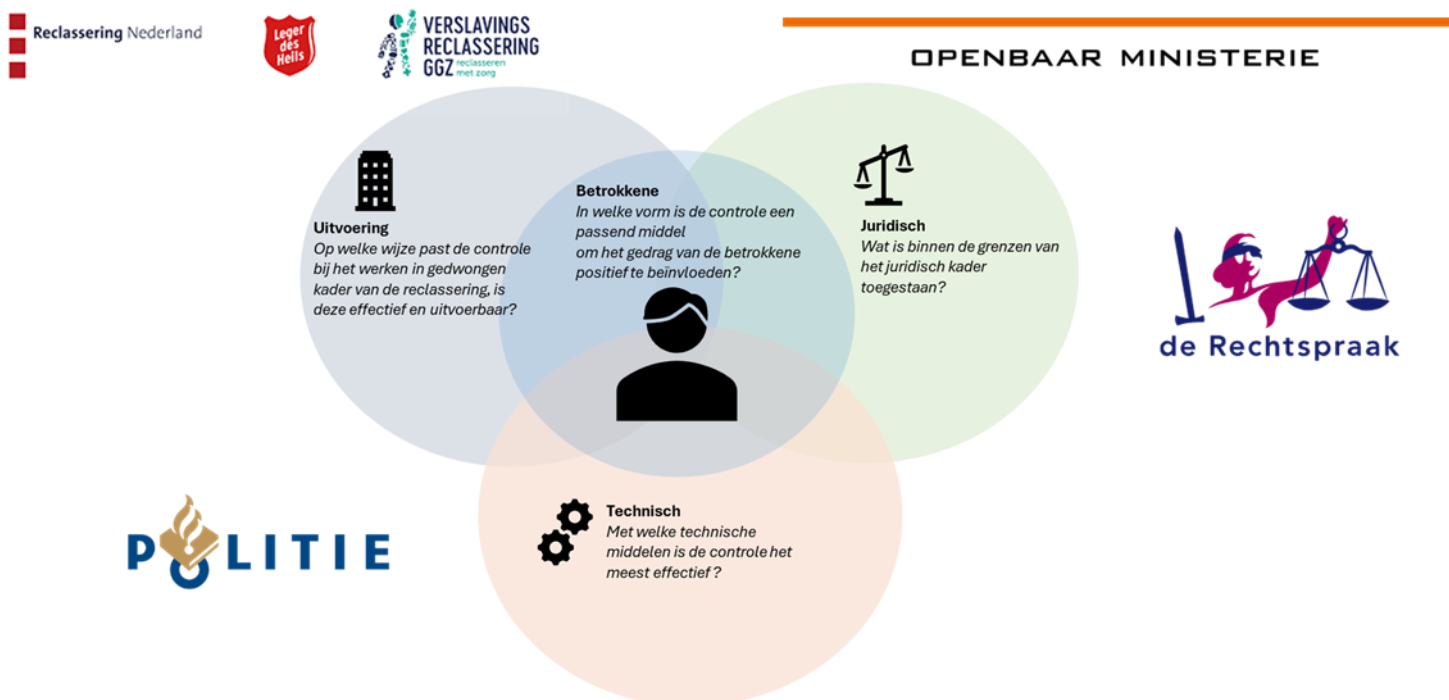
8. Bevindingen en aanbevelingen

8.1 Inleiding

In dit hoofdstuk ronden we het onderzoek af. Hier komt de informatie van de voorgaande hoofdstukken samen en volgt de afronding van de drie deelonderzoeken: de evaluatie van de oude werkwijze, het advies over de doorontwikkeling van de controle en de inzichten van de verkenning om de controle uit te breiden naar andere online delicten.

In de conclusies en aanbevelingen komen de lenzen die zijn beschreven in paragraaf 1.2 terug (zie figuur 6). Allereerst is informatie van de hoofdstukken 2 t/m 7 al aan de hand van deze lenzen verzameld en geanalyseerd. In de synthese van deze informatie reflecteren we in dit hoofdstuk nogmaals op deze lenzen.

Op die manier houden de conclusies en aanbevelingen rekening met het juridisch kader (wat is juridisch toegestaan?), de uitvoering (wat past bij de taak van de Reclassering?), de techniek (met welke middelen is controle effectief?) en de (rechten van de) betrokkene (in welke vorm is de controle een passend middel om het gedrag van de betrokkene positief te beïnvloeden?).



Figuur 6. De lenzen en betrokken actoren

8.2 Evaluatie oude werkwijze controle

De werkwijze – die gold van 2017 tot medio 2023 – sluit onvoldoende aan op het doel van de bijzondere voorwaarde

In deze conclusie toetsen we de oude werkwijze aan het juridisch kader. Uit de analyse in hoofdstuk 3. van de wetssystematiek van de bijzondere voorwaarden, de bedoeling van de wetgever en de arresten van de Hoge Raad kan worden geconcludeerd dat het opleggen van een bijzondere voorwaarde ten doel heeft (herhaald) strafbaar gedrag te voorkomen door goed levensgedrag van

de veroordeelde te bevorderen. Belangrijk voor de keuze voor een bepaalde voorwaarde is dat de bijzondere voorwaarde daadwerkelijk het doel van *gedragsverandering* dient. De controle van digitale gegevensdragers kan bijdragen aan dat doel. Door de bijzondere voorwaarde dient de veroordeelde namelijk de inhoud van zijn gegevensdragers te openbaren, waardoor controle op recidive of een mogelijke terugval mogelijk is. Om onder meer de inbreuk op de persoonlijke levenssfeer zo beperkt mogelijk te houden, mag de controle niet verder gaan dan noodzakelijk.

De Hoge Raad (paragraaf 3.3) en de lagere rechtspraak (hoofdstuk 4.) lijken – om met Mevis te spreken – door de jaren heen geworsteld te hebben met de vraag wat precies wel en niet mag in het licht van de controle en welke eisen aan het toezicht moeten worden gesteld. Deze onduidelijkheid had zijn weerslag op de uitvoering van de controle in de praktijk. In de arresten van de Hoge Raad van 31 mei 2022¹⁶¹ en 29 november 2022¹⁶² zijn de buitengrenzen waarbinnen de Hoge Raad de controle toelaatbaar acht verhelderd. Het is aan de lagere rechtspraak om binnen deze grenzen de praktijk voldoende duidelijkheid te bieden door de formulering van de bijzondere voorwaarde en het toezicht daarop. Binnen de door de Hoge Raad gestelde buitengrenzen zou de variatie in eisen moeten afnemen, wat de rechtszekerheid voor de praktijk vergroot.

In de oude werkwijze (zie paragrafen 5.6 t/m 5.9) voerde de Reclassering tezamen met de politie jaarlijks in vijftig gevallen een controle van gegevensdragers uit, waarbij de politie ondersteunde en verantwoordelijk was voor de technische uitvoering. Door de beperkte capaciteit stelde de politie als voorwaarde dat werd gecontroleerd in de gevallen waarin er indicaties waren dat strafbaar materiaal aanwezig zou zijn op de digitale gegevensdragers. Dit kon vervolgens leiden tot een nieuw opsporingsonderzoek. Met deze risicogerichte selectie werd slechts de groep gecontroleerd die hoogstwaarschijnlijk opnieuw een strafbaar feit had gepleegd.

Door deze focus aan te brengen, kon niet ingezet worden op gedragsverandering van de gehele doelgroep. Het controleren van de cliënten waarvan het aannemelijk is dat zij al in de fout zijn gegaan, kan bijdragen aan het goede levensgedrag en het voorkomen van nieuw strafbaar gedrag bij deze specifieke doelgroep in de toekomst. Maar doordat een groot deel van de doelgroep niet werd gecontroleerd, draagt deze aanpak minder bij aan de (preventieve) effecten die de controle heeft voor de gehele doelgroep waaraan de bijzondere voorwaarde is opgelegd. Bovendien dient een vonnis waarin de controle als onderdeel van de bijzondere voorwaarde is opgelegd, te worden uitgevoerd. De controle is niet voor niets opgelegd, uit het Reclasseringsadvies en de risicobeoordeling zal waarschijnlijk¹⁶³ naar voren zijn gekomen dat controle wenselijk is voor de specifieke betrokkene.

Als de controle niet wordt uitgevoerd of de kans op controle klein is, gaat dit ten koste van het stok-achter-de-deur effect van de controle.¹⁶⁴ Daarnaast wil de Reclassering met de controle juist op die situaties kunnen acteren waarin de cliënt mogelijk op het punt staat te recidiveren, zodat in het kader van risicomangement preventieve maatregelen kunnen worden genomen om het strafbare gedrag te voorkomen en daarmee het goede levensgedrag te bevorderen. Daarvoor was binnen deze werkwijze geen ruimte. Ons inziens past bij het doel en de essentie van de bijzondere voorwaarde een brede benadering, waarin alle cliënten aan wie de bijzondere voorwaarde is opgelegd worden gecontroleerd, ongeacht of er sterke signalen zijn dat de cliënt al de fout is ingegaan. De oude werkwijze sluit daar door haar gerichte focus op diegenen waarvan vermoedens

¹⁶¹ HR 31 mei 2022, ECLI:NL:HR:2022:807.

¹⁶² HR 29 november 2022, ECLI:NL:HR:2022:1763.

¹⁶³ Het blijft uiteraard mogelijk dat de OvJ de controle vordert of de rechter de controle oplegt, terwijl de Reclassering dat niet heeft geadviseerd.

¹⁶⁴ Uitgaande van het feit dat de voorwaarden veel vaker van vijftig keer per jaar werden opgelegd – waarbij meerdere keren per jaar kan worden gecontroleerd – is de controle gemaximeerd op vijftig keer per jaar, minimaal te noemen. De jurisprudentieanalyse ziet enkel op de gepubliceerde uitspraken op rechtspraak, dus deze cijfers zijn niet representatief. Uit de startnotitie blijkt dat de rechter jaarlijks in ongeveer 300 zaken de bijzondere voorwaarde oplegt. Helaas hebben wij de cijfers hierover niet ontvangen.

bestaan dat ze de bijzondere voorwaarde hebben overtreden, onvoldoende op aan en gaat daarnaast voorbij aan het feit dat een opgelegde bijzondere voorwaarde in een vonnis ook daadwerkelijk dient te worden uitgevoerd.

De werkwijze – die gold van 2017 tot medio 2023 – levert spanning op met de taak van de Reclassering

In deze conclusie staan we stil bij de vraag hoe de oude werkwijze zich verhoudt tot de taak van de Reclassering (paragraaf 5.2). De Reclassering heeft als taak de veroordeelde te begeleiden naar een gedragsverandering en daar toezicht op te houden, om op die manier de kans op recidive te verkleinen. De opgelegde bijzondere voorwaarden schrijven bepaalde gedwongen elementen van het toezicht voor. Binnen het toezicht moet echter ruimte blijven voor maatwerk om de begeleiding zo vorm te geven dat de cliënt kan leren, proberen, vallen en opstaan. De balans tussen controleren en begeleiden ziet er per cliënt verschillend uit en houdt verband met de waarden van de benodigde zorg, de veiligheid en de autonomie van de cliënt. In het bereiken van de gedragsverandering is de zogenoemde werkaliantie tussen de cliënt en de reclasseringsmedewerker van groot belang. Het (borgen van) het onderling vertrouwen en het werken aan gezamenlijk gestelde doelen is voor de werkaliantie een belangrijke basis.

De focus op het vinden van strafbaar materiaal bij de cliënten van wie sterke aanwijzingen zijn dat zij in de fout zijn gegaan en op het meewerken aan een controle die vervolgens kan leiden tot een nieuw opsporingsonderzoek, kan de werkaliantie tussen de reclasseringsmedewerker en de cliënt onder druk zetten. Dit kan leiden tot stroefheid bij de cliënt: de cliënt ervaart de interactie als negatief en verzet zich tegen verandering. Het begeleiden en begrenzen van cliënten moet in evenwicht met elkaar zijn. Dat werd bemoeilijkt door deze focus. Gevolg hiervan is dat de oude werkwijze spanning oplevert met de begeleidende taak van de Reclassering.

Ook de gevallen waarin de controle niet werd uitgevoerd, leveren spanning op met de taak van de Reclassering en de werkaliantie. In die gevallen werd een aan de Reclassering opgelegde taak niet uitgevoerd. Duidelijkheid over het juridisch kader, de gemaakte afspraken en wat cliënt en reclasseringsmedewerker over een weer van elkaar kunnen verwachten zijn voor de werkaliantie van belang (paragraaf 5.2). Het niet uitvoeren van de controle kan leiden tot onduidelijkheid aan de kant van de cliënt over wat hem in het reclasseringstraject precies te wachten staat en kan daardoor impact hebben op het onderling vertrouwen. Dit wringt te meer nu uit de analyse van de dadergroep blijkt dat de zekerheid dat een controle wordt uitgevoerd erg belangrijk is voor deze groep om niet terug te vallen in het strafbaar gedrag.

Concluderend levert de oude werkwijze spanning op met de waarden die horen bij de begeleidende en toezichthoudende taak van de Reclassering en met de werkaliantie op het niveau van de reclasseringsmedewerker en de cliënt.

De huidige instellingen van de gebruikte software leveren spanning op met de taak van de Reclassering

Het softwareprogramma dat werd gebruikt bij de oude werkwijze (paragraaf 5.8) kan zowel strafbare feiten als signalen van risicovol gedrag detecteren. Het gaat om een softwareprogramma in de vorm van een 'hit/no-hit systeem'. Het softwareprogramma bevat een mogelijkheid om afbeeldingen op gegevensdragers te vergelijken met een database van uit eerder politieonderzoek bekende versleutelde bestanden van seksuele uitbuiting van kinderen. Het softwareprogramma slaat de afbeeldingen op die *hits* opleveren. Deze afbeeldingen worden in de applicatie getoond. Een *hit* op de database van uit eerder politieonderzoek bekende versleutelde bestanden van seksuele uitbuiting van kinderen levert de verdenking van een strafbaar feit op. Dat is vanuit een opsporingsoogpunt een logische functionaliteit, maar levert, zoals in de voorgaande conclusie is omschreven, spanning op met de taak en waarden van de Reclassering en de werkaliantie waarin

het borgen van het vertrouwen tussen reclasseringsmedewerker en cliënt van belang is.

Doordat de software (mede) geschikt is voor detecteren van nieuwe strafbare feiten, is de software in huidige vorm, gelet op het voorgaande, minder geschikt voor de taak van de Reclassering, omdat dit spanning oplevert met de werkaliantie en de taak en waarden van de Reclassering.

Er is geen sprake van een schending van het nemo tenetur-beginsel

Zodra een zaak onherroepelijk is geworden en tot tenuitvoerlegging van de straf wordt overgegaan, is artikel 6 van het EVRM en het daaraan verbonden nemo tenetur-beginsel niet meer van toepassing. Van een *criminal charge* is op dat moment namelijk geen sprake meer. Wanneer de Reclassering een controle van de bijzondere voorwaarden uitvoert, valt die controle als zodanig niet onder de reikwijdte van dit beginsel. Dit is echter anders in het geval de controle ertoe leidt dat een verdenking ontstaat op basis waarvan opsporingsbevoegdheden worden ingezet. In dat geval is wel sprake van een *criminal charge*, maar betekent dit niet zonder meer dat er sprake is van een schending van het nemo tenetur-beginsel.

Met de gehanteerde instellingen van het softwareprogramma konden ook strafbare feiten in de vorm van materiaal van seksuele uitbuiting van kinderen worden gedetecteerd. De controle kon ertoe leiden dat een verdenking ontstond. Bij een verdenking werden op basis van de werkafspraken tussen politie, openbaar ministerie en Reclassering Nederland door de politie opsporingsbevoegdheden ingezet. Zoals hiervoor reeds is weergegeven, was in die situatie sprake van een *criminal charge*. Het nemo tenetur-beginsel was in die gevallen van toepassing. Dit bracht met zich dat ook ten tijde van de controle van de bijzondere voorwaarde het in paragraaf 6.2.3 beschreven toetsingskader van het EHRM in acht genomen moest worden. Op basis van toepassing van dit toetsingskader op de uitvoering van de controle van gegevensdragers komen wij in paragraaf 6.2.4 tot de conclusie dat van een algemene schending van het beginsel bij die controle geen sprake is.

Kenmerken die de effectiviteit van de controle beïnvloeden

In termen van effectiviteit nemen wij het gezichtspunt van de gedragsverandering als uitgangspunt, waarbij met de controle door de Reclassering toezicht wordt gehouden op het gedrag en naleving van de bijzondere voorwaarden, zodat waar nodig kan worden bijgestuurd. Dat sluit aan op het doel van de bijzondere voorwaarde en de taak van de Reclassering.

Uit paragraaf 5.10 is gebleken dat het niet mogelijk is harde uitspraken te doen over de effectiviteit van de controle gelet op een aantal beperkingen. Zo is door het ontbreken van of beperkt inzicht in cijfers niet duidelijk wat de precieze uitkomsten van de controle en van de opvolging daarvan waren. Ten slotte is er geen wetenschappelijk onderzoek beschikbaar naar deze specifieke interventie. Dergelijk onderzoek is ook erg lastig, omdat de controle altijd onderdeel is van een breder palet aan maatregelen, waardoor het moeilijk is bepaalde effecten aan een specifieke interventie toe te schrijven.

Hieronder noemen we enkele kenmerken die op basis van beschikbaar wetenschappelijk onderzoek en volgens de interviews invloed hebben op de effectiviteit.

Allereerst is het op basis van het *Risk-Need-Reponsivity* model belangrijk dat de intensiteit van de controle is afgestemd op het recidiverisico. Bij een lage recidivekans kan een hoge controle-intensiteit – denk bijvoorbeeld aan het wekelijks controleren – juist averechts werken. De Reclassering houdt hiermee rekening in het advies dat wordt uitgebracht door de voorgestelde maatregelen daarop af te stemmen, bijvoorbeeld in het advies over de frequentie van de controle.

Ten tweede wordt verondersteld dat van de dreiging van de controle al een positief effect kan uitgaan, namelijk dat deze dreiging de betrokkene weerhoudt om in het oude gedrag terug te vallen. Om dit effect te bereiken dient de dreiging van de controle wel voldoende reëel te zijn.

Ook hangt de effectiviteit af van het type dader. Uit de gesprekken is gebleken dat het hierbij om een spectrum gaat. Aan de ene kant de daders waarbij de controle effectief zal zijn, omdat ze gemotiveerd zijn om het gedrag te veranderen en controle een stok achter de deur is om hun drang te beheersen. Aan de andere kant van het spectrum zit een dadergroep die moeilijker te controleren is omdat deze gemotiveerd is het gedrag te verhullen. Dat betekent niet dat de controle in zijn geheel niet effectief kan zijn, omdat het verhullen constante aandacht vergt en deze groep op den duur tegen de lamp kan lopen. Dit zal afhangen van aantal en frequentie van de controles.

Daarnaast zal de effectiviteit van de controle samenhangen met de intensiteit ervan. Bepalend hiervoor is de vraag hoeveel gegevensdragers worden gecontroleerd, wat de software kan detecteren, of een handmatige controle wordt verricht en hoe intensief deze is.

De controle is niet waterdicht. Alleen de gegevensdragers die zichtbaar zijn worden gecontroleerd en ook het softwareprogramma kent beperkingen. Zo kan het softwareprogramma wel inzicht geven in het feit dat de cliënt iets heeft gewist, maar niet wat is gewist. Van belang is dat het softwareprogramma niet toepasbaar op alle beschikbare besturingssystemen. Een waterdichte controle is voor de werkwijze van de Reclassering ook niet nodig om voldoende effectief te zijn vanuit het gezichtspunt van gedragsverandering. Het is voor de Reclassering met name belangrijk dat de controle voldoende aanknopingspunten biedt om het gesprek over het gedrag te voeren. Wanneer uit de controle risicovol gedrag naar voren komt, kunnen vervolgstappen worden genomen.

Ten slotte kan inzicht in de digitale modus operandi bijdragen aan de effectiviteit van de controle doordat de uitkomsten van de controle hiermee beter kunnen worden geïnterpreteerd en geduid. Elke zedendelinquent heeft zo zijn eigen zoekmethoden, voorkeursapplicaties en digitale gedragspatronen. Als de Reclassering hiervan op de hoogte is, kan een aanwijzing dat de cliënt bijvoorbeeld actief is op een bepaalde applicatie of forum al een duidelijk signaal van risicovol gedrag opleveren, terwijl dat zonder deze informatie moeilijker is vast te stellen. De Reclassering kan inzicht in de digitale modus operandi krijgen door hierover het gesprek te voeren met de cliënt, deze informatie bij politie op te vragen en door het uitvoeren van de controles zelf.

8.3 Aanpassing/doorontwikkeling van de controle

Uit de evaluatie van de oude werkwijze (zoals deze is afgesproken in de werkwijze van 2017) is gebleken dat, gelet op het juridisch kader en de taak van de Reclassering, een aanpassing van de controle noodzakelijk is. Het is dan ook positief dat de Reclassering op dit moment deze nieuwe werkwijze ontwikkelt en daarbij de randvoorwaarde stelt dat de controle past bij haar taak. Het streven is dat Reclassering de nieuwe werkwijze in 2025 zelfstandig gaat uitvoeren. In de gesprekken kon geen duidelijkheid worden gegeven hoe de controles er in de toekomst uit gaan zien.

Wat wel duidelijk is, is dat de focus van de toekomstige controle komt te liggen op risicovol gedrag. De Reclassering wil niet actief op zoek gaan naar strafbare feiten. Op dit moment wordt onderzocht hoe de software zo kan worden aangepast, dat gezocht kan worden naar risicovol gedrag. De Reclassering zal eerst met een beperkte groep cliënten ervaring opdoen met de nieuwe werkwijze, om deze op basis daarvan verder bij te kunnen stellen.

In de volgende paragrafen volgen de aanbevelingen voor de doorontwikkeling van de controle. Deze zijn opgedeeld in aanbevelingen over de procedurele en organisatorische randvoorwaarden en aanbevelingen over de inhoud van de controle zelf. Deze aanbevelingen kunnen ook toegepast worden op andere strafrechtelijke titels dan de voorwaardelijke veroordeling met bijzondere voorwaarden, bijvoorbeeld de terbeschikkingstelling met voorwaarden en de voorwaardelijke invrijheidsstelling. Wel is van belang dat voor elke andere strafrechtelijke titel een afzonderlijke afweging moet worden gemaakt of de controle proportioneel is in relatie tot het doel van de titel.

8.3.1 Aanbevelingen procedurele en organisatorische randvoorwaarden

De Reclassering moet voldoende capaciteit en middelen hebben

Voor succesvolle implementatie van een nieuwe werkwijze zullen de nodige capaciteit en middelen moeten worden vrijgemaakt. Met de evaluatie in het achterhoofd, is de capaciteit een van de voornaamste punten om aan te pakken, nu juist het gebrek aan capaciteit ertoe leidde dat de controle slechts in een beperkt aantal gevallen werd uitgevoerd. Dat heeft vervolgens ook de focus van de werkwijze op potentiële overtreeders bepaald.

De Reclassering heeft op dit moment nog niet de technische kennis in huis om de controle zelf uit te voeren en om de rapportage die volgt uit het softwareprogramma te interpreteren. Uit de gesprekken met de politie is gebleken dat het expertiseniveau om de controle uit te voeren minimaal een HBO ICT-opleiding vereist. Momenteel is het personeel daarvoor niet opgeleid en is de expertise onvoldoende aanwezig. Hiervoor zullen aparte formatieplaatsen moeten worden gecreëerd, om mensen met een ICT/technologische achtergrond te kunnen aannemen. Hoeveel dat er zijn, zal afhangen van het aantal opgelegde bijzondere voorwaarden die de Reclassering moet uitvoeren.

Op dit moment is nog niet bekend hoeveel tijd de Reclassering nodig zal hebben om een controle uit te voeren en om de bevindingen te interpreteren. Zodra dat bekend is, kan in combinatie met de schatting van het jaarlijks aantal controles een berekening van de benodigde capaciteit en middelen worden gemaakt.

Een factor om rekening mee te houden is de kans dat het aantal opgelegde bijzondere voorwaarden in de nabije toekomst zal toenemen, mede door de Wet seksuele misdrijven. Op basis van deze wet kan de controle voor nieuwe online seksuele delicten worden opgelegd. De wet stelt namelijk van alle 'hands-on'-seksuele delicten, de online varianten expliciet strafbaar. Daarnaast is seksueel getint chatten met minderjarigen expliciet strafbaar gesteld (zie paragraaf 2.3). Een toename in bijzondere voorwaarden, vereist een navenante toename van capaciteit en middelen.

Indien de benodigde middelen niet of onvoldoende beschikbaar worden gesteld, komt het uitgangspunt dat de controles bij alle cliënten aan wie de bijzondere voorwaarde is opgelegd ook dient te worden uitgevoerd, onder druk te staan, en daarmee de effectiviteit van deze bijzondere voorwaarde.

De opgelegde bijzondere voorwaarde moet uitvoerbaar zijn

De Reclassering is verplicht om de onherroepelijk geworden rechterlijke uitspraak en de daarin geformuleerde bijzondere voorwaarde uit te voeren. Uit de gesprekken is gebleken dat dit niet altijd mogelijk is, doordat de formulering van de bijzondere voorwaarde in de praktijk niet uitvoerbaar blijkt. De door het Kenniscentrum Cybercrime opgestelde modelformulering blijkt dit probleem niet te hebben verholpen. Een van de problemen is dat de hoeveelheid controles die nodig zijn, uiteindelijk sterk afhankelijk zal zijn van het individuele geval. Het is begrijpelijk dat de rechter de

frequentie van het aantal controles beperkt, omdat de Hoge Raad een begrenzing aan het aantal controles vereist. In het overgrote deel van de gevallen wordt het maximum gesteld op drie controles per jaar. Om de controle-intensiteit passend te maken (en waar nodig bij te kunnen stellen) voor succesvolle gedragsbeïnvloeding van de individuele cliënt, stelt de Reclassering meer ruimte nodig te hebben voor maatwerk. Uit de jurisprudentieanalyse van hoofdstuk 4. is gebleken dat de elementen van de modelbepaling inmiddels in een groot deel (ongeveer de helft) van de vonnissen wordt opgelegd. Uit de jurisprudentieanalyse van hoofdstuk 4. bleek dat vanaf 2023 alle vonnissen – en in de jaren daarvoor ook al in toenemende mate – een beperking opleggen aan het maximaal aantal controles dat bij een cliënt mag worden uitgevoerd.

Met het oog op de inwerkingtreding van de Wet seksuele misdrijven is het van belang dat de bijzondere voorwaarde die ziet op het gedrag waarvan de veroordeelde zich moet onthouden, wordt herijkt om te voorkomen dat de bijzondere voorwaarde een herhaling bevat van de algemene voorwaarde. Zo is een veel voorkomende bijzondere voorwaarde dat veroordeelde zich onthoudt van het op digitale wijze met een seksuele intentie communiceren met minderjarigen/kinderen. Het is de vraag of de rechter deze formulering onder de nieuwe wet nog als bijzondere voorwaarde zal opleggen, aangezien deze zeer dicht tegen de formulering van het nieuwe strafbare feit, geformuleerd in artikel 251, eerste lid, onderdeel a, Sr zit.

Aangezien de doorontwikkeling van de controle nog in volle gang is, adviseren wij het openbaar ministerie, de Raad voor de Rechtspraak en de Reclassering een modelbepaling of bouwsteen te formuleren voor de oplegging van de bijzondere voorwaarde. Op die manier wordt uitvoerbaarheid beter verzekerd. Wel moet de modelbepaling of bouwsteen ruimte laten voor de onafhankelijke positie van de rechter om een individuele afweging te kunnen maken. Een blijvende wisselwerking tussen deze ketenpartners is nodig om op de hoogte te blijven van de actualiteiten en de uitvoerbaarheid van de controle in de praktijk, zodat daar op kan worden ingespeeld. Op die manier wordt voorkomen dat de beelden die over de controle bestaan bij partijen te veel uiteen gaan lopen. Een voorbeeld hiervan is dat uit de gesprekken is gebleken dat de geïnterviewden van de rechterlijke macht pas in een laat stadium op de hoogte raakten van de capaciteitsproblemen of daar in zijn geheel nog niet van op de hoogte waren. Onderling overleg is ook belangrijk met het oog op de vraag in hoeverre uitbreiding van de controle naar andere delicten mogelijk is, omdat hiervoor voldoende capaciteit moet zijn. In het onderling contact tussen ketenpartners dient uiteraard de onafhankelijke positie van de rechterlijke macht te worden gerespecteerd.

[Indien een controle door de rechter wordt opgelegd, moet deze worden uitgevoerd](#)

Indien de controle wordt opgelegd, heeft de Reclassering een plicht om deze uit te voeren. Aan die plicht moet dan ook (kunnen) worden voldaan. Dit komt allereerst het stok-achter-de-deur effect ten goede. Op die manier worden de positieve effecten die de controle heeft voor de gehele doelgroep ingezet, waarmee de werkwijze aansluit bij het doel en de essentie van de bijzondere voorwaarde. Als gemaakte afspraken worden nagekomen, komt dat ook de werkalliantie tussen reclasseringsmedewerker en cliënt ten goede.

8.3.2 Aanbevelingen inhoud controle

[De focus van de controle moet liggen op het verkrijgen van inzicht in risicovol gedrag](#)

Het onderzoek laat een spanningsveld zien tussen de taak van de Reclassering als het gaat om het toezicht en de controle op de naleving van de bijzondere voorwaarde(n) en de focus van de oude werkwijze, waarbij enkel cliënten werden gecontroleerd waarvan sterke vermoedens bestonden dat zij opnieuw een strafbaar feit hadden gepleegd. Het aanpassen van de software (zie hierna)

verkleint deze spanning, omdat daarmee niet langer direct op de aanwezigheid van het strafbaar materiaal wordt gezocht.

De spanning is voor dit type delicten echter niet in zijn geheel weg te nemen, omdat het gedrag waarvan de cliënt zich op grond van de bijzondere voorwaarde moet onthouden, heel dicht aan zit tegen het strafbare gedrag. Immers, indien een cliënt een website bezoekt waarvan bekend is dat er materiaal van seksuele uitbuiting van kinderen op aanwezig is, komt die handeling al heel dicht in de buurt van het strafbare feit.¹⁶⁵ Desondanks menen wij dat deze spanning acceptabel is, zolang de controle zich richt op het risicovolle gedrag en de gedragsverandering van de cliënten die de bijzondere voorwaarde hebben opgelegd gekregen. Een zekere spanning is ook inherent aan het werk van de Reclassering; deze kan bijvoorbeeld ook in het gesprek met een cliënt naar voren komen. Wel is belangrijk dat er duidelijke afspraken tussen de Reclassering en het openbaar ministerie zijn over de opvolging bij het aantreffen van een mogelijk strafbaar feit en daarmee van overtreding van de algemene voorwaarde (zie hierna). Door de focus te leggen op risicovol gedrag kan de reclasseringsmedewerker met de controle een beeld of aanknopingspunten krijgen hoe het met de cliënt gaat, om daarover vervolgens met de cliënt in gesprek te gaan. Daarbij kunnen vragen worden gesteld of hij zich onthoudt van gedrag zoals bepaald in de bijzondere voorwaarde, en kan worden achterhaald of er aanwijzingen zijn dat hij mogelijk gaat terugvallen.

De software moet op geautomatiseerde wijze risicovol gedrag kunnen detecteren

Gelet op het feit dat een handmatige controle een veel grotere inbreuk oplevert op de persoonlijke levenssfeer van de cliënt, moet de controle door middel van een geautomatiseerd softwareprogramma plaatsvinden (paragraaf 6.3).

Uit het voorgaande is gebleken dat het softwareprogramma dat werd gebruikt in de oude werkwijze niet geschikt is voor de Reclassering, doordat dit primair gericht is op de opsporing van strafbaar materiaal (paragraaf 5.8). Zoals we hiervoor hebben beschreven, levert dit spanning op met de taak van de Reclassering en de werkaliantie tussen reclasseringsmedewerker en cliënt.

Om die reden raden wij aan om de bibliotheek met versleutelde afbeeldingen van seksuele uitbuiting van kinderen als functie in het softwareprogramma uit te schakelen. De andere functies leveren naar verwachting geen problemen op, omdat daar aanwijzingen van risicovol gedrag uit kunnen worden gehaald, die – hoewel sommige signalen er dicht tegenaan kunnen zitten – niet meteen strafbare feiten inhouden. Deze manier van het uitvoeren van controle zal de Reclassering gaan beproeven met de tijdelijke voorziening. Het uitschakelen van de bibliotheek neemt niet weg dat het softwareprogramma nog steeds alle gegevens scant inclusief afbeeldingen. Daarmee blijft de gegevensverwerking impactvol voor de persoonlijke levenssfeer van de cliënt.

De vraag is vervolgens hoe het risicovolle gedrag op toereikende wijze gecontroleerd kan worden met het softwareprogramma. De Reclassering denkt daarbij zelf aan een lijst met vaste zoekwoorden die in verband kunnen worden gebracht met het risicovolle gedrag. Wij menen dat daarnaast bepaalde algemeen bekende signalen van risicovol gedrag nuttig zijn om mee te nemen, zoals het bezoeken van bepaalde websites, het aanwezig hebben van bepaalde applicaties (zoals een Tor-browser of wisprogramma's). Om de effectiviteit van het softwareprogramma te verhogen adviseren wij om bij de controle de digitale modus operandi van de cliënt in acht te nemen door de aanwijzingen van zijn bekende digitale gedragspatronen in de beschouwing te betrekken.

¹⁶⁵ Overigens is het niet aan de Reclassering om vast te stellen of inderdaad sprake is van een nieuw strafbaar feit. Het melden van een mogelijke overtreding van de bijzondere voorwaarden is aan de Reclassering, en het onderzoeken of er inderdaad sprake van een nieuw strafbaar feit aan het openbaar ministerie. Op grond van artikel 6: 3 : 14 lid 4 Sv. geldt dat als blijkt dat de veroordeelde de voorwaarde niet naleeft, de reclasseringsinstelling daarvan 'onverwijld melding' doet aan het openbaar ministerie en Onze Minister.

De verwachting is dat op grond van de indicaties van risicovol gedrag die uit de controle van gegevensdragers volgen, niet zonder meer een nieuwe verdenking van een strafbaar feit zal ontstaan op basis waarvan door de politie een nieuw opsporingsonderzoek wordt gestart waarbij onderzoeksbevoegdheden worden ingezet. Het nemo tenetur-beginsel speelt in die omstandigheid naar alle waarschijnlijkheid geen rol bij de controle van gegevensdragers door de Reclassering.

Een specifieke rechtsgrondslag voor de controle in een wet in formele zin verdient de voorkeur

Uit de analyse van artikel 8 EVRM (paragraaf 6.3) concluderen wij dat de controle een ingrijpende maatregel is die een inbreuk op levert in het privéleven van de cliënt. Dit, omdat het softwareprogramma grote hoeveelheden en potentieel zeer gevoelige gegevens verwerkt, waaronder soms bijzondere categorieën van persoonsgegevens. In lijn met de geanalyseerde arresten van de Hoge Raad, het advies van de Afdeling advisering van de Raad van State over onder meer de Wet gegevensverwerking door samenwerkingsverbanden, en met name de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 3 april 2024, en in het licht van artikel 10, eerste lid, Grondwet, verdient het de voorkeur om voor een dergelijke inbreuk een specifieke rechtsgrondslag op te nemen in een wet in formele zin. Deze specifieke rechtsgrondslag ontbreekt momenteel. Een logische plek voor deze grondslag zou artikel 14c, tweede lid, Sr zijn.

Gelet op het genoemde advies van de Afdeling advisering van de Raad van State, zijn hoofdelementen die in algemene zin in ieder geval in de formele wet moeten worden neergelegd de reikwijdte en de structurele elementen van een regeling. Die hoofdelementen zijn naar het inzicht van de onderzoekers in ieder geval het doel van de controle, dat de controle en daarmee de inbreuk op de persoonlijke levenssfeer beperkt dient te blijven tot het toezicht op de naleving van de bijzondere voorwaarden en dat de controle geautomatiseerd moet plaatsvinden.

Aanbevolen wordt om tevens rekening te houden met de ontwikkeling van de techniek, die kan leiden tot methoden en instrumenten die ingrijpender controles in de toekomst aanvaardbaar maken. Daarnaast is het advies om randvoorwaarden die invulling geven aan het doel van de controle, technologie-neutraal te formuleren. Gedacht kan worden aan een resultaatverplichting die voorschrijft dat het softwareprogramma aan bepaalde eisen voldoet, in plaats van het voorschrijven van concrete technieken.

Het is aan de wetgever om een afweging te maken of lagere regelgeving nodig is om bijvoorbeeld de geautomatiseerde controle technisch nader te specificeren. Dit in aanvulling op de ruimte die aan de rechter gelaten wordt om een nadere invulling te geven aan de bijzondere voorwaarde, afgestemd op het individuele geval.

8.4 Uitbreiding naar andere online delicten

Voldoende capaciteit, deskundigheid, en een aannemelijke mate van effectiviteit zijn randvoorwaarden voor uitbreiding

Uitbreiding van de controle naar andere online delicten, vereist allereerst voldoende capaciteit bij de Reclassering. Dat is in de huidige situatie niet het geval. Aanbevolen wordt de Reclassering de ruimte te geven om de komende jaren de controle van digitale gegevensdragers bij cliënten die veroordeeld zijn voor een delict als bedoeld in artikel 252 Sr te monitoren en te evalueren. Als uit evaluatie blijkt dat de controle goed verloopt, voldoende capaciteit kan worden vrijgemaakt om de controle toe te passen bij een ander online delict, de uitbreiding voor het type delict werkbaar en effectief wordt geacht, kunnen afspraken worden gemaakt met de ketenpartners over uitbreiding. Bij uitbreiding zullen ook meer ICT-deskundigen moeten worden aangenomen. Met voldoende

beschikbare capaciteit en kennis wordt ook voorkomen dat de Reclassering voor verrassingen komt te staan in geval van onvoorzienbare toenames in het aantal opgelegde controles.

Online terrorisme, extremisme en radicalisering

Het hebben van een extremistische overtuiging of het ontwikkelen van radicale ideeën is niet strafbaar, wel het plegen van een (terroristisch) misdrijf op grond van deze overtuiging of ideeën. Voor die misdrijven zou de bijzondere voorwaarde mogelijk bruikbaar kunnen zijn om recidive te voorkomen. Uit de gesprekken is naar voren gekomen dat er verschillend wordt gedacht over de mate waarin het verboden gedrag voldoende precies kan worden omschreven, gelet op de glijdende schaal tussen het risicovolle en strafbare gedrag. De Reclassering heeft hier de laatste jaren ervaring mee op gedaan en ziet mogelijkheden om het gedrag voldoende precies te formuleren, waardoor controle mogelijk wordt. In vergelijking met daders van een delict als bedoeld in artikel 252 Sr is het moeilijker het gedrag van deze dadergroepen te veranderen, onder andere doordat een deel zich heeft afgekeerd van of een laag vertrouwen heeft in de overheid, en actieve misleiding niet ondenkbaar is. Daarnaast wordt een deel van de doelgroep steeds jonger. Met name de jongeren in de doelgroep worden online gerekruteerd. De directe omgeving is hier veelal niet van op de hoogte doordat de gedragingen zich volledig online afspelen. Het gaat veelal om een kwetsbare doelgroep, die de gevolgen van het gedrag over het algemeen nog niet goed kan overzien. Bij de overweging om de controle in te zetten voor dit (jongere) deel van de doelgroep zal goed nagedacht moeten worden over de impact die het heeft op de toekomst van deze jongeren. De software die wordt ingezet bij de controle van digitale gegevensdragers van cliënten die veroordeeld zijn voor een delict als bedoeld in artikel 252 Sr is naar eerste inschatting in mindere mate geschikt, omdat hiermee onvoldoende de inhoud van de online communicatie kan worden gecontroleerd. Wel kan de software inzicht geven in het feit dat iemand actief is geweest op bepaalde applicaties, zoals Telegram.

Cybercrime

Cybercrime is een verzamelnaam voor online criminaliteit waarbij onderscheid kan worden gemaakt tussen twee typen delicten. Enerzijds gaat het om delicten die de computer als hulpmiddel gebruiken. Daarbij hebben offline delicten zich (ten dele) verplaatst hebben naar de online wereld en zich daarop hebben 'aangepast'. Anderzijds gaat het om delicten die de computer als doelwit hebben. Omdat sprake is aan een verscheidenheid aan delicten zal per delict moeten worden bekeken wat de aard van het online gedrag is, hoe de specifieke digitale modus operandi eruit ziet en of het verboden gedrag voldoende precies kan worden omschreven. Dit om te bepalen of dit gedrag controleerbaar is zonder dat het onderzoek te diepgravend wordt. Dat vergt (technische) kennis van deze delicten, zeker naarmate deze technisch gezien complexer worden. Een DDOS aanval is bijvoorbeeld technisch ingewikkelder dan het plegen van fraude via een online platform als Marktplaats.

Omdat cybercrime veel verschillende delicten omvat, is er ook grote variëteit in het type daders en in hun mate van professionaliteit. Voor de meer eenvoudige online delicten hoeft de technische bekwaamheid niet hoog te liggen. Er zal echter ook een groep daders zijn met een hogere mate van professionaliteit, die kunnen beschikken over middelen en een crimineel netwerk, wat hen in staat stelt hun gedrag af te schermen en de controle te ontlopen. De dadergroep met een hoge mate van professionaliteit lijkt zich daarom niet goed te lenen voor het opleggen van de bijzondere voorwaarde van controle van digitale gegevensdragers. Daarnaast ervaren daders van cybercrime positieve prikkels om het gedrag in stand te houden, omdat cyberdelicten over het algemeen een lage pakkans hebben en er snel veel geld en status mee kan worden verdiend. Hiermee zal de dadergroep in vergelijking met daders van een delict als bedoeld in artikel 252 Sr, naar verwachting minder geneigd zijn om mee te werken.

Of de software die wordt gebruikt bij de controle van gegevensdragers geschikt kan zijn voor daders van cybercrime hangt af van het precieze delict. In zijn algemeenheid zal de software niet geschikt zijn voor de meer geavanceerde delicten en de cyberdelicten waarbij controle van online communicatie van belang is. Voor de eenvoudigere delicten, waarbij met name gezocht moet worden op het voorhanden hebben van bestanden of het bezoeken van bepaalde websites, kan het programma geschikt zijn.

Andere online seksuele delicten

Een deel van de andere online seksuele delicten is qua risicovol gedrag en dadergroep nauwer verwant aan een delict als bedoeld in artikel 252 Sr, waardoor uitbreiding van de controle eenvoudiger te realiseren kan zijn. Een voorbeeld hiervan is het bezitten of vervaardigen van materiaal van seksuele uitbuiting van dieren. Het is mogelijk dat een deel van de daders ook qua dadereigenschappen, zoals technische kennis en bereidheid om mee te werken, vergelijkbaar is. Aanbevolen wordt nader onderzoek te doen naar de overeenkomsten en verschillen zijn tussen deze daders. Als op inhoud van communicatie gecontroleerd dient te worden zal andere of aangepaste software nodig zijn. Ook bij deze delicten is van belang dat per delict wordt bekeken of de software voldoende op risicovolle gedragingen kan zoeken, zonder dat het onderzoek te diepgravend wordt en neerkomt op het detecteren van strafbare feiten. Inzicht in de digitale modus operandi kan behulpzaam zijn om ervoor te zorgen dat het onderzoek niet te diepgravend wordt. Ten slotte is het nuttig om evaluaties van de controle van gegevensdragers op materiaal van seksuele uitbuiting van kinderen te betrekken bij de vraag in hoeverre de controles voor andere online seksuele delicten werkbaar zijn, gelet op de verwantschap van de delicten.

Literatuurlijst

AIVD, Nationale politie & NCTV 20224

AIVD, Nationale politie & NCTV, *Met de rug naar de samenleving. Een analyse van de soevereinenbeweging in Nederland*, april 2024.

Andrews e.a. 1990

D. A. Andrews, I. Zinger, R. D. Hoge, J. Bonta, P. Gendreau, F. T. Cullen, et al., 'Does correctional treatment work? A clinically relevant and psychologically informed meta-analysis. *Criminology*' 1990, 28.

Andrew, Bonta & Hoge 1990

D.A. Andrews, J. Bonta, & R.D Hoge, *Classification for effective rehabilitation: Rediscovering psychology. Criminal Justice and Behavior*, 1990, 17.

Bale 2017

H. Bale, *Online Child Sexual Offending. Psychological Characteristics of Offenders and the Process of Exploitation*, University of Edinburgh. 2017.

Beslisnota Directoraat-Generaal Straffen en Beschermen 2024

Beslisnota Directoraat-Generaal Straffen en Beschermen, Directie Sanctie- en Slachtofferbeleid van 9 februari 2024.

Bleichrodt 1996

F.W. Bleichrodt, *Onder voorwaarde. Een onderzoek naar de voorwaardelijke veroordeling en andere voorwaardelijke modaliteiten*. diss. Katholieke Universiteit. Deventer: Gouda Quint 1996.

Bleichrodt & Vegter 2021

F.W. Bleichrodt & P.C. Vegter, *Sanctierecht*. Deventer: Wolters Kluwer 2021.

Bosker e.a. 2020

J. Bosker, J. Monnee-van Doornmalen, R. Enskens, D. van der Plaat, *Effectieve werkwijzen in het reclasseringstoezicht. Een systematisch literatuuroverzicht*. KFZ 2020.

Bosker & Menger 2024

J. Bosker & A. Menger, *Werken in gedwongen kader*. Amsterdam: SWP Uitgeverij 2024.

De Hullu 2021

J. de Hullu, *Materieel strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht*, Deventer: Wolters Kluwer 2021.

Ezinga en Boelens 2019

M. Ezinga & M. Boelens, *Onderzoek naar terrorisme, extremisme en contraterrorisme*, WODC 2019.

Hurk, Van den & De Vries 2021

J.W. van Den Hurk & S.J. de Vries, *Onderzoek aan digitale-gegevensdragers. Een technische en juridische verkenning*, Deventer: Wolters Kluwer 2021.

Hustinx 1956

J.P. Hustinx, *De bijzondere voorwaarde. Preadviezen ter gelegenheid van de studiedag voor de reclassering*. 's-Gravenhage: Nationaal bureau voor reclassering 1956.

Kranenborg & Verhey 2024

H.R. Kranenborg & L.F.M. Verhey, *De Algemene verordening gegevensbescherming in Europees en Nederlands perspectief (tweede druk)*, Deventer: Wolters Kluwer 2024.

Ligthart 2022

S. Ligthart, *Coercive brain-reading in criminal justice: An analysis of European human rights law* Cambridge: University Press 2022.

Nan, BSb 2021

J.S. Nan, 'Een probleem rondom het nemo tenetur-beginsel?', *BSb* 2021 afl. 4, nr. 4.

Pivaty, Ter Vrugt & De Vocht 2021

A.Pivaty, P. ter Vrugt & D. de Vocht, *EmpRISe Netherlands: Policy Report*, 2021, UVT (www.empriseproject.org/policy-briefs/).

Post 2023

E. Post, *De kunst van het straffen? Forensische zorg als premisse*, diss. Vrije Universiteit 2023.

Ruijter 2024

S.Ruijter e.a, *In- en doorstroom van online criminaliteit in de strafrechtsketen*, NCSR 2024.

Stoeldraaijers e.a 2024

C. Stoeldraaijers e.a , *Radicale reclame op sociale media: Een onderzoek naar online rekrutering door en voor extremistische groepen*. NSCR juni 2024.

Struijk & Van der Wolf, AA 2018

S. Struijk & M. van der Wolf, 'Gevaarscriteria in het strafrechtelijk sanctierecht: een risicovol ratjetoe?', AA november 2018.

Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse Adopted by the Interagency Working Group in Luxembourg 2016

Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse Adopted by the Interagency Working Group in Luxembourg, 28 Januari 2016.

Van Toor 2017

D.A.G van Toor, *Het schuldige geheugen?* (diss. Nijmegen). Deventer: Wolters Kluwer 2017.

Van Toor, TBS&H 2021

D.A.G. van Toor, 'Het nemo-teneturbeginsel bij digitale opsporingsbevoegdheden: oproep tot discussie over fundamentele bezinning van de normering van het opsporingsonderzoek in een digitale context', *TBS&H* 2021, afl. 2 nr. 2.

Vegter & De Vries 2024

P.C. Vegter & E.J. de Vries, *Bijzondere voorwaarden bij V.I. Over het stellen van bijzondere voorwaarden door het Openbaar Ministerie in het kader van de voorwaardelijke invrijheidsstelling. Een rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het in art. 122 lid 1 Wet RO bedoelde toezicht*, januari 2024.

Veiligheidsagenda politie 2015-2018**Veiligheidsagenda politie 2019-2022****Veiligheidsagenda politie 2023-2026****Van der Wagen & Oerlemans 2024**

W. van der Wagen & J.J Oerlemans, *Basisboek cybercriminaliteit*. Den Haag: Boom 2024.

Van der Wagen 2019

W. van der Wagen e.a, *Cyberdaders: uniek profiel, unieke aanpak?* WODC 2019.

Werkafspraken bijzondere voorwaarden in zedenzaken 2017

Werkafspraken bijzondere voorwaarden in zedenzaken; controle digitale gegevensdragers tussen politie, openbaar ministerie en Reclassering Nederland, juni 2017.

Werkproces Indigo Den Haag 2013

Werkproces Indigo Den Haag (politie, OM, Reclassering, Waag, cq andere GGZ instelling) d.d. 20 augustus 2013.

Van Wijk 2019

A. van Wijk e.a. Niet meer doen. Een onderzoek naar de INDIGO-afdoening, Den Haag, 2019.

Bijlage I: De geschiedenis van de bijzondere voorwaarden

De geschiedenis van de voorwaardelijke straffen en bijzondere voorwaarden

De voorwaarde dat meegewerkt moet worden aan de controle van de digitale gegevensdragers valt in de ‘restcategorie’ van de bijzondere voorwaarden, te weten onder de rubriek ‘andere voorwaarden, het gedrag van de veroordeelde betreffende’. Die zinsnede is opgenomen in artikel 14c, tweede lid, onderdeel 14^o, Sr, maar komt in min of meer dezelfde bewoordingen terug in wetsartikelen met betrekking tot andere (afdoenings)modaliteiten in het Wetboek van Strafrecht en het Wetboek van Strafvordering. Soms is dat in de wettelijke bepaling opgenomen en soms blijkt dit uit toelichting bij verschillende artikelen waarbij expliciet wordt verwezen naar de mogelijkheid voorwaarden op te nemen als bedoeld in artikel 14c Sr.

In de loop van de vorige en deze eeuw zijn voor zowel volwassenen als jeugdigen op verschillende momenten bepalingen in werking getreden op grond waarvan voorwaarden kunnen worden verbonden aan een strafrechtelijke modaliteit. Denk bijvoorbeeld aan tbs met voorwaarden, een strafbeschikking met aanwijzing, een voorwaardelijke PIJ-maatregel (of voorwaardelijke beëindiging ervan) en voorwaardelijke jeugddetentie.¹⁶⁶ De bijzondere voorwaarde kan om die reden (mogelijk) ook verbonden worden aan andere modaliteiten. Dit blijkt ook uit recent onderzoek (2024) verricht door Vegter & De Vries (waarin zij verwijzen naar een rapport van de procureur-generaal bij de Hoge Raad in het kader van het in artikel 122, eerste lid, Wet RO bedoelde toezicht),¹⁶⁷ waarin wordt aangegeven dat de voorwaarde die centraal staat in dit onderzoek, weliswaar sporadisch, wordt verbonden aan een voorwaardelijke invrijheidsstelling.¹⁶⁸ Ook blijkt uit dat onderzoek dat de voorwaarde onderwerp van gesprek is in rechtspraak. Meer specifiek wordt gesteld: “Vanuit de Reclassering is naar voren gebracht dat de uitvoering van een dergelijke voorwaarde problematisch is omdat de politie kampt met een capaciteitsgebrek; aan de manier waarop de voorwaarde nu wordt geformuleerd kan geen uitvoering worden gegeven. Ook worden op directieniveau gesprekken gevoerd over de rechtmatigheid van deze voorwaarde.”¹⁶⁹

De voorwaarde ‘andere voorwaarden, het gedrag van de veroordeelde betreffende’ is in 1915 in de wet opgenomen, toen de voorwaardelijke veroordeling haar intrede deed in het strafrecht. De totstandkoming van de voorwaardelijke veroordeling wordt in de literatuur over het algemeen toegeschreven aan de introductie van de moderne richting in het strafrecht, waarbij afscheid werd genomen van de idee dat vergelding het hoofdzakelijke doel is van bestraffing. In de moderne richting kwam plaats voor de speciale preventie als strafdoel. Er komt meer oog voor de gedachte

¹⁶⁶ Bij de totstandkoming van de wetgeving inzake tbs met voorwaarden wordt expliciet verwezen naar de regeling van de voorwaardelijke veroordeling als het gaat om het stellen van bijzondere voorwaarden. Ook in latere wijzigingen van de regeling is de verwijzing naar de bijzondere voorwaarden in het kader van een voorwaardelijke veroordeling gebleven, zie bijvoorbeeld *Kamerstukken II*, 2009/2010, 32 319, nr. 3. In de toelichting op de totstandkoming van de strafbeschikking en de mogelijkheid om daaraan aanwijzingen te verbinden ‘het gedrag van de verdachte betreffende’ wordt expliciet verwezen naar artikel 14c Sr. zie *Kamerstukken II*, 2004/2005, 29 849, nr. 3. Als het gaat om jeugdigen en de mogelijkheid om voorwaarden te verbinden aan voorwaardelijke straf of maatregel kent artikel 77z Sr. een vergelijkbare lijst met voorwaarden als opgenomen in artikel 14c Sr. Zie voor de voorwaardelijke beëindiging van de PIJ-maatregel artikel 6:6:32 lid 5 Sv.

¹⁶⁷ P.C. Vegter & E.J. de Vries, *Bijzondere voorwaarden bij V.I. Over het stellen van bijzondere voorwaarden door het Openbaar Ministerie in het kader van de voorwaardelijke invrijheidsstelling. Een rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het in art. 122 lid 1 Wet RO bedoelde toezicht*, januari 2024.

¹⁶⁸ P.C. Vegter & E.J. de Vries, *Bijzondere voorwaarden bij V.I. Over het stellen van bijzondere voorwaarden door het Openbaar Ministerie in het kader van de voorwaardelijke invrijheidsstelling. Een rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het in art. 122 lid 1 Wet RO bedoelde toezicht*, januari 2024, p. 142. Voor voorwaardelijke invrijheidsstelling en de mogelijkheid om daaraan ‘andere voorwaarden, het gedrag van de veroordeelde betreffende’, zie artikel 6:2:11 Sv. voor volwassen veroordeelden en artikel 6:6:28 Sv. jo. artikel 77z Sr.

¹⁶⁹ P.C. Vegter & E.J. de Vries, *Bijzondere voorwaarden bij V.I. Over het stellen van bijzondere voorwaarden door het Openbaar Ministerie in het kader van de voorwaardelijke invrijheidsstelling. Een rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het in art. 122 lid 1 Wet RO bedoelde toezicht*, januari 2024, p. 143-144.

dat het strafrecht kan bijdragen aan gedragsverandering van de dader ook met het oog op het beschermen van de samenleving. Aandacht voor speciale preventie is één van de redenen dat de voorwaardelijke veroordeling en daarbij behorende bijzondere voorwaarden in 1915 in het Wetboek van Strafrecht wordt opgenomen. Andere redenen voor het introduceren van voorwaardelijke straffen met de mogelijkheid daaraan bijzondere voorwaarden te verbinden, zijn het beperken van het aantal kortdurende vrijheidsstraffen en het besparen van kosten.¹⁷⁰ De invoering van de mogelijkheid een voorwaardelijke veroordeling op te leggen brengt meer mogelijkheden met zich als het gaat om de individualisering van de straftoemeting.¹⁷¹

Van de vrije hand naar meer rechtszekerheid

Bij invoering van de mogelijkheid om bijzondere voorwaarden te verbinden aan (onder meer) een voorwaardelijke veroordeling en voorwaardelijke invrijheidstelling gaf de wetgever het OM en de rechterlijke macht grote vrijheid om te bepalen wat een bijzondere voorwaarde precies inhield; de wet schreef enkel voor dat de rechter 'voorwaarden het gedrag van de veroordeelde betreffende' kon opleggen.

In de literatuur zijn vele voorbeelden van 'creatieve' voorwaarden terug te vinden.¹⁷² Met de invoering van de bijzondere voorwaarden kreeg ook de Reclassering een rol bij het geven van advies en het houden van toezicht. De proeftijd, verbonden aan de voorwaardelijke veroordeling die voor misdrijven kon worden opgelegd, werd vastgesteld op maximaal drie jaar en voor overtredingen op maximaal twee jaar. Waarom de wetgever uiteindelijk voor deze termijn heeft gekozen, blijkt niet duidelijk uit de totstandkomingsgeschiedenis.¹⁷³

Wettelijke verankering van het stellen van specifieke bijzondere voorwaarden werd kennelijk niet nodig geacht, behalve de voorwaarde tot gehele of gedeeltelijke vergoeding van de door het strafbare feit veroorzaakte schade te vergoeden. Vragen over de reikwijdte van de voorwaarden waren er echter wel, zo blijkt uit een arrest van de Hoge Raad uit 1926. In dat arrest boog de Hoge Raad zich over de vraag wat verstaan moest worden onder 'voorwaarden het gedrag van de veroordeelde betreffende'. De vraag die in dit arrest voorlag was of de bijzondere voorwaarde dat de veroordeelde zich ter verpleging moest laten opnemen in een inrichting wel opgelegd kon worden. De Hoge Raad bepaalde dat onder 'voorwaarden het gedrag betreffende (...)' moest worden verstaan: 'voorschriften betreffende zijn handel en wandel te huis en in de samenleving, zijn wijze van leven'.¹⁷⁴ Die uitspraak leidde tot twijfel of opname in een inrichting ter verpleging wel toelaatbaar was op grond van de algemene formulering in de wet, mede vanwege de ingrijpendheid van de maatregel. Om die reden werd in 1929 in artikel 14c Sr de bijzondere voorwaarde opgenomen dat de veroordeelde zich gedurende een bepaalde periode ter verpleging zal laten opnemen in een daartoe aan te wijzen inrichting.

In de tweede helft van de vorige eeuw staat de bijzondere voorwaarde in de belangstelling vanwege de vraag of bijvoorbeeld castratie en het ondergaan van een refusalkuur¹⁷⁵ als bijzondere voorwaarden konden worden gesteld.¹⁷⁶ In verschillende (recente) arresten van de Hoge Raad

¹⁷⁰ E. Post, *De kunst van het straffen? Forensische zorg als premisse*, diss. Vrije Universiteit 2023, p. 72-73 en 329 en 334.

¹⁷¹ F.W. Bleichrodt, *Onder voorwaarde. Een onderzoek naar de voorwaardelijke veroordeling en andere voorwaardelijke modaliteiten*, diss. Katholieke Universiteit Nijmegen 1996, p. 28.

¹⁷² Zie bijvoorbeeld Post 2023, p. 76-77.

¹⁷³ E. Post, *De kunst van het straffen? Forensische zorg als premisse*, diss. Vrije Universiteit 2023, p. 74.

¹⁷⁴ J.P. Hustinx, *De bijzondere voorwaarde. Preadvies ter gelegenheid van de studiedag voor de reclassering*. 's-Gravenhage: Nationaal bureau voor reclassering 1956, p. 10-11.

¹⁷⁵ Refusal wordt gebruikt als ontwenningmiddel bij de behandeling van alcoholisme.

¹⁷⁶ Hustinx 1956, p. 20-21.

wordt nog steeds verwezen naar het arrest van de Hoge Raad van 26 november 1968.¹⁷⁷ In dat arrest werd door de Hoge Raad bepaald dat de bijzondere voorwaarde dat de veroordeelde binnen twaalf uur na zijn vrijlating Nederland diende te verlaten, ontoelaatbaar was, omdat:

“deze voorwaarde niet valt aan te merken als strekkende ter bevordering van een goed levensgedrag van de veroordeelde noch te betreffen een gedraging waartoe de veroordeelde uit een oogpunt van maatschappelijke betamelijkheid gehouden moet worden geacht.”

Beide hiervoor genoemde termen ‘goed levensgedrag’ en ‘maatschappelijke betamelijkheid’ hebben een normatief element.¹⁷⁸ Het is de vraag of de term ‘goed levensgedrag’ wel bruikbaar is in het huidige strafrecht. De wetgever stelt deze norm namelijk niet, maar de rechter die het criterium toepast moet interpreteren wat ‘goed levensgedrag’ is. Al in 1970 wees Enschedé erop dat in de “huidige pluriforme samenleving geen ondubbelzinnig antwoord meer mogelijk is op wat ‘goed levensgedrag’ is”.¹⁷⁹ In zijn proefschrift (1996) stelt Bleichrodt, mede onder verwijzing naar uitspraken van de Hoge Raad, dat het criterium van de maatschappelijk betamelijkheid reeds proportionaliteit impliceert. Alhoewel er ook aandacht is voor de subsidiariteitsgedachte lijkt de Hoge Raad deze, aldus Bleichrodt, niet in ‘volle gestrengheid’ toe te passen. “De Hoge Raad laat ‘enige ruimte voor een surplus aan de beperking van de handelingsvrijheid boven het strikt noodzakelijke’. ‘De criteria van proportionaliteit, subsidiariteit, individualisering en de doelcriteria van de Hoge Raad dienen m.i. in onderlinge samenhang te worden gezien [...]”¹⁸⁰

Met het wetsvoorstel van 2010 wordt de rechtsonzekerheid die gepaard ging met de algemene formulering van de bijzondere voorwaarde – tot op zekere hoogte – weggenomen door een aantal bijzondere voorwaarden in de wet op te nemen.¹⁸¹ De wijziging leidde niet tot een limitatieve lijst van voorwaarden die de rechter kan opleggen, want de algemene bepaling dat de rechter voorwaarden betreffende het gedrag kan opleggen, werd gehandhaafd. Het wetsvoorstel hangt ook nauw samen met het kabinetsbeleid tot het terugdringen van recidive. Omdat voor het verminderen van recidive is gedragsverandering noodzakelijk is, staat de persoonsgerichte aanpak hierbij centraal, zo blijkt uit de memorie van toelichting. Het wetsvoorstel beoogt ook de effectiviteit van het reclasseringstoezicht te verhogen.¹⁸² Het opnemen van dertien bijzondere voorwaarden in de wet wordt een feit met inwerkingtreding in april 2012.

Verruiming van de proeftijd c.q. duur

Een ander element dat van belang is bij de oplegging van de bijzondere voorwaarde, is de duur van de proeftijd. Immers, hoe langer de proeftijd, hoe ingrijpender de oplegging van een bepaalde bijzondere voorwaarde - zoals de controle van gegevensdragers - in potentie kan zijn voor de veroordeelde. In dat kader is voor de voorwaardelijke veroordeling de wetswijziging die in 2006 is doorgevoerd van belang. Deze wijziging leidde tot een verruiming van de proeftijd.

In een amendement op het wetsvoorstel ‘Wijziging van het Wetboek van Strafrecht en de Wegenverkeerswet 1994, in verband met de herijking van een aantal wettelijke strafmaxima’ in 2003 stelt Kamerlid Wolfsen voor om een proeftijd ten hoogste tien jaar te hanteren in die gevallen

¹⁷⁷ Hoge Raad 26 november 1968 *NJ* 1970/123.

¹⁷⁸ Conclusie PG, 22 februari 2022, ECLI:PHR:2022:170.

¹⁷⁹ Conclusie PG, 22 februari 2022, ECLI:PHR:2022:170; noot Enschedé onder arrest Hoge Raad 26 november 1968, *NJ* 1970, 123.

¹⁸⁰ F.W. Bleichrodt, *Onder voorwaarde. Een onderzoek naar de voorwaardelijke veroordeling en andere voorwaardelijke modaliteiten*, diss. Katholieke Universiteit Nijmegen 1996, p. 85.

¹⁸¹ Eerder was al wel de bijzondere voorwaarde in de wet opgenomen dat de rechter kon bepalen dat een som geld werd gestort in het schadefonds geweldsmisdrijven, *Stb.* 1993, 29.

¹⁸² *Kamerstukken II*, 2009/2010, 32 319, nr. 3.

waarin het OM dit heeft gevorderd en de kans op recidive aanzienlijk wordt geacht.¹⁸³ De toelichting is heel kort. De mogelijkheid om een langere proeftijd wordt belangrijk gevonden: “In een klein maar belangrijk aantal gevallen is het wenselijk om een langere periode “greep” te houden op de veroordeelde. Zo kan toezicht in een verplicht kader door de Reclassering op sommige ontuchtplegers wenselijk kan zijn”. Ook kan langer toezicht nodig zijn met het oog op behandeling in een gedwongen kader.¹⁸⁴ Enige tijd later volgt een gewijzigd amendement. De tekst komt te luiden dat de proeftijd tien jaar kan bedragen indien er ernstig rekening mee moet worden gehouden dat de veroordeelde wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen. In de toelichting daarop wordt aangegeven dat deze tekst meer recht doet aan de wetssystematiek, de bedoeling van de indieners van het amendement en de discussie die hierover is gevoerd in de Tweede Kamer. De proeftijd wordt ‘expliciet beperkt’ tot misdrijven die gericht zijn tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen.¹⁸⁵ Daarmee is de kans van herhaling, zo stellen Struijk & Van der Wolf, expliciet te relateren aan de aard van het misdrijf, een geweldsmisdrijf.¹⁸⁶ Of een proeftijd van tien jaar kan worden verbonden aan de voorwaarde die centraal staat in dit onderzoek, is maar zeer de vraag zoals hierna ook zal blijken bij de bespreking van de jurisprudentie van de Hoge Raad.

¹⁸³ *Kamerstukken II*, 2003/2004, 28 484, nr. 15.

¹⁸⁴ *Kamerstukken II*, 2003/2004, 28 484, nr. 15.

¹⁸⁵ *Kamerstukken II*, 2004/2005, 28 484, nr. 50.

¹⁸⁶ S. Struijk & M. van der Wolf, Gevaarscriteria in het strafrechtelijk sanctierecht: een risicovol ratjetoe?, AA november 2018.

Bijlage II: Respondentenlijst

Om de anonimiteit van de respondenten te verzekeren zijn slechts de functienaam en/of de organisaties waar de respondenten werkzaam zijn vermeld. Respondenten van de volgende organisaties zijn geïnterviewd:

- De Algemene Inlichtingen- en Veiligheidsdienst: analist
- Strafrechtadvocaat
- De Nationale politie: beleidsadviseur, landelijk coördinator en technisch rechercheur
- Het Openbaar Ministerie: twee officieren van justitie en beleidsadviseur
- Reclassering Nederland: drie beleidsadviseurs, jurist, twee reclasseringsmedewerkers
- Het Nederlands Instituut voor Forensische Psychiatrie en Psychologie: GZ-psycholoog
- Rechtbank: twee rechters
- Gerechtshof: twee raadsheren
- De Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen: onderzoeker
- Hoofddocent strafrecht
- Hoogleraar staats- en bestuursrecht

HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies



Bezuidenhoutseweg 161, 2594 AG Den Haag • T +31 (0) 6 39 27 85 33
E info@hooghiemstra-en-partners.nl • www.hooghiemstra-en-partners.nl
ING Bank NL49INGB0008938076 • KvK 73390356 • BTW 8595.06.447.B01