S. Royer & J.J. Oerlemans[1]

Naar een nieuwe regeling voor beslag op gegevensdragers

Computerrecht 2017/200

Gegevensdragers, zoals smartphones, tablets en computers, bevatten een schat aan informatie over hun eigenaars en gebruikers. Ze zijn daarom belangrijke tools in de zoektocht naar de waarheid in strafzaken. Digitaal bewijs is van groot belang zowel in cybercrimezaken als bij klassieke misdrijven. De inbeslagname en het uitlezen van gegevensdragers brengen helaas ook een verregaande privacy-inmenging met zich mee. In dit artikel bespreken de auteurs de huidige regelgeving en rechtspraak over de inbeslagname van gegevensdragers in België en Nederland. Vervolgens zoomen ze in op de relevante rechtspraak van het Europees Hof van de Rechten voor de Mens. Het artikel eindigt met een aantal mensenrechtenconforme aanbevelingen voor de Belgische en Nederlandse wetgever.

1. Inleiding

Digitaal bewijs wordt steeds belangrijker in strafzaken. In cybercrimezaken zijn de sporen op de computer van de verdachte uiteraard cruciaal. Zo nemen speurders in kinderpornozaken tijdens een huiszoeking alle relevante gegevensdragers in beslag om ze te onderzoeken op kinderpornografisch materiaal. Enkele terabytes aan te onderzoeken informatie is daarbij geen uitzondering. Ook in niet-cybercrime gerelateerde zaken, zoals moord- of drugsonderzoeken, kan digitaal bewijs van belang zijn. Een voorbeeld is te lezen in een recente uitspraak van de Rechtbank Rotterdam, waarin het Openbaar Ministerie een poging tot moord ten laste heeft gelegd. De verdachte probeerde haar man van het leven te beroven door hem te overgieten met terpentine en tijdens zijn slaap in brand te steken. De zoekgeschiedenis op haar smartphone leverde cruciaal bewijs op van de vereiste 'voorbedachte rade' bij moord. Op haar smartphone waren namelijk de veelzeggende zoektermen te vinden: "met terpentine overgieten", "terpentine verdampt", "oorzaak uitgebrande slaapkamer", "terpentine brand" en "man steekt dakloze die aan het slapen is in brand".[2] Een ander voorbeeld betreft een drugszaak waarin de Rechtbank Noord-Nederland expliciet in haar uitspraak opmerkt hoe de verdachte via *WhatsApp* prijslijsten van drugs en "aanbiedingen van de maand" naar zijn cliënteel stuurde, hetgeen bewijs voor drugshandel opleverde.[3]

De inbeslagname en het uitlezen van gegevensdragers zoals smartphones, tablets en computers, vormen een ernstige inmenging in het recht op privacy van de betrokkene. Die privacy-inmenging is verregaander dan twintig jaar geleden, vanwege de grote hoeveelheid en verscheidenheid aan opgeslagen gegevens en de manier waarop we tegenwoordig onze computers en smartphones gebruiken.

In België en Nederland zijn de afgelopen twee jaren belangrijke arresten gewezen over de inbeslagname van gegevensdragers. Daarnaast zijn er in dit kader enkele wetsvoorstellen geïmplementeerd of in ontwikkeling. In dit artikel staat de vraag centraal of de recente wijzigingen en voorstellen een stap in de goede richting zijn. Om die vraag te beantwoorden zetten we eerst de regelingen voor de inbeslagname van gegevensdragers in België en Nederland uiteen. Vervolgens bespreken we de knelpunten in het licht van verschillende grondrechten en de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: EHRM). Een nieuwe regeling moet uiteraard minimaal aan de vereisten van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) voldoen. We besluiten met vier suggesties om de huidige regeling voor de inbeslagname van elektronische gegevens en gegevensdragers te verbeteren. Het artikel behandelt alleen het algemene regime voor de inbeslagname van gegevensdragers en gaat niet in op de bijzondere beschermingsmechanismen voor o.a. beroepsgeheimhouders of journalisten.

2. De inbeslagname van gegevensdragers in België

Tot voor de Wet digitaal speurwerk[4] bepaalde de Belgische strafprocedure niet uitdrukkelijk welke instantie bevoegd was voor een informaticazoeking. Een informaticazoeking is het doorzoeken van een gegevensdrager die al dan niet in beslag is genomen (bijvoorbeeld het uitlezen van de inhoud van een smartphone). In de rechtsleer heersten verschillende opvattingen over welke instantie bevoegd was om de inhoud van een gegevensdrager te doorzoeken: elke politie-

1 Sofie Royer is doctoraatsassistent bij het Instituut voor Strafrecht aan de KU Leuven. Jan-Jaap Oerlemans is als onderzoeker verbonden aan eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden.

2 Rb. Rotterdam 16 mei 2017, ECLI:NL:RBROT:2017:4101. Zie bijvoorbeeld ook Hof Arnhem 4 mei 2012, ECLI:NL:GHARN:2012:BW4764 waarbij bewijs in een moordzaak werd geleverd door zoekwoorden als "Walther PPK", "Walther PPK onderhoud", "dood" en "kogel door het hoofd".

3 Zie Rb. Noord-Nederland 9 maart 2017, ECLI:NL:RBNNE:2017:843 en Rb. Midden-Nederland 3 januari 2017, ECLI:NL:RBMNE:2017:93.

4 Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS* 17 januari 2017 (hierna: Wet digitaal speurwerk). Voor een uitgebreide bespreking van de vernieuwingen door die wet, zie C. Conings & S. Royer 'Het verzamelen en vastleggen van digitaal bewijs in strafzaken' in: V. Buelens, C. Conings (e.a.), *Verslagboek permanente vorming 2016-2017*, Antwerpen: Intersentia 2017, p. 99-151 (hierna: Conings & Royer in: Buelens & Conings e.a. 2017).

ambtenaar, de officieren van gerechtelijke politie, de procureur des Konings of de onderzoeksrechter?[5] De uitbreiding van de informaticazoeking naar andere informaticasystemen die zich op een afstand bevinden en waarmee het oorspronkelijk doorzochte systeem is verbonden (bijvoorbeeld verbinding maken met de *Facebookapp* op een smartphone), wordt de netwerkzoeking genoemd. De netwerkzoeking is sinds de Wet informaticacriminaliteit[6] wel wettelijk geregeld (oud art. 88*ter* Belgische Wetboek van Strafvordering (hierna: B-Sv), nieuw art. 39*bis*, § 3 B-Sv). Oorspronkelijk was de onderzoeksrechter hiervoor exclusief bevoegd, maar ondertussen kan ook de procureur des Konings dit bevelen.[7]

Op 11 februari 2015 maakte het Hof van Cassatie een einde aan de discussie over wie bevoegd was voor de informaticazoeking. Het oordeelde dat "*het uitlezen van het geheugen van een mobiele telefoon […] een maatregel [is] die voortvloeit uit de inbeslagneming die kan worden uitgevoerd in het kader van een opsporingsonderzoek, zonder andere vormvereisten dan die welke bepaald zijn voor die onderzoekshandeling*". Het Hof voegde hieraan toe dat wanneer de inbeslagname van de gegevensdrager zelf niet gerechtvaardigd is, de procureur des Konings de relevante gegevens kan laten kopieren op dragers van de overheid. Politieagenten die belast zijn met het strafonderzoek hebben toegang tot gegevens die zijn opgeslagen op gegevensdragers en mogen die onderzoeken.[8] De wetgever nam de inhoud van dit arrest in een eigen interpretatie over in de Wet digitaal speurwerk.[9] Artikel 39*bis*, § 2 B-Sv bepaalt nu dat een officier van gerechtelijke politie een gegevensdrager die hij in beslag neemt, ook mag uitlezen. Wanneer hij de gegevensdrager niet in beslag neemt, is een bevel van de procureur des Konings nodig om de gegevens te kopiëren.[10] De al dan niet concrete inbeslagname van het informaticasysteem is volgens ons een eigenaardig onderscheidingscriterium om de bevoegdheid tot uitlezen te bepalen.[11] Er is immers een even grote privacy-inmenging wanneer de gegevensdrager in beslag wordt genomen en nadien doorzocht als wanneer de gegevensdrager ter plaatse wordt uitgelezen. Tot slot bepaalt artikel 39*bis*, § 2, lid 3 B-Sv dat speurders voor het begin van de zoeking elke externe verbinding moeten verhinderen en de vliegtuigmodus van het apparaat dus moeten inschakelen. Dit moet beletten dat ze zich tijdens het uitlezen begeven op netwerken die zich elders bevinden en waarvoor nu een apart bevel van de procureur des Konings vereist is.[12]

Hoewel de soepele beslag- en doorzoekingsbevoegdheid van gegevensdragers bij sommige auteurs op instemming kon rekenen,[13] waren het arrest van het Hof van Cassatie en de nieuwe bepaling in de Wet digitaal speurwerk ook het voorwerp van scherpe kritieken. Wij volstaan met de bezwaren die voor dit artikel van belang zijn. Algemeen luiden die dat het uitlezen van een smartphone of andere persoonlijke informaticasystemen een ernstige inmenging in de privacy inhoudt en dus met strenge waarborgen moet worden omgeven.[14] De vraag rijst of het nieuwe artikel 39*bis*, § 2 B-Sv de toets aan het recht op privéleven (art. 8, § 2 EVRM) doorstaat (*infra*). De afwezigheid van een voldoende voorzienbare en toegankelijke wettelijke rechtsgrond lijkt met het arrest en de nieuwe wet alvast te zijn opgelost. De overige kritieken op de cassatierechtspraak blijven wel onverkort gelden. Zo schuilt één van de problemen in de proportionaliteitstoets waaraan inmengingen in het recht op privéleven moeten voldoen. Speurders kunnen immers onbeperkt gegevens doorzoeken als ze de gegevensdrager zelf in beslag nemen of als ze over een bevel van de procureur beschikken. Een voorafgaande, onafhankelijke controle door een rechter ontbreekt. Ook wordt in de rechtsleer betreurd dat de wetgever niet heeft voorzien in een gebruiksverbod en een uitdrukkelijke plicht tot verwijdering van gegevens die geen verband houden met het onderzochte misdrijf.[15]

3. De inbeslagname van gegevensdragers in Nederland

In Nederland worden gegevensdragers als voorwerpen beschouwd die binnen een opsporingsonderzoek vatbaar zijn voor inbeslagname.[16] De algemene basis voor de inbeslagna-

5 *Pro* een rechterlijk bevel, zie o.a. C. Meunier, 'La loi du 28 november 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ére numérique', *RDPC* 2001, p. 663. *Contra* een rechterlijk bevel, zie o.a. J. Kerkhofs & P. van Linthout, *Cybercrime*, Brussel: Politeia 2013, p. 137-171.

6 Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001.

7 De Wet digitaal speurwerk uit 2016 versoepelde dus de voorwaarden voor de netwerkzoeking. Over het oude regime, zie C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013/5 (p. 23-32) (hierna: Conings & Oerlemans 2013).

8 Cass. 11 februari 2015, AR P141739F, *JT* 2015, afl. 6615, p. 634, concl. D. Vandermeersch; *RW* 2015-16, p. 621, noot C. Conings; *RDTI* 2015, afl. 61, p. 79, noot C. Forget; *T.Strafr.* 2015, afl. 3, p. 140, noot G. Schoorens; *Vigiles* 2015, afl. 4, p. 132, noot P. Vanwalleghem.

9 Wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, p. 12-16.

10 De wetgever verloor uit het oog dat het Hof van Cassatie eerder aanvaardde dat officieren van gerechtelijke politie in het kader van een regelmatige zoeking, alle goederen die kunnen dienen om de waarheid aan het licht te brengen, in beslag moeten nemen. Die rechtspraak kan volgens ons ook naar het databeslag worden doorgetrokken. Cass. 19 februari 2002, AR P001100N.

11 Conings & Royer in: Buelens & Conings e.a. 2017, p. 103.

12 De zogenaamde netwerkzoeking (artikel 39*bis*, § 3 B-Sv).

13 G. Schoorens, 'Noot onder Cass. 11 februari 2015', *T.Strafr.* 2015, afl. 3, p. 141-142; P. Vanwalleghem, 'Over het uitlezen van een gsm zonder tussenkomst van de onderzoeksrechter', *Vigiles* 2015, afl. 4, p. 134-136.

14 C. Conings, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America', noot onder Cass. 11 februari 2015, *RW* 2015-16, p. 624-625; C. Forget, 'Quelles garanties entourent la saisie de données informatiques et l'exploitation d'un système de données informatiques' (noot onder Cass. 11 februari 2015), *RDTI* 2015, afl. 61, p. 82-90; V. Franssen en S. Tosza, 'Vers plus de droits pour le justiciable sur internet? Un nouveau cardre légal pour lutter contre la criminalité dans la société de l'information' in: V. Franssen en A. Masset (eds.), *Les droits du justiciable face à la justice pénale*, Luik: Anthemis 2017, (205), p. 218.

15 D. Dewandeleer, 'Misdrijven en strafonderzoek in de IT-context' in *Straf- en strafprocesrecht*, Brugge: Die Keure 2010, (125), p. 141. Andere punten van kritiek gaan over de opheffing van het beslag en de onbepaalde bewaringsduur. F. Lugentz en D. Vandermeersch, *Saisie et confiscation en matière pénale*, Brussel: Bruylant 2015, p. 100; R. Verstraeten en L. Delbrouck, 'Beslag in strafzaken' in *Comm. Strafrecht* 2014, (1), p. 32.

16 HR 29 maart 1994, *NJ* 1994/577, m.nt. T.M. Schalken.

me van gegevensdragers in Nederland wordt gevormd door artikel 94 van het Nederlandse Wetboek van Strafvordering (hierna: N-Sv) jo. artikel 95 N-Sv en 96 N-Sv.[17] Inbeslaggenomen voorwerpen kunnen aan nader onderzoek worden onderworpen.[18] Voor gegevensdragers impliceert 'nader onderzoek' ook de analyse van gegevens die op de gegevensdrager staan opgeslagen.

Voor de inbeslagname van gegevensdragers tijdens een doorzoeking gelden, afhankelijk van de locatie, meer of minder waarborgen.[19] De officier van justitie kan bijvoorbeeld een bevel tot een doorzoeking in een kantoor uitvaardigen, waarna de inbeslagname van gegevensdragers kan plaatsvinden.[20] Slechts bij een doorzoeking in een woning en inbeslagname van gegevensdragers is een machtiging van een rechter-commissaris vereist.[21] Daarnaast kan een opsporingsambtenaar na aanhouding van een verdachte gegevensdragers in beslag nemen, voor zover de inbeslagname de waarheidsvinding dient of noodzakelijk is om wederrechtelijk verkregen voordeel aan te tonen.[22] In deze laatste situatie beslist echter een hulpofficier van justitie uiteindelijk over de inbeslagname en het daaropvolgend uitlezen van de gegevens die opgeslagen zijn op de gegevensdrager.[23] De hulpofficier van justitie geeft de gegevensdrager terug, indien de doelstelling van beslag niet meer aanwezig is.

De laatste jaren woedt er een discussie in de Nederlandse politiek en rechtspraak over de vraag of gegevensdragers speciale bescherming moeten krijgen binnen het strafrecht.[24] De vraag rijst of de huidige regeling voor inbeslagname voldoet, gezien de privacy-inmenging die de inbeslagname en het uitlezen van gegevens op gegevensdragers met zich meebrengen. In dit kader heeft de Hoge Raad op 4 april 2017 een belangrijk arrest gewezen in een zaak over de inbeslagname en het uitlezen van gegevens op een smartphone.[25] Een opsporingsambtenaar doorzocht na inbeslagname de inhoud van de smartphone, waarna hij gegevens – specifiek: één WhatsApp-gesprek – eruit viste, printte en toevoegde aan het strafdossier. Kort gezegd overweegt de Hoge Raad dat de regeling in artikel 94 N-Sv jo. artikel 95 N-Sv en 96 N-Sv voor de inbeslagname van een gegevensdrager door opsporingsambtenaren een onvoldoende grondslag is, indien daarbij een "*min of meer volledig beeld wordt verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker*". In dat geval is minstens een bevel van een officier van justitie of een machtiging van een rechter-commissaris vereist. De Hoge Raad geeft aan dat onderzoek door de rechter-commissaris op zijn plaats is in die gevallen waarin op voorhand is te voorzien dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn.[26] De regelingen waarbij al een bevel van een officier van justitie of een daarbij komend bevel van de rechter-commissaris is vereist, worden daarentegen door de Hoge Raad voldoende geacht.[27] Bovendien is de algemene bevoegdheid voor inbeslagname door opsporingsambtenaren volgens de Hoge Raad wel voldoende als de met het onderzoek samenhangende inbreuk op de persoonlijke levenssfeer als beperkt kan worden beschouwd.[28] Als voorbeeld geven de hoogste rechters aan dat "*dit het geval zou kunnen zijn indien het onderzoek slechts bestaat uit het raadplegen van een gering aantal bepaalde op de elektronische gegevensdrager of in het geautomatiseerde werk opgeslagen of beschikbare gegevens*".

Volgens ons is deze nuancering op de vereiste waarborgen voor de inbeslagname van gegevensdragers ongelukkig. Het brengt namelijk onzekerheid met zich mee, omdat nu bij elke zoeking de vraag kan worden opgeworpen of de inmenging in de persoonlijke levenssfeer door de zoeking 'slechts beperkt' is gebleven of niet. Alleen bij een 'volledige doorzoeking', waarbij een gegevensdrager in zijn geheel wordt gekopieerd en volledig – eventueel met behulp van forensische software – wordt onderzocht, is het helder dat de algemene bevoegdheid tot inbeslagname door opsporingsambtenaren niet voldoende is als grondslag. Meer principieel menen wij bovendien dat de inbeslagname van een gegevensdrager nooit slechts een beperkte inmenging in de rechten en vrijheden van de betrokkene met zich meebrengt.[29] Wij durven de stelling aan dat de meeste smartphonegebruikers het als een ernstige inbreuk op hun privéleven ervaren als de politie hun smartphone afneemt en 'enkele WhatsApp-berichtjes', de telefoongeschiedenis, of enkele foto's uitleest ten behoeve van haar taakuitoefening en niet als een 'beperkte privacy-inbreuk', zoals de Hoge

17 Zie voor een uitgebreide analyse van de Nederlandse regeling E. De Gritter, 'Opsporing in de digitale wereld: het onderzoek van in beslag genomen gegevensdragers', *Delikt en Delinkwent* 2016/43 (p. 493-503); P.A.M. Mevis, J.H.J. Verbaan, B.A. Salverda, 'Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten', Erasmus University/WODC 2016 (hierna: Mevis, Verbaan & Salverda 2016); B.J. Koops, C. Conings & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheid*, Preadvies voor de jaarvergadering van de Nederlands-Vlaamse Vereniging voor Strafrecht, Oisterwijk: Wolf Legal Publishers 2016 (hierna: Koops, Conings & Verbruggen 2016) en R. van den Bosch, 'Privacy in het digitale tijdperk: over de rechtmatigheid van het onderzoek aan een in beslag genomen smartphone', *TPWS* 2016/48, afl. 17 (p. 47-50) (hierna: Van den Bosch 2016).

18 Zie ook *Kamerstukken II* 1989/90, 21551, 3, p. 12-13.

19 Zie ook B.J. Koops, R.E. Leenes, P.J.A. de Hert & S. Olislaegers, *Misdaad en opsporing in de wolken: Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, TILT/WODC: Tilburg/Den Haag 2012, p. 59 (hierna: Koops e.a. 2012).

20 Op basis van art. 96c N-Sv.

21 Op basis van art. 110 N-Sv.

22 Op basis van art. 53 N-Sv en N-95 Sv. Volgens Koops, Conings en Verbruggen (2016) komt dit in de praktijk regelmatig voor.

23 Zie art. 116 N-Sv en paragraaf II.4 van de Aanwijzing inbeslagneming (artikel 94 Wvsv), *Stcrt.* 2014, 18598.

24 Zie het discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken', 4 juni 2014, p. 52-53; Hof Arnhem-Leeuwarden 22 april 2015, *Computerrecht* 2015/127 (p. 210-215), m.nt. J.J. Oerlemans; en J.J. Oerlemans, 'Rechtspraak verdeeld over rechtmatigheid van het doorzoeken van smartphones', *Computerrecht* 2016/116 (p. 204-205).

25 HR 4 april 2017, ECLI:NL:HR:2017:592, *NJ* 2017/230, m.nt. Kooijmans.

26 Zie HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.6.

27 Zie HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.4.

28 Zie HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.6.

29 Zie in soortgelijke termen ook Koops e.a. 2012, p. 59; Conings & Oerlemans 2013, p. 26; Hof Arnhem-Leeuwarden 22 april 2015, *Computerrecht* 2015/127 (p. 210-215), m.nt. J.J. Oerlemans; Van den Bosch 2016, p. 47-50; Koops, Conings & Verbruggen 2016, p. 78-80 en HR 4 april 2017, ECLI:NL:HR:2017:592, *NBSTRAF* 2017, afl. 6, m.nt. mr. T. Urbanus.

Raad suggereert.[30] De vraag rijst of de subjectieve beleving van de smartphonegebruiker het juiste criterium is. Toch lijkt de privacybeleving bij de Hoge Raad op dit punt wel erg ver te liggen van de privacybeleving die meer algemeen in de maatschappij heerst. Het arrest biedt wel extra bescherming voor het *volledig* uitlezen van inbeslaggenomen gegevensdragers door een bevel van een officier van justitie met eventueel een machtiging van de rechter-commissaris te vereisen.

Van belang is ook dat de Nederlandse wetgever op 7 februari 2017 een conceptwetsvoorstel heeft gepubliceerd dat ingaat op een nieuwe regeling voor de inbeslagname van gegevens en gegevensdragers.[31] Het wil een hogere waarborg introduceren voor het uitlezen van gegevens op een inbeslaggenomen gegevensdrager in de vorm van een bevel van een officier van justitie. Gezien de grote hoeveelheid persoonlijke gegevens die op een gegevensdrager opgeslagen kunnen zijn, acht de wetgever het wenselijk dat op zijn minst een officier van justitie het bevel moet geven om een computer of andere gegevensdrager in beslag te nemen. Als de wet al voorschrijft dat een rechter-commissaris deze toestemming moet verlenen, zoals bij een doorzoeking in een woning, dan blijft de huidige regeling gehandhaafd. Het arrest van de Hoge Raad laat bij een beperkte privacy-inbreuk de mogelijkheid open voor opsporingsambtenaren een gegevensdrager in beslag te nemen en uit te lezen, terwijl het wetsvoorstel voor het uitlezen van de gegevens een bevel van een officier van justitie vereist.[32] Het is aan de Nederlandse wetgever om wellicht in 2018 – wanneer het wetsvoorstel naar verwachting aan de Tweede Kamer wordt aangeboden – definitief voor meer bescherming van de inbeslagname van gegevensdragers te kiezen.

4. De rechtspraak van het EHRM

De inbeslagname van gegevensdragers doet op meerdere mensenrechtelijke vlakken vragen rijzen. Wij vragen ons daarom af of de wetgever terecht de regelgeving van de inbeslagneming van gegevensdragers op de klassieke regelgeving over het beslag ent. Eerst en vooral brengt de inbeslagname van gegevensdragers een stevige inmenging in het recht op privéleven met zich mee.[33] Gegevensdragers zoals smartphones worden immers steeds compacter en kunnen tegelijkertijd steeds meer informatie opslaan. Bovendien reizen draagbare gegevensdragers, zoals smartphones, tablets en laptops, overal mee met hun eigenaar, zodat zij dus meer persoonlijke informatie met zich meedragen (denk aan foto's, locatiegegevens, medische afspraken in de agenda en de internetzoekgeschiedenis). De vraag rijst of die verhoogde privacy-inmenging een aparte bevoegdheid voor de inbeslagname van gegevensdragers rechtvaardigt. Klassiek omvat de beslagbevoegdheid immers een doorzoekingsbevoegdheid. Vaak vindt de inbeslagname van voorwerpen, bijvoorbeeld wapens en drugs, plaats met het oog op verder onderzoek.[34] De wetgever scheert de beslag- en de doorzoekingsbevoegheid voor gegevensdragers over eenzelfde kam, maar verliest uit het oog dat een fundamenteel verschil bestaat tussen voorwerpen en gegevensdragers. De informatie die het ballistisch onderzoek van een inbeslaggenomen wapen bijvoorbeeld oplevert, is geenszins vergelijkbaar met de informatie die zich op een smartphone bevindt. Hoewel naar Belgisch recht geen rechterlijke tussenkomst vereist is voor het doorzoeken van de inhoud van een inbeslaggenomen handtas, die ook in beperkte mate foto's, afspraken of brieven kan bevatten, gaat de vergelijking met een smartphone niet op. Zowel de Belgische als de Nederlandse wetgever blijven niettemin vasthouden aan de verhoogde bescherming van de woning, die ze nog altijd als het centrum van het privéleven beschouwen.[35] Hieruit volgt dat de doorzoeking van vaste computers die zich eerder in de klassiek beschermde omgeving van een woning bevinden pas plaatsvindt na een rechterlijke tussenkomst, omdat een rechterlijk bevel vereist is om die plaatsen te doorzoeken.

Het EHRM beschouwt de doorzoeking en inbeslagname van elektronische gegevens of gegevensdragers steevast als een inmenging in één van de rechten beschermd door artikel 8, lid 1 EVRM, die aan de uitzonderingsvoorwaarden van artikel 8, lid 2 EVRM moet voldoen.[36] De inbeslagname en daaropvolgende doorzoeking vinden slechts plaats in het kader van een strafrechtelijk onderzoek. Daarmee wordt een legitiem doel nagestreefd.[37] Daarnaast moet het nationale recht in een toegankelijke en voorzienbare rechtsgrond voor de opsporingshandeling voorzien.[38] Met het nieuwe artikel 39*bis* B-Sv bestaat een voldoende voorzienbare en toegankelijke wettelijke rechtsgrond in de Belgische strafprocedure (*supra*). In Nederland bestaat ook een voorzienbare en toegankelijke wettelijke procedure voor de inbeslagname

30 Illustratief is het arrest van het Hof Arnhem-Leeuwarden 14 juli 2017, ECLI:NL:GHARL:2017:6069, waarin het Hof oordeelt dat er sprake is van een 'beperkte privacy-inbreuk', ondanks dat de politie de foto's en video's op de inbeslaggenomen smartphone van de verdachte heeft bekeken.

31 Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek (concept). Beschikbaar op: www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek. Het conceptwetvoorstel borduurt voort op het eerder genoemde discussiestuk over de inbeslagname van gegevensdragers.

32 Zie ook p. 50 van de toelichting op het conceptwetsvoorstel.

33 Zie ook C. Conings, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America', noot onder Cass. 11 februari 2015, *RW* 2015-16, (622), p. 624-625 en J.J. Oerlemans, *Investigating Cybercrime*, diss. Leiden, Amsterdam: Leiden University Press 2017, p. 125-126.

34 C. Conings, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America', noot onder Cass. 11 februari 2015, *RW* 2015-16, (622), p. 623.

35 In zowel België als Nederland is principieel een bevel van de onderzoeksrechter vereist (zie artikel 87 e.v. B-Sv, respectievelijk artikel 110 N-Sv). Zie hierover ook T. Timan en B.J. Koops, 'Sociale media en surveillance: over verschuivende rollen en vervagende grenzen', *Strafblad* oktober 2014, p. 284-290.

36 Meer bepaald het algemene recht op respect voor privéleven, respect voor privéleven binnen een woning en het recht op respect voor privécorrespondentie. Zie o.a. EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 65; EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 85; EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 41 en EHRM 16 oktober 2007, nr. 74336/01, (*Wieser en Bicos Beteiligungen GmbH/Oostenrijk*), par. 43.

37 Zie o.a. EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 68.

38 Zie bijvoorbeeld EHRM 27 september 2005, nr. 50882/99 (*Petri Sallinen e.a./Finland*), par. 92, waarin niet voldaan is aan die voorwaarde.

van gegevensdragers. De vraag is echter of de regelingen voldoende waarborgen bevatten om te voldoen aan de vereisten die het EHRM stelt op het vlak van de kwaliteit van wetgeving.[39] Als laatste voorwaarde moeten zoekingen en inbeslagnames noodzakelijk in een democratische samenleving zijn om het nagestreefde doel te bereiken. Het EHRM aanvaardt dat zoekingen en inbeslagnames voor de preventie van misdrijven noodzakelijk kunnen zijn, bijvoorbeeld om fysiek bewijsmateriaal te verzamelen.[40] Bovendien moeten de maatregelen proportioneel zijn. De lidstaten genieten in die beoordeling een zekere appreciatiemarge.[41] Een belangrijk aspect betreft de omvang van het beslag. Het is immers waarschijnlijk dat de gegevensdrager voor de strafprocedure irrelevante informatie bevat. De inbeslagname van de totaliteit van een gegevensdrager houdt volgens het Hof echter niet *per se* een schending van artikel 8 EVRM in,[42] maar het EHRM gaat wel na of er een onderscheid tussen relevante en irrelevante informatie wordt gemaakt.[43] Ook de mogelijkheid dat zich tussen de inbeslaggenomen gegevens data bevinden die onder het beroepsgeheim vallen, is problematisch in het licht van artikel 8 EVRM.[44]

4.1 *Voorafgaande rechterlijke machtiging vereist?*

Het EHRM vereist dat de interne procedure in voldoende en adequate waarborgen tegen misbruik en willekeur voorziet bij privacy-indringende maatregelen.[45] Zo lijkt het Hof in meerdere arresten aan te geven dat een rechterlijke tussenkomst voor de doorzoeking en inbeslagname van elektronische gegevens of gegevensdragers wenselijk is.[46] Niettemin stelt het een voorafgaandelijke rechterlijke machtiging niet uitdrukkelijk voorop, maar neemt dit wel mee in de beoordeling van de proportionaliteit. Een *a posteriori* rechterlijke controle kan het gebrek aan een voorafgaande rechterlijke controle compenseren.[47] Zo hield het EHRM er in de zaak *Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië* rekening mee dat er een apart rechterlijk bevel was voor de inbeslagname van de gegevensdrager en de doorzoeking ervan na de doorbreking van de verzegeling.[48] In de zaak *Trabajo/Spanje* ging het EHRM na of er sprake was van een 'noodsituatie'. Dit is een situatie waarbij de politie een rechterlijke machtiging niet langer kan afwachten zonder het onderzoek ernstig te belemmeren.[49] Een noodsituatie kan volgens het Hof het gebrek aan voorafgaande rechtelijke toetsing rechtvaardigen.[50] In de zaak *Trabajo/Spanje* was echter geen sprake van een noodsituatie. Het EHRM besloot dat de inbeslagname en het volledig uitlezen van alle bestanden op de computer zonder voorafgaande rechterlijke machtiging niet noodzakelijk was in een democratische samenleving en dus strijdig was met artikel 8 EVRM.[51]

Een voorafgaande rechterlijke controle is volgens het EHRM niet altijd een voldoende waarborg tegen mogelijk misbruik, bijvoorbeeld wanneer de rechterlijke machtiging te ruim is opgesteld.[52] Het disproportionele karakter van het beslag hangt dus vaak samen met een te ruim omschreven zoekingsbevel. Het EHRM veroordeelde België al wegens te ruime huiszoekingsbevelen in *Van Rossem/België* waarin een groot aantal papieren dossiers en documenten tijdens vijf huiszoekingen in beslag werden genomen in afwezigheid van de verdachte. Het huiszoekingsbevel waarin de onderzoeksrechter zijn zoekingsbevoegdheid in ruime bewoordingen aan een officier van gerechtelijke politie delegeerde,[53] moest volgens het Hof minstens de gegevens vermeld in de vordering van de procureur des Konings, bevatten.[54] Wanneer goederen buiten de draagwijdte van de machtiging in beslag worden genomen, maakt dit in elk geval een schending uit van artikel 8 EVRM, zelfs als ze na-

39 Zie ook Hof Arnhem-Leeuwarden 22 april 2015, *Computerrecht* 2015/127 (p. 210-215), m.nt. J.J. Oerlemans en HR 25 oktober 2016, ECLI:NL:PHR:2016:1047, concl. A-G F.W. Bleichrodt, r.o. 79-86.

40 EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 68; EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 91.

41 Zie bijvoorbeeld EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 89-90.

42 EHRM 2 april 2015, nr. 63629/10 en 60567/10 (*Vinci Construction et GTM génie Civil et Services/Frankrijk*), par. 76, waarin het Hof het beslag niet als een massabeslag bestempelde, maar wel tot een schending van art. 8 EVRM besloot wegens de afwezigheid van een effectieve *a posteriori* rechterlijke controle. Zie ook EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding As a.o./Noorwegen*), par. 173 e.v.; EHRM 16 januari 2009, nr. 10447/03, (*Maschino/Frankrijk*), nr. 34 waarin een grote hoeveelheid papieren informatie in beslag werd genomen in het kader van een fiscaal geschil.

43 EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 49 en EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 45.

44 Zie o.a. EHRM 2 april 2015, nr. 63629/10 en 60567/10 (*Vinci Construction et GTM génie Civil et Services/Frankrijk*), par. 79; EHRM 13 juli 2012, nr. 30457/06 (*Robathin/Oostenrijk),* nr. 52; EHRM 16 oktober 2007, nr. 74336/01, (*Wieser en Bicos Beteiligungen GmbH/Oostenrijk*), par. 43-65 en EHRM 7 juni 2007, nr. 71362/01, (*Smirnov/Rusland*), nr. 48.

45 Zie o.a. EHRM 2 april 2015, nr. 63629/10 en 60567/10 (*Vinci Construction et GTM génie Civil et Services/Frankrijk*), par. 66; EHRM 13 juli 2012, nr. 30457/06 (*Robathin/Oostenrijk),* nr. 44; EHRM 16 oktober 2007, nr. 74336/01 (*Wieser en Bicos Beteiligungen GmbH/Oostenrijk*), par. 43-57; EHRM 25 februari 1993, nr. 10828/84, (*Funke/Frankrijk),* par. 56.

46 Zie o.a. EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 45-48; EHRM 13 juli 2012, nr. 30457/06 (*Robathin/Oostenrijk),* nr. 44; EHRM 16 oktober 2007, nr. 74336/01 (*Wieser en Bicos Beteiligungen GmbH/Oostenrijk*), par. 43-58.

47 EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 46.

48 EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 98.

49 EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 36.

50 EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 46.

51 *In casu* was er immers geen risico dat de bestanden zouden verdwijnen, omdat de computer zich in de handen van de politie bevond en niet met het internet verbonden was. EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 45-48.

52 EHRM 28 april 2016, AR 41085/05, (*Bagiyeva/Oekraïne*), nr. 52. Zie ook EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 70 en 72: "*Although it might have been feasible to frame the warrants in more precise terms, it was sufficient, in the circumstances, that their scope was limited by reference to the nature of the alleged offence […]*". Zie echter de *dissenting opinion* van de rechters Grozev en Ranzoni die op grond van de Van Rossem-rechtspraak menen dat het bevel niet voldoende specifiek was, nu de speurders naast verschillende gegevensdragers ook cash geld in beslag hadden genomen.

53 Namelijk om "*alle voorwerpen en bescheiden van nut voor het onderzoek*" in beslag te nemen. EHRM 9 december 2004, nr. 41872/98 (*Van Rossem/België*); E. Brems, 'Van Rossem zorgt voor nauwkeuriger huiszoekingsbevel', *Juristenkrant* 2005, afl. 101, p. 13; A. Jacobs, 'Perquisitions et droits de défense: une remise en question des pratiques par la Cour européenne des droits de l'homme' (noot onder EHRM 9 december 2004), *RDPC* 2005, p. 903-927.

54 Dit omvat dus de inbreuken, hun voorlopige kwalificatie en het voorwerp van de huiszoeking. De Belgische cassatierechtspraak heeft zich, minstens gedeeltelijk, aan de Europese verplichtingen aangepast. Zie Cass. 11 januari 2006, nr. P051371F, *RW* 2006-07, p. 174, noot T. Decaigny.

dien worden teruggegeven.[55] In de proportionaliteitstoets gaat het EHRM dus na of de draagwijdte van de rechterlijke machtiging voldoende beperkt was.[56]

Het EHRM houdt daarnaast rekening met andere procedurele waarborgen. Zo besloot het EHRM in de zaak *Bernh Larsen Holding As a.o./Noorwegen* ten eerste dat artikel 8 EVRM niet was geschonden.[57] In het kader van een fiscaal geschil werd beslag gelegd op de volledige inhoud van een server die drie bedrijven deelden. De beslagenen beschikten wel over de mogelijkheid om beroep aan te tekenen tegen de inbeslagname en in afwachting werden de inbeslaggenomen gegevens verzegeld. Bovendien moest volgens de plaatselijke regelgeving de beslagene aanwezig zijn wanneer die verzegeling werd verbroken[58] en was de overheid verplicht de irrelevante gegevens terug te geven. Na de doorzoeking moest de overheid ook de inhoud en de sporen van de initiele kopie verwijderen.[59] Het Hof hield er wel rekening mee dat het ging over een fiscaal geschil. De inmengingen in het privéleven zijn in dat geval volgens het Hof "*not of the same seriousness and degree as is ordinarily the case of search and seizure carried out under criminal law*".[60] Het is dus niet uitgesloten dat het EHRM in een gelijkaardige strafzaak wel een schending vaststelt.[61] Ten tweede kan ook de aanwezigheid van getuigen tijdens de zoekingen en inbeslagnames een bijkomende waarborg zijn,[62] maar is niet altijd voldoende, namelijk wanneer blijkt dat de inventaris niet overeenkomt met de inbeslaggenomen stukken.[63] De aanwezigheid van een IT-specialist onder de speurders is ten derde een pluspunt.[64]

Als een voorafgaande rechterlijke controle niet aanwezig is,[65] hecht het EHRM bijzonder veel aandacht aan de mogelijkheid tot een effectieve *a posteriori* rechterlijke controle om de inbeslagname op zich te betwisten en de opheffing ervan te vragen.[66] Het EHRM aanvaardt dat gegevensdragers zoals computers tijdens de strafprocedure inbeslaggenomen blijven, om fysiek bewijsmateriaal veilig te stellen. Een effectieve *a posteriori* rechterlijke controle houdt niettemin in dat de rechterlijke instantie de relevantie van de inbeslaggenomen gegevens voor de strafprocedure nagaat.[67] Een belangrijke voorwaarde om *a posteriori* de opheffing van het beslag te kunnen vragen, is de aanwezigheid van een precieze lijst van inbeslaggenomen stukken. Het EHRM verbindt de incorrecte inventaris van inbeslagname in *Bagiyeva/Oekraïne* rechtstreeks aan de schending van artikel 8 EVRM.[68] De grote hoeveelheid inbeslaggenomen stukken doet geen afbreuk aan de verplichting om een precieze inventaris op te stellen. Zonder een precieze lijst van inbeslaggenomen stukken kan de beslagene immers *a posteriori* geen opheffing van het beslag vragen en kan de rechter die normaal over het beslag oordeelt, geen controle uitoefenen.[69]

4.2 *Andere verdragsrechten: eerlijk proces, effectief rechtsmiddel en recht op eigendom*

De inbeslagname van gegevensdragers doet ook vragen rijzen in het licht van andere grondrechten. Zo beschouwt het EHRM de klacht die inhoudt dat elektronisch bewijs werd gemanipuleerd of vervalst, als een probleem van onrechtmatig verkregen bewijs die ze niet behandelt in het kader van artikel 8 EVRM.[70] In de zaak *Khodorkovskiy en Lebedev/Rusland* riepen de verzoekers in dat de elektronische gegevens onrechtmatig waren verkregen en dus niet betrouwbaar waren. Het EHRM herinnert de verzoekers eraan dat de nationale rechters in principe oordelen of bewijsmateriaal betrouwbaar is. Ook de toelaatbaarheid van bewijsmateriaal is een nationale kwestie. Het EHRM gaat wel na of de verzoekers de mogelijkheid hadden om de authenticiteit te betwisten. *In casu* waren er volgens de verzoekers sterke vermoedens dat de speurders bijkomend bewijsmateriaal hadden ingeplant. Omdat de zoekingen zich op verschillende plaatsen afspeelden, konden de getuigen niet alles in het oog houden. Bovendien zou de informatie van een server gekopieerd zijn naar een *re-writable* harde schijf.[71] Het Hof was niet overtuigd van dit betoog.[72] In het algemeen is

55 EHRM 28 april 2016, AR 41085/05 (*Bagiyeva/Oekraïne*), par. 54.
56 EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 89-91.
57 Zie EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding As a.o./Noorwegen*), *Computerrecht* 2013/119, m.nt. M.M. Groothuis. Zie evenwel de *dissenting opinion* van rechters Berro-Lefèvre en Laffranque.
58 Zie ook EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 99, waarin het EHRM stelt dat de aanwezigheid van de beslagene bij het breken van de verzegeling een belangrijke waarborg is, "*which would have allowed them to perform an ex post facto check of the content of the computer in order to reveal any possible manipulation of the relevant files*".
59 EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding As a.o./Noorwegen*), par. 165 e.v.
60 EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding As a.o./Noorwegen*), par. 173.
61 Bijvoorbeeld in de zaak EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 45-48.
62 EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 91.
63 EHRM 28 april 2016, nr. 41085/05 (*Bagiyeva/Oekraïne*), par. 54.
64 EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 96
65 EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 73.
66 Zie o.a. EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 49; C. Conings, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America', noot onder Cass. 11 februari 2015, *RW* 2015-16, (622), p. 626. Zie ook EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 37-38.
67 "*[...] the lack of any consideration of the relevance of the seized information for the investigation and of the applicants' complaint regarding the personal character of some of the information stored on the computers rendered the judicial review formalistic and deprived the applicants of sufficient safeguards against abuse*" EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 49.
68 EHRM 28 april 2016, nr. 41085/05 (*Bagiyeva/Oekraïne*), par. 54.
69 EHRM 9 december 2004, nr. 41872/98 (*Van Rossem/België*), par. 50; A. Jacobs, 'Perquisitions et droits de défense: une remise en question des pratiques par la Cour européenne des droits de l'homme' (noot onder EHRM 9 december 2004), *RDPC* 2005, (903), p. 916.
70 EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L./Roemenië*), par. 101.
71 EHRM 25 juli 2013, nr. 11082/06 en 13772/05 (*Khodorkovskiy en Lebedev/Rusland*), par. 674 e.v.
72 EHRM 25 juli 2013, nr. 11082/06 en 13772/05 (*Khodorkovskiy en Lebedev/Rusland*), par. 700 e.v.

de afwezigheid van een effectief rechtsmiddel om de zoeking en/of het beslag aan te vechten in strijd met artikel 13 EVRM.[73] Het EHRM ging in dit geval niet na of dit ook een schending van het recht op een eerlijk proces (art. 6 EVRM) met zich meebrengt.[74]

Tot slot kan ook het recht op eigendom in het gedrang komen door de inbeslagname van een gegevensdrager. Zo stelde het EHRM een schending vast van artikel 1 Protocol 1 EVRM, in een zaak waarin beslag werd gelegd op de centrale server van een advocaat. Het Hof oordeelde dat de server niet zelf het voorwerp, middel of product van een misdrijf was, maar dat alleen de informatie opgeslagen op de server van belang was voor het onderzoek. Het Hof hield ook rekening met de persoonlijke en professionele ongemakken vanwege het meer dan zesjarig beslag op de server.[75] In *Prezhdarovi/Bulgarije* namen opsporingsambtenaren de computers in beslag van een computerclub die naar verluidt illegale *games* aanbood. Hoewel de eigenaar van de club ook een schending van artikel 6 EVRM en artikel 1 Protocol 1 EVRM inriep, behandelde het EHRM die zaak enkel in het licht van artikel 8 EVRM (*supra*).[76]

5. Suggesties

In dit artikel hebben we het Belgische en Nederlandse regime voor de inbeslagname van gegevensdragers tegen het licht gehouden. Ook de verplichtingen die voortvloeien uit de rechtspraak van het EHRM over de inbeslagname van gegevensdragers werden uitgebreid onderzocht. Op basis van die rechtspraak en in de overtuiging dat de inbeslagname van gegevensdragers een ernstige inmenging in de rechten en vrijheden van de betrokkenen met zich meebrengt, doen wij de volgende vier suggesties voor beide wetgevers.

5.1 *Onderscheid beslag- en de doorzoekingsbevoegdheid*

Wegens de verhoogde privacy-inmenging door het beslag op gegevensdragers, dringt zich volgens ons een onderscheid op tussen de beslag- en de doorzoekingsbevoegdheid. Een aparte inmenging in de rechten en vrijheden van de betrokkene vindt plaats bij enerzijds de inbeslagname van gegevensdragers en anderzijds het uitlezen van de gegevensdragers door een opsporingsambtenaar of IT-specialist. Dit onderscheid bestaat vooralsnog niet duidelijk in de huidige wetgeving. Wij kunnen ons niet vinden in het standpunt van de Nederlandse hoogste rechters dat in bepaalde omstandigheden de inbeslagname van een gegevensdrager én het uitlezen van enkele bestanden een 'beperkte inmenging' in het recht op privéleven is.

Het is onduidelijk of het EHRM meer waarborgen vereist voor de inbeslagname van gegevensdragers op zich, die niet gepaard gaat met het uitlezen van de gegevens. Niettemin lijkt een bevel op het niveau van de procureur des Konings/officier van justitie in dat geval wel wenselijk, gezien de – volgens ons – meer dan beperkte inmenging met de rechten en vrijheden van de betrokkene (waaronder het recht op eigendom en het recht op privacy). Een opsporingsambtenaar moet wel tot een kortdurende inbeslagname van gegevensdragers kunnen overgaan (bijvoorbeeld bij heterdaad, wanneer een groot risico bestaat op vernietiging/verdwijning van het bewijsmateriaal), zodat hij de tijd heeft om ondertussen de bevoegde magistraat te bereiken. Het EHRM is streng in de beoordeling van die dringende omstandigheden.[77] Voor de Nederlandse situatie kan met betrekking tot de initiële inbeslagname ook worden overwogen de beslissing omtrent de inbeslagname bij de hulpofficier van justitie te houden. Het beleggen van de beslissing bij een hulpofficier van justitie vormt een extra waarborg en blijft praktisch uitvoerbaar.

Voor het uitlezen en onderzoeken van de gegevensdragers en het in beslag nemen van de relevante gegevens[78] is anderzijds een rechterlijk bevel, met minstens een motivering en een proportionaliteitstoets vereist. Deze toets moet, eventueel achteraf als dat nodig is, een schriftelijke neerslag krijgen. De uitlezing moet beperkt blijven tot wat noodzakelijk is. Er moet dan wel een waarborg bestaan dat de verdachte/beslagene in tussentijd de gegevens op de gegevensdrager niet kan manipuleren. De vliegtuigmodus kan een praktische oplossing zijn voor dit obstakel. Dit sluit aan bij recente rechtspraak waarin het EHRM oordeelde dat een voorafgaande rechterlijke toetsing het verloop van de strafprocedure niet verhindert, wanneer er geen risico is op manipulatie van het bewijsmateriaal.[79]

5.2 *Invulling proportionaliteitsvereiste*

Het Belgische en Nederlandse regime voor de inbeslagname van gegevensdragers geven onvoldoende invulling aan het proportionaliteitsvereiste. Dit is problematisch vanwege de hoeveelheid gegevens die tegenwoordig op gegevensdragers is opgeslagen. De noodzakelijkheidstoets voor inbeslagname moet tweeledig zijn. Ten eerste mogen slechts die gegevensdragers in beslag worden genomen die noodzakelijk zijn voor de waarheidsvinding in strafzaken. Ten tweede mogen slechts gegevens die noodzakelijk zijn voor de strafprocedure, worden onderzocht. Het zoekingsbevel of de machtiging moet voldoende precies zijn met betrekking tot de onderzochte feiten, verdachte personen en te doorzoeken data.

73 EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 86.
74 EHRM 19 januari 2017, nr. 63638/14 (*Posevini/Bulgarije*), par. 92.
75 In dezelfde zaak vroeg het EHRM zich ook af of de wetsbepaling die het beslag toelaat op alle voorwerpen "*that could be instrumental for detecting a crime*" voldoet aan de "*quality of law*"-test. Het Hof spreekt zich verder niet uit over de vraag. Niettemin was het interessant geweest, nu in de Belgische strafvordering ook alles wat nuttig kan zijn voor de waarheidsvinding, in beslag kan worden genomen (art. 35 B-Sv). EHRM 7 juni 2007, nr. 71362/01 (*Smirnov/Rusland*), par. 56.
76 EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 34. Zie evenwel de *dissenting opinion* van rechter Vehabovic die meent dat artikel 8 EVRM in deze zaak niet van toepassing is.
77 EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*), par. 45: "*The Court, however, doubts whether the circumstances were really pressing, giving that the prosecutor ordered the said operation three weeks before it was conducted*." Zie ook EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 46-47.
78 Voor zover dit mogelijk is op een forensisch verantwoorde manier.
79 EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda/Spanje*), par. 46.

Daarbij moet wel de vraag worden gesteld in hoeverre naar ander strafbaar materiaal mag worden gezocht. Zo is het denkbaar dat speurders ook naar kinderporno kunnen zoeken op de inbeslaggenomen computer, hoewel het onderzoek in eerste instantie niet gericht was op kinderpornografie. Ook kan het in bepaalde onderzoeken wenselijk zijn om netwerkanalyses van criminele netwerken op de inbeslaggenomen gegevensdragers uit te voeren om tot identificatie van andere verdachten in criminele netwerken te komen.

De gebruiken voor databeslag in het Belgische en Nederlandse mededingingsrecht zouden ook voor de strafrechtspraktijk nuttige richtlijnen kunnen zijn.[80] Zo mogen speurders in het kader van de mededingingsprocedures niet massaal beslag op gegevens leggen, maar moeten ze op voorhand selecteren aan de hand van precieze sleutelwoorden.[81] Die sleutelwoorden mogen niet algemeen zijn, maar moeten binnen de juridische en economische context van de opdracht vallen. Bovendien is een bevestiging vereist van de geselecteerde gegevens aan de hand van een tweede sleutelwoord en vervolgens via statistisch verantwoorde steekproeven. Het bedrijf dat wordt onderzocht, moet aanwezig zijn bij de selecties en de kans krijgen om binnen een redelijke termijn bezwaren op te werpen. De gegevens die niet binnen de selectie vallen, moeten tot slot onherroepelijk verwijderd worden.

5.3 *Voldoende rechtelijke controle achteraf*

Als er geen rechterlijke machtiging aan de inbeslagname en het uitlezen van gegevensdragers voorafgaat, is een effectieve *a posteriori* rechterlijke toets onontbeerlijk.[82] Om die rechterlijke controle mogelijk te maken, moet een duidelijke inventaris van alle inbeslaggenomen goederen en gegevens worden opgesteld. Een hieraan gerelateerde suggestie is dat een regime voor bewaring en vernietiging van inbeslaggenomen gegevens moet worden uitgewerkt, omdat dit zowel in België als Nederland onbestaand is.[83] Het is van belang dat er een adequate klachtenregeling voorhanden is. De Nederlandse beklagprocedure in artikel 552a N-Sv voorziet niet in de mogelijkheid gegevens op een gegevensdrager te vernietigen die ten onrechte in beslag zijn genomen.[84] De beslagene moet ook over een procedurele mogelijkheid beschikken om persoonlijke gegevens die niet relevant zijn voor de strafprocedure, te kunnen terugkrijgen. In het conceptwetsvoorstel tot wijziging van boek 2 van het Nederlandse Wetboek van Strafvordering wordt hierover een regeling voorgesteld. In België geldt de procedure voor de opheffing van het beslag op fysieke goederen ook voor gegevens en gegevensdragers, maar bestaat onduidelijkheid over de precieze toepassing.[85] Om aan eventuele forensische bezwaren tegemoet te komen, is het denkbaar dat de beslagene zelf een gegevensdrager ter beschikking stelt, waarop de irrelevante gegevens kunnen worden gekopieerd.

5.4 *Richtlijnen voor inbeslagname en bewaring van gegevensdragers en digitaal bewijs*

In België bestaat geen openbare richtlijn op nationaal niveau voor de inbeslagname van gegevensdragers.[86] Een richtlijn voor de inbeslagname van gegevensdragers moet beter tot uitdrukking brengen hoe met digitaal bewijs moet worden omgesprongen en welke precieze stappen speurders zouden moeten doorlopen.[87] Een uiteenzetting van het regime voor de inbeslagname van voorwerpen voldoet niet, vanwege de specifieke eisen van *digital forensics*, die bijvoorbeeld verschillen voor smartphones en computers. Zo rijzen er ook prangende vragen over digitaal forensisch onderzoek waarbij computersystemen blijven aanstaan en wanneer de gegevens zich in de *cloud* bevinden.

Tot slot verdient ook de fysieke bewaring van harde schijven die digitaal bewijsmateriaal bevatten, aandacht. Dit begint met het op de juiste manier inpakken en transporteren van de harde schijven. Net zoals de bewaring van papieren dossiers, kunnen harde schijven en de opgeslagen gegevens immers onderhevig zijn aan externe factoren, zoals hitte, vocht of elektromagnetische velden. Om de authenticiteit van het bewijsmateriaal te verzekeren moet dit hele proces bovendien in processen-verbaal uitvoerig worden beschreven. Het risico bestaat dat na jarenlange bewaring in slechte omstandigheden, de gegevens niet langer leesbaar zijn.[88] Zelfs als de gegevens niet verloren gingen door de jarenlange bewaring, moet bovendien rekening worden gehouden met de constant evoluerende technologie, voornamelijk van smartphones. Gegevens moeten minstens leesbaar blijven tot een definitieve uitspraak, eventueel zelfs zolang een herzieningsprocedure tot de mogelijkheden behoort. Volgens ons zijn de inzichten van IT-specialisten bij de discussie voor een nieuwe regeling voor de inbeslagname van gegevensdragers nog onvoldoende meegenomen. Er is onvermijdelijk een grote rol voor hen weggelegd, zowel op de *crime scene* als in het verspreiden van kennis over de omgang met gegevensdragers en digitaal bewijs.[89]

80 Cass. 22 januari 2015, AR C130532F, 45-46, nr. 77; Conings & Royer in: Buelens & Conings (2016), p. 145; S. Gnedasi, 'Enkele reflecties over waarborgen bij onderzoek computergegevens', *AFT* 2015, afl. 3, (11), p. 20-21. In Nederland is de 'ACM Werkwijze digitaal onderzoek 2014' van 11 februari 2014 van toepassing. Zie enkele toepassingsgevallen over de betwiste reikwijdte van het digitale onderzoek binnen het mededingingsrecht (hetgeen voor het overige buiten het bestek van dit artikel valt): Rb. Den Haag 9 april 2003, ECLI:NL:RBSGR:2003:AF7087, r.o. 3; Rb. Den Haag 13 oktober 2008, ECLI:NL:RBSGR:2008:BH2647, r.o. 4.5-4.7 (over de oude Richtlijn van 6 juni 2003); en Rb. Den Haag 12 juli 2017, ECLI:NL:RBDHA:2017:7968, r.o. 2.4 en 2.9 (over de Richtlijn van 11 februari 2014).

81 Ondertussen bestaan er nauwkeurigere manieren om de relevante informatie te selecteren, zoals *predictive coding*.

82 Een *a posteriori* rechterlijke controle is ook van belang als er wel een rechterlijke machtiging was, bijvoorbeeld om na te gaan of de speurders binnen het kader van de machtiging hebben gehandeld. C. Conings, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld*, diss. KU Leuven 2016, p. 303.

83 Koops, Conings & Verbruggen 2016, p. 121-122.

84 HR 4 april 2017, ECLI:NL:HR:2017:592, *NJ* 2017/230, m.nt. T. Kooijmans.

85 Art. 28*sexies* Sv.

86 Op Europees vlak bestaan er wel aanbevelingen, zoals die van de European Union Agency for Network and Information Security, 'Electronic evidence – a basic guide for First Responders', maart 2015, www.enisa.europa.eu.

87 Zie ook Mevis, Verbaan & Salverda 2016, p. 78.

88 S. Mason & D. Seng (eds.), *Electronic evidence*, Londen: Institute of advanced legal studies 2017, p. 298.

89 G. Opernica, 'The lifecycle of electronic evidence', Presentatie op ERA conference, Londen, 8 juni 2017; G. Oparnica, 'Digital evidence and digital forensic education', *Digital evidence and electronic signature law review* 2016, p. 143-147.