



Raad voor de  
rechtspraak

De staatssecretaris Toeslagen en  
Douane  
Mw mr. S.Th.P.H. Palmen  
Postbus 20201  
2500 EE Den Haag

bezoekadres  
Kneuterdijk 1  
2514 EM Den Haag

correspondentieadres  
Postbus 90613  
2509 LP Den Haag

datum 19 december 2024

t (088) 361 00 00  
f (088) 361 00 22  
[www.rechtspraak.nl](http://www.rechtspraak.nl)

bijlage(n)  
onderwerp Advies Wetsvoorstel internettoezicht douane

Geachte mevrouw Palmen,

Bij e-mail van 3 oktober 2024, volgende op de brief met kenmerk 2024-0000435046, verzocht u de Raad voor de rechtspraak (de 'Raad') advies uit te brengen inzake de Wet tot Wijziging van de Algemene douanewet met betrekking tot de controlebevoegdheden op het internet, maatregelen ter verbetering van het douanetoezicht (het 'Wetsvoorstel').

## HET WETSVOORSTEL

De douane mag gegevens en informatie verzamelen in het kader van risicobeheer. Dat verzamelen kan ook door middel van het doorzoeken van het internet. Wanneer persoonsgegevens worden verwerkt bij het doorzoeken van het internet naar goederen, bij het handhaven van sancties of bij het voorkomen dat (absoluut) verboden goederen de Europese Unie worden binnengebracht, wordt een inbreuk gemaakt op de persoonlijke levenssfeer van diegene van wie de persoonsgegevens worden verwerkt. Dit Wetsvoorstel beoogt transparantie over het gebruik van internet. De regels hierover dienen duidelijk in de wet verankerd te zijn, zodat inzichtelijk is in welke gevallen en onder welke voorwaarden persoonsgegevens verwerkt kunnen worden. Om dit te bewerkstelligen voorziet het Wetsvoorstel in de opname van expliciete grondslagen, waarborgen en randvoorwaarden voor de verwerking van persoonsgegevens bij het doorzoeken van het internet in de Algemene douanewet (Adw).<sup>1</sup>

Het Wetsvoorstel strekt onder meer tot regulering van openbronnenonderzoek op internet (ook wel: Digital Open Source Intelligence (Digital OSINT)). In een nieuwe afdeling 'internettoezicht' worden verschillende controlebevoegdheden geïntroduceerd. Het is de Raad opgevallen dat voor een aantal (onderdelen van deze) controlebevoegdheden reeds een strafvorderlijke grondslag bestaat, dan wel dat in de (nabije) toekomst met de inwerkingtreding van het beoogde nieuwe Wetboek van Strafvordering in een dergelijke strafvorderlijke grondslag zal worden voorzien. De Raad meent dat het verschil in rechtskarakter van de bevoegdheden (controle versus opsporing) geen belemmering vormt om de

---

<sup>1</sup> MvT, p. 2 en 3.



# de Rechtspraak

Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 2 van 14

(toekomstige) strafvorderlijke bevoegdheden als vertrekpunt te nemen bij de analyse van de in dit Wetsvoorstel opgenomen controlebevoegdheden.

Na overleg met de gerechten, adviseert de Raad als volgt.<sup>2</sup>

## ADVIES

De Raad onderschrijft het belang van het wettelijk normeren van controlebevoegdheden die een meer dan beperkte inbreuk op de persoonlijke levenssfeer tot gevolg kunnen hebben. Over de precieze uitwerking van die bevoegdheden heeft de Raad enkele opmerkingen die hier artikelsgewijs besproken worden.

### Ten aanzien van artikel 1:23m

De Raad heeft een aantal opmerkingen over de opsomming van artikel 1.23m en de onderlinge verhouding tussen de begrippen in die opsomming.

Allereerst merkt de Raad op dat ‘*virtual reality*’ (zoals Metaverse) lijkt te ontbreken in de opsomming, terwijl in de MvT bij artikel 1:23o lid 2 wel wordt verwezen naar virtuele werelden, zoals Metaverse.

De opsomming van artikel 1:23m lid 1 begint met het begrip ‘het wereldwijde web’, oftewel: het world-wide-web (www) (artikel 1:23m lid 1 sub a). De term world-wide-web wordt onder meer gebruikt om te verwijzen naar het informatiesysteem waarin (kort gezegd) webpagina’s via URL’s/hyperlinks toegankelijk zijn voor gebruikers.<sup>3</sup> Artikel 1:23m lid 2 bevat een nadere definitie van het world-wide-web, namelijk alle verschijningsvormen daarvan waaronder geïndexeerde delen, niet-geïndexeerde delen, indexeerbare delen en niet-indexeerbare delen. De term ‘indexeerbaar’ verwijst naar de vindbaarheid van internetvindplaatsen via internetzoekmachines, zoals Google. Of een internetvindplaats vindbaar is, vindbaar gemaakt kan worden voor een zoekmachine/crawler (door opname daarvan in een zogenoemd robots.txt-bestand<sup>4</sup>) dan wel niet vindbaar gemaakt kan worden, is voor de definitie in artikel 1:23m irrelevant. Met andere woorden: volgens deze definitie mag het gehele world-wide-web (al dan niet geautomatiseerd) worden doorzocht. Het valt op dat de definitie niet is beperkt tot publiek toegankelijke delen van het world-wide-web, terwijl de rest van de bepaling en de MvT wel doen vermoeden dat een dergelijke beperking bedoeld is. Bovendien, als we een vergelijking trekken met het nieuwe WvSv, is opvallend dat ‘openbare toegankelijkheid’ wel een sleutelbegrip is in

<sup>2</sup> De Raad voor de rechtspraak heeft op grond van artikel 95 van de Wet op de rechterlijke organisatie een wettelijke adviestaak met betrekking tot nieuwe wets- en beleidsvoorstellen die gevolgen hebben voor de rechtspraak. De adviezen worden vastgesteld na overleg met de gerechten. De Raad voor de rechtspraak is een adviescollege in de zin van artikel 79 en 80 van de Grondwet. Bij het opstellen van zijn adviezen beoordeelt de Raad de voorgenomen wet- en regelgeving in het bijzonder op de gevolgen voor de organisatie en de werklast van de gerechten en op de (praktische) toepasbaarheid en uitvoerbaarheid. Rechteren zijn bij de behandeling van individuele zaken niet gebonden aan de inhoud van de wetgevingsadviezen van de Raad voor de rechtspraak.

<sup>3</sup> Zie voor een definitie bijvoorbeeld: [What is the World Wide Web \(WWW\)? | Definition from TechTarget.](#)

<sup>4</sup> Zie voor een beschrijving van de functie van het robots.txt-bestand in het crawling-proces van de Google zoekmachine: [Robots.txt Introduction and Guide | Google Search Central | Documentation | Google for Developers.](#)



## de Rechtspraak

Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 3 van 14

de toekomstige strafvorderlijke bevoegdheid tot het verrichten van openbronnenonderzoek (voor zover daardoor naar verwachting een meer dan beperkte inbreuk op de persoonlijke levenssfeer kan ontstaan) als bedoeld in artikel 2.8.8 Wetboek van Strafvordering (hierna: Sv) nieuw.<sup>5</sup>

Een website/webapplicatie is publiek toegankelijk indien de toegang daartoe niet is afgeschermd met een gebruikersnaam en wachtwoord (en/of 2FA of MFA) zodat voor het verwerken van de gegevens geen beveiliging hoeft te worden doorbroken. De definitie van artikel 1:23m lijkt zich er niet tegen te verzetten dat (al dan niet op geautomatiseerde wijze) gegevens uit afgeschermd websites/webapplicaties worden verwerkt. Met andere woorden: de reikwijdte van de geïntroduceerde controlebevoegdheden lijkt aanmerkelijk ruimer te zijn dan de reikwijdte van de nieuwe strafvorderlijke bevoegdheid tot openbronnenonderzoek. Zoals hierboven al gemeld, lijkt het onwaarschijnlijk dat dit de bedoeling is geweest. De Raad adviseert dit beter tot uitdrukking te brengen in de wettekst.

Indien de opsomming in artikel 1:23m lid 1 toch zo bedoeld is, adviseert de Raad om in de wettekst of de MvT aandacht te besteden aan de normering van het doorbreken van beveiligingen die voor het verkrijgen van toegang tot niet publiek toegankelijke website/webapplicaties nodig zal zijn. Er is dan immers sprake van het toekennen van een bevoegdheid die veel weg heeft van de ‘hackbevoegdheid’ zoals vastgelegd in de artikelen 126nba, 126uba en 126zpa Sv.

Een ander aspect waarover de Raad opmerkingen heeft, betreft de verhouding tussen de in de opsomming opgenomen onderdelen van het world-wide-web (artikel 1:23m lid 1 sub b t/m e). Een ‘peer-to-peer netwerk’ (ook wel: P2P-netwerk) (artikel 1:23m lid 1 sub b) betreft een netwerk van geautomatiseerde werken die elk fungeren als een node voor het delen van gegevensbestanden binnen de groep.<sup>6</sup> Het gebruik van een P2P-netwerk verloopt via een P2P-client, een softwareprogramma waarmee de gebruiker (kort gezegd) de verbindingen met andere nodes in het netwerk kan beheren door onder andere het instellen van een maximumbandbreedte voor downloaden en uploaden van gegevensbestanden. P2P-netwerken, zoals BitTorrent, vormen gedecentraliseerde netwerken waarin geautomatiseerde werken rechtstreeks via het internet met elkaar communiceren. De term ‘P2P-netwerk’ verwijst in zoverre naar een specifieke configuratie waarin geautomatiseerde werken op een efficiënte manier gegevensbestanden kunnen uitwisselen en die over het reguliere world-wide-web heen is gelaagd (een zgn. ‘overlay network’<sup>7</sup>). De term ‘Usenet’ (ook wel aangeduid als: nieuwsgroepen) verwijst naar een gedecentraliseerd netwerk waarin geautomatiseerde werken rechtstreeks tekstberichten of binaire gegevensbestanden uitwisselen en dat eveneens over het reguliere world-wide-web heen is

---

<sup>5</sup> Zie over het begrip ‘publiek toegankelijk’ m.n. *Kamerstukken II 2022/23*, 36327, nr. 3, p. 680 t/m 683 en p. 1420). Zie voor een meer uitvoerige beschouwing R.J.A. Klaar, [De strafvorderlijke normering van het geautomatiseerd overnemen van persoonsgegevens uit publiek toegankelijke bronnen met behulp van webcrawlers](#), *Tijdschrift Modernisering Sv* 2022, par. 2.1.

<sup>6</sup> Zie voor een definitie bijvoorbeeld: [What is peer-to-peer network \(P2P network\)? | Definition from TechTarget](#).

<sup>7</sup> Zie voor een definitie bijvoorbeeld: [What is an overlay network? \(techtarg.com\)](#): (...). An overlay network is any virtual layer on top of physical network infrastructure. (...). The overlay creates a new overlay where traffic can be programmatically directed through new virtual network routes or paths instead of requiring physical links.”



Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 4 van 14

gelaagd.<sup>8</sup> Het is daarom onjuist om ‘*overlay networks*’, zoals P2P-netwerken, het Usenet, maar bijvoorbeeld ook het Tor-netwerk, als van het world-wide-web afgescheiden fenomenen te beschouwen. P2P-netwerken en Usenet lijken als ‘*overlay networks*’ eerder tot het niet-indexeerbare (niet door internetzoekmachines vindbare/ontsloten) gedeelte van het world-wide-web te behoren. Nu het world-wide-web in artikel 1:23m lid 2 geacht wordt geïndexeerde (vindbare), niet-geïndexeerde (niet-vindbare) en niet-indexeerbare (niet vindbaar te maken) websites en webapplicaties (oftewel: het deep web en het dark web (MvT, p. 30) te omvatten, lijkt de noodzaak om P2P-netwerken en het Usenet als afzonderlijke internetbronnen te benoemen te ontbreken.

Daarnaast merkt de Raad op dat de (publieke toegankelijke gedeelten van) social media-platforms (artikel 1:23m lid 1 sub d) een verzameling webpagina’s en webapplicaties betreft die onderdeel zijn van het (geïndexeerde) world-wide-web. De noodzaak om sociale media als afzonderlijke internetbron te benoemen lijkt daarom ook hier te ontbreken. Voor zover het world-wide-web wordt geacht social media te omvatten, rijst bovendien de vraag in hoeverre de definitie van sociale media verenigbaar is met de definitie van het world-wide-web, nu het world-wide-web ook niet-vindbare en niet vindbaar te maken websites omvat. Met andere woorden: besloten chatgroepen en afgeschermdes social media-profielen mogen in dat geval ook worden doorzocht. Uit de MvT blijkt inderdaad dat twee controlebevoegdheden (artikel 1:23n lid 1 en artikel 1:23o lid 2) strekken tot onderzoek aan besloten chatgroepen.<sup>9</sup> Kortom: nu in artikel 1:23m lid 1 sub d onder i. t/m iii. publiek toegankelijke delen van social media worden genoemd, terwijl artikelen 1:23n lid 1 en 1:23o lid 2 strekken tot het doorzoeken van besloten gedeelten van social media, rijst de vraag of artikel 1:23m lid 1 sub d niet beter kan worden geschrapt.

Ten aanzien van artikel 1:23m lid 1 sub e, het ‘internet der dingen’ (oftewel: ‘Internet of Things’, afk.: IoT), merkt de Raad het volgende op. De definitie van ‘IoT’ is beperkt tot apparaten die niet beveiligd zijn met een gebruikersnaam/wachtwoord. Het al dan niet voorzien zijn van een beveiliging speelt daarentegen rol in de eerder besproken definitie van sociale media. De Raad merkt op dat hier sprake lijkt te zijn van inconsistentie. Daarnaast rijst de vraag of IoT-devices die slechts zijn voorzien van een standaard gebruikersnaam/wachtwoord (admin/admin) onder deze definitie vallen. Die vraag wordt niet beantwoord in de MvT. Nu de Europese Commissie bij [EU-Verordening 2022/30](#) minimumeisen aan de digitale veiligheid van IoT-devices heeft gesteld, waaronder dat de gebruiker wordt verplicht om voor ingebruikname van het digitale apparaten zelf een sterk wachtwoord in te stellen, valt te verwachten dat het aantal met het internet verbonden digitale apparaten dat slechts van een standaard gebruikersnaam/wachtwoord dan wel niet van enige beveiliging is voorzien verder zal afnemen.

Door het opnemen van deze dienst in de opsomming wordt voorzien in een mogelijkheid om digitale apparaten die met het internet zijn verbonden te onderzoeken, voor zover die apparaten niet zijn

---

<sup>8</sup> Zie voor een definitie bijvoorbeeld: [What is a newsgroup? – TechTarget Definition](#).

<sup>9</sup> Uit de MvT (p. 30) blijkt dat voor het lid worden van een besloten chatgroep toestemming door de r-c ex artikel 1:23n lid 1 is vereist. Voor het deelnemen aan een besloten groep in ‘een virtuele wereld, zoals Metaverse’ is toestemming door een daartoe door de Minister van Financiën aangewezen ambtenaar (die geen onderdeel is van het team dat het openbronnenonderzoek verricht) ex artikel 1:23o lid 2 vereist (zie MvT, p. 33).



# de Rechtspraak

Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 5 van 14

beveiligd met een gebruikersnaam en wachtwoord. De vraag rijst in hoeverre het afzonderlijk benoemen van IoT meerwaarde heeft. Bestaat het gehele internet immers niet uit met elkaar verbonden apparaten?<sup>10</sup> Het afzonderlijk benoemen van IoT houdt vermoedelijk verband met de mogelijkheid om met gebruikmaking van Automated Osint-tools, zoals Censys<sup>11</sup>, Shodan<sup>12</sup> of Maltego<sup>13</sup>, een beeld te verkrijgen van met het internet verbonden digitale apparaten op een bepaalde locatie, binnen een bepaalde IP-range of die aan bepaalde voorwaarden voldoen (zoals het gebruik van een standaard gebruikersnaam/wachtwoord: admin/admin)<sup>14</sup>. Met *Automated Osint-tools* is het (in elk geval) met betrekking tot niet beveiligde digitale apparaten evenwel ook mogelijk om daarvan gegevens (met name metadata) te verkrijgen. Het is bijvoorbeeld mogelijk om de geolocatie, de kenmerken van het besturingssysteem, en de tijd/periode dat een IP-adres actief is (uptime) te verkrijgen.<sup>15</sup> Daarnaast kennen *Automated Osint-tools* niet zelden een ‘poortscan-functie’, waarmee IoT-devices op kwetsbaarheden kunnen worden gescand.<sup>16</sup> Dergelijke gegevens worden niet zelden door opsporingsdiensten gebruikt om de mogelijkheden tot het binnendringen van een met het internet verbonden apparaat te onderzoeken. Onderdeel daarvan is het scannen op het gebruik van een standaard gebruikersnaam/wachtwoord (admin/admin). De Raad werpt de vraag op of het gebruik van dergelijke poortscan-functies onder het bereik van de controlebevoegdheid (artikel 1:23o) valt en adviseert dit punt nader te toelichten in de MvT.

## **Ten aanzien van artikel 1:23n**

### **De rechter-commissaris**

Het Wetsvoorstel geeft geen definitie van het begrip rechter-commissaris. De Raad gaat ervan uit dat bedoeld wordt op de rechter-commissaris in strafzaken. Deze rechter heeft immers in strafrechtelijke procedures soortgelijke taken/bevoegdheden (bescherming van het briefgeheim in de artikelen 101 en 114 Sv en 2.7.42 Sv nieuw). De uitoefening van toezichthoudende bevoegdheden met betrekking tot het opsporingsonderzoek door de rechter-commissaris vloeit voort uit artikel 170 Sv. De in dit Wetsvoorstel gecreëerde betrokkenheid van de rechter-commissaris bij de beoordeling van de rechtmatigheid van een *controlebevoegdheid* is een bijzondere. Volgens de MvT is er voor een voorafgaand bevel van de rechter-commissaris gekozen omdat de rechter-commissaris ook al een rol heeft bij een schending van

---

<sup>10</sup> Hetzelfde bezwaar geldt voor de aanduiding van een geautomatiseerd werk als “een groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch (...)gegevens verwerken” als bedoeld in artikel 80sexies Wetboek van Strafrecht (Sr). Deze omschrijving laat (de onwenselijke) ruimte bestaan om daaronder alle met het internet verbonden apparaten te begrijpen.

<sup>11</sup> Zie: [search.censys.io](https://search.censys.io).

<sup>12</sup> Zie: [Shodan Search Engine](https://shodan.io).

<sup>13</sup> Zie: <https://www.maltego.com>.

<sup>14</sup> In de concept-MvT (p. 29-30) staat ook dat er geen bevoegdheid wordt verleend aan de inspecteur tot het gebruik van het internet der dingen indien hij bij het desbetreffende apparaat moet inloggen met een persoonlijke gebruikersnaam en een persoonlijk wachtwoord.

<sup>15</sup> Zie voor een dergelijk overzicht van met de Automated Osint-tool Shodan verkrijgbare gegevens J. Matherly, “[The Complete Guide to Shodan](#)”, Appendix A: Banner Specification.

<sup>16</sup> Zie voor een lijst van de netwerkpoorten van met het internet verbonden digitale apparaten die door de Automated Osint-tool Shodan worden gescand bijvoorbeeld: [api.shodan.io/shodan/ports](https://api.shodan.io/shodan/ports).



Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 6 van 14

het briefgeheim als bedoeld in artikel 1:36 Adw. Hoewel de Raad de keuze begrijpt, ligt een nadere onderbouwing in de MvT van de noodzaak en wenselijkheid van de uitbreiding van de rol van de rechter-commissaris toch voor de hand. De MvT maakt bovendien niet duidelijk waarom ervoor is gekozen de taak om op verzoek een bevel te geven, exclusief te beleggen bij de rechter-commissaris in het arrondissement Rotterdam. De Raad adviseert – mede in het licht van het toetsingskader wettelijke concentratie<sup>17</sup> – ook die keuze nader toe te lichten in de MvT.

#### Bevel of machtiging

In het voorgestelde artikel 1:23n is bepaald dat de rechter-commissaris een bevel geeft. De Raad werpt de vraag op of op dit punt niet meer de systematiek van het strafprocesrecht zou moeten worden gevolgd waarin de rechter-commissaris bij de uitoefening van zijn toezichthoudende taak de officier van justitie *machtigt* tot het geven van een bevel. Daarmee zou ook worden aangesloten bij andere recente regelingen waarin de rechter-commissaris is betrokken bij het toezicht op de naleving. Zo kan de Autoriteit Consument en Markt (ACM) ter bescherming van consumenten na voorafgaande machtiging van de rechter-commissaris (belast met de behandeling van strafzaken) bij de rechtbank Rotterdam een last opleggen aan de beheerder van een internetdomein om consumenten te waarschuwen, de inhoud van een online interface te verwijderen of de inhoud ervan ontoegankelijk te maken of de toegang te beperken of een domeinnaam te schrappen. In het wetsvoorstel Uitvoeringswet Digitale Marktenverordening is de ACM belast met toezicht op de naleving van Verordening EU2022/1925 (de digitale markten-verordening). De met toezicht belaste ambtenaren van de ACM zijn onder andere bevoegd op grond van het bepaalde in artikel 12b Instellingswet Autoriteit Consument en Markt na een voorafgaande machtiging van de rechter-commissaris<sup>18</sup>, een woning zonder toestemming van de bewoner te betreden teneinde inzage te vorderen in bescheiden, daarvan kopieën te maken dan wel deze in beslag te nemen (artikel 12 b jo 12d lid 1 Instellingswet). Het verschil tussen een bevel en een machtiging is juridisch relevant, want het verstrekken van een bevel impliceert een verplichting van de ontvanger dat bevel op te volgen, terwijl een machtiging aan de ontvanger ruimte laat al dan niet een daarop gebaseerd bevel te doen uitgaan.

Artikel 1:36 Adw kent een – reeds langer bestaande – soortgelijke bepaling voor brieven. Ook in die bepaling dient de rechter-commissaris een bevel te geven. In de MvT staat bij de toelichting op dat artikel dat bij de invoer van goederen per brief onderzoek mogelijk is *zonder machtiging* van de rechter indien de afzender op de brief heeft aangegeven dat ambtelijke controle is toegestaan. In de overige gevallen biedt, aldus de MvT, artikel 1:36 uitkomst.<sup>19</sup> Hieruit zou kunnen worden afgeleid dat ondanks de redactie in artikel 1:36 Adw die ziet op het afgeven van een bevel, de wetgever mogelijk ook hier een machtiging voor ogen heeft gehad.

De Raad geeft tegen de achtergrond van het voorgaande in overweging om het Wetsvoorstel op dit punt te heroverwegen en zo nodig aan te passen dan wel de keuze voor een bevel in plaats van een

---

<sup>17</sup> [Toetsingskader wettelijke concentratie \(rechtspraak.nl\)](https://rechtspraak.nl)

<sup>18</sup> De rechter-commissaris belast met de behandeling van strafzaken bij de rechtbank Rotterdam

<sup>19</sup> *Kamerstukken II 2005/06, 30580, nr. 3, p. 111.*



Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 7 van 14

machtiging nader toe te lichten in de MvT.

### Beroep

De Raad merkt op dat het Wetsvoorstel anders dan de eerder genoemde regelingen waarbij de rechter-commissaris in strafzaken bij toezicht en handhaving buiten het strafrecht wordt betrokken (de Wet Handhaving Consumentenbescherming en het wetsvoorstel Uitvoeringswet Digitale Marktenverordening) niet voorziet in de mogelijkheid beroep in te stellen (bij de rechtbank Rotterdam) indien de rechter-commissaris het verzoek afwijst. De Raad adviseert om het Wetsvoorstel op dit punt aan te vullen.

### Het doorzoeken van besloten gedeelten van sociale media

Ten aanzien van de controlebevoegdheid vastgelegd in het voorgestelde artikel 1:23n merkt de Raad op dat relevant is welke delen van sociale media als ‘besloten’ gelden. De MvT bevat hiervoor weinig aanknopingspunten. In strafrechtelijke zin kan dezelfde afbakeningsvraag onder meer aan de orde zijn in het kader van de beoordeling of opruiende uitlatingen in een besloten chatgroep/besloten forum ‘in het openbaar’ zijn gedaan. In dat verband is met name de toegankelijkheid van de groep/het forum voor willekeurige derden relevant, die onder meer wordt bepaald door het (verloop van) het aantal leden van een besloten chatgroep/besloten forum en de vraag of en zo ja welke voorwaarden gelden voor lidmaatschap/deelname.<sup>20</sup> Nu de inschatting of het te controleren deel van sociale media een openbaar/publiek toegankelijk dan wel besloten karakter heeft primair aan de inspecteur is en die inschatting bepalend is voor het al dan niet doen van een verzoek aan de rechter-commissaris, worden gezichtspunten voor deze beoordeling in de MvT gemist. De Raad adviseert de MvT op dit punt uit te breiden.

Daarnaast merkt de Raad op dat het gebruik van het woord ‘doorzoeken’ in het voorgestelde artikel 1:23n lijkt te impliceren dat gegevens niet mogen worden overgenomen. Ter vergelijking: in het huidige Wetboek van Strafvordering en in het wetsvoorstel voor het nieuwe Wetboek van Strafvordering worden in diverse strafvorderlijke bepalingen juist expliciet termen als ‘opnemen’ (in relatie tot stromende gegevens) en ‘overnemen’ en ‘vastleggen’ (in relatie tot opgeslagen gegevens) gebruikt om te bepalen dat niet alleen het raadplegen/kennisnemen van gegevens, maar ook het kopiëren daarvan is geoorloofd.<sup>21</sup> In de MvT in de slotalinea bij artikel 1:23n wordt opgemerkt dat het maken van een integrale kopie (dus het overnemen van gegevens) om deze op een later tijdstip te analyseren tot 3 dagen nadat de rechter-commissaris toestemming heeft verleend, is toegestaan.<sup>22</sup> Dat lijkt op gespannen voet te staan met de term ‘doorzoeken’. De Raad adviseert het Wetsvoorstel op dit punt te verduidelijken. Ook adviseert de Raad om daarbij mee te nemen wat er na analyse zal gebeuren met

---

<sup>20</sup> Zie m.n. hof Den Haag, 13 november 2023, [ECLI:NL:GHDHA:2023:2207](#).

<sup>21</sup> Zie voor “opnemen” bijvoorbeeld de IP-tap/telefoontap (artt. 126m/126t/126zg Sv). Zie voor ‘overnemen’ bijvoorbeeld artikel 2.8.8. Sv nieuw (stelselmatig openbronnenonderzoek, onderdeel van de modernisering van het Wetboek van Strafvordering, *Kamerstukken II 2022/23*, 36327, nr. 3, p. 679 e.v.). Zie voor ‘vastleggen’ bijvoorbeeld artikel 556 Sv (kennisname van gegevens na inbeslagneming).

<sup>22</sup> MvT, p. 31.



# de Rechtspraak

Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 8 van 14

gegevens die softwarematig zijn verzameld, maar die niet duiden op goederen als bedoeld in artikel 1:23n lid 3.

In het verlengde van het voorgaande valt op dat voor het *gebruik* van verzamelde gegevens (individueel en als verzameling) geen rechterlijke toets plaatsvindt. Het is de vraag welke algoritmes op die verzamelde gegevens kunnen worden toegepast en met welke gevolgen. De collectieve verzameling, van een groepering van individuele gegevens, kan ook een voorwerp zijn waar een algoritme op kan worden toegepast. De Raad mist een toetsing – anders dan het doel waarvoor het bevel wordt gegeven – van het latere gebruik van de verzamelde persoonsgegevens. De Raad adviseert het Wetsvoorstel op dit punt uit te breiden.

### Toetsingskader en proportionaliteit en subsidiariteit

In het voorgestelde artikel 1:23n lid 2 is volgens de MvT een omvangrijk kader vastgelegd waaraan de rechter-commissaris een verzoek van de inspecteur moet toetsen.<sup>23</sup> In het verzoek van de inspecteur moeten de noodzaak, proportionaliteit, subsidiariteit en gerichtheid van de onderzoekshandelingen worden toegelicht (artikel 1:23n lid 2 sub a t/m d). Deze eisen lijken elkaar te overlappen, in elk geval door de wijze waarop ze in de MvT nader worden geduid. De MvT bepaalt met betrekking tot noodzaak onder meer dat de inspecteur moet aangeven waarom andere controlebevoegdheden niet toereikend zijn<sup>24</sup>, terwijl met betrekking tot subsidiariteit wordt bepaald dat de inspecteur moet aangeven waarom niet kan worden volstaan met de inzet van een bevoegdheid die een lichtere inbreuk op de privacy van de betrokkene(n) inhoudt. Het aspect ‘gerichtheid’ lijkt een deelaspect van ‘proportionaliteit’ te betreffen. De MvT definieert ‘gerichtheid’ als (kort gezegd) het vermijden dan wel tot een onvermijdbaar minimum beperken van de inbreuk op de privacy van personen op wie de controle niet gericht is. Onder ‘proportionaliteit’ wordt (kort gezegd) de verhouding tussen de impact van de beoogde inzet en de inbreuk op de privacy van de betrokkene(n) verstaan.<sup>25</sup> Kortom, van de inspecteur wordt naar de kern gezien een onderbouwing van de proportionaliteit/subsidiariteit van de voorgenomen inzet verwacht. Van de rechter-commissaris wordt op basis van het verzoek van de inspecteur een beoordeling daarvan verwacht. Het lijkt daarom logischer om alleen die twee eisen op te nemen, danwel de nu voorgestelde vier eisen beter af te bakenen in de MvT.

### Geheimhouders

In de systematiek van het Wetboek van Strafvordering ligt sterk besloten dat het van groot maatschappelijk belang is dat een ieder zich tot een geheimhouder moet kunnen wenden zonder de vrees te hebben dat met die geheimhouder uitgewisselde informatie ter kennis komt van vervolgende autoriteiten. De geheimhouders waarvoor dat geldt betreft een beperkte groep, aangeduid in de artikelen 218 en 218a Sv. Het daaraan gekoppelde verschoningsrecht is niet absoluut; daarop kan in bepaalde gevallen inbreuk worden gemaakt. De Raad merkt op dat het Wetsvoorstel niet voorziet in een voorziening voor communicatie met geheimhouders en adviseert om daaraan aandacht te besteden.

---

<sup>23</sup> MvT, p. 30-31.

<sup>24</sup> MvT, p. 31

<sup>25</sup> MvT, p. 31.

datum 19 december 2024  
pagina 9 van 14

### **Artikel 1:23o**

Deze bepaling betreft de algemene controlebevoegdheid om (al dan niet anoniem/heimelijk) op geautomatiseerde wijze het internet te doorzoeken. In artikel 1:23o lid 1 is opgenomen dat daartoe onder meer zoekmachines kunnen worden ingezet die ‘de cache’ doorzoeken. Uit de MvT volgt dat met ‘cache’ wordt bedoeld op de ‘browser cache’ of ‘web cache’ van hostingdiensten dan wel de internetprovider waarvan de betreffende hostingdienst klant is.<sup>26</sup> De Raad gaat er van uit dat de term ‘cache’ in deze bepaling kan verwijzen naar ‘*content delivery network caching*’. Dit betreft een netwerk van een geografisch verspreide groep servers, die ertoe dienen om de inhoud van websites/webapplicaties zo dicht mogelijk bij de eindgebruikers tijdelijk op te slaan (te ‘*cachen*’).<sup>27</sup> Het gaat dan niet om de browser cache die lokaal op een digitaal apparaat van een internetgebruiker wordt opgeslagen. Het verkrijgen van toegang tot en het overnemen van gegevens in de browser cache die zich op een digitaal apparaat van de gebruiker bevindt, zou immers de inzet van strafvorderlijke bevoegdheden impliceren, namelijk de (heimelijke) netwerkzoeking of de hackbevoegdheid (binnendringen in het digitale apparaat van de gebruiker). Dit Wetsvoorstel lijkt niet te voorzien in controlebevoegdheden die dergelijke, vanuit de privacy van de gebruiker beschouwd (zeer) ingrijpende onderzoekshandelingen legitimeren. De Raad adviseert dit uitdrukkelijk in de MvT op te nemen en toe te lichten om eventuele verwarring daarover te voorkomen.

De controlebevoegdheid omvat zowel het gebruik van ‘standaard’ internetzoekmachines, zoals Google of Wolfram Alpha, maar ook Automated Osint-tools (zoals: Maltego en Meltwater<sup>28</sup>) die geschikt zijn voor het uitvoeren van risicoanalyses. De Raad realiseert zich dat de reikwijdte van deze controlebevoegdheid aanzienlijk is. Het omvat zowel het alledaagse gebruik van Google als het gebruik van Automated Osint-tools waarmee verrijking van gegevens (het combineren van gegevens met de bedoeling om daaruit nieuwe verbanden/inzichten tussen die gegevens te verkrijgen) kan plaatsvinden. Uit de MvT (slotzin) bij artikel 1:23p lid 1 volgt dat artikel 1:23o lid 1 slechts legitimeert tot een eenmalige zoekactie.<sup>29</sup>

Artikel 1:23l bepaalt dat de verzamelde gegevens binnen het toegestane doel alleen mogen worden gebruikt voor identificatie van personen voor zover dat in het kader van een redelijke taakuitoefening door de inspecteur of voor de persoonlijke veiligheid van de betrokken ambtenaar of zijn directe omgeving noodzakelijk is.

De MvT bij artikel 1:23o lid 1 bepaalt dat elke uitoefening van deze controlebevoegdheid een welomschreven taakopdracht vereist die (kort gezegd) een onderbouwing bevat van de

---

<sup>26</sup> MvT bij artikel 1:23o lid 1 (p. 31): “de cache kan zich zowel bij de provider bevinden als bij de betreffende website die de cliënt is bij die provider.” De formulering “website die cliënt is bij de provider” is merkwaardig, nu het hosten van een website per definitie het gebruik van een hostingdienst (en internet) meebrengt.

<sup>27</sup> Zie voor een definitie bijvoorbeeld: [What is a content delivery network \(CDN\)? | How do CDNs work? | Cloudflare.](#)

<sup>28</sup> Zie: [Meltwater: Media, Social & Consumer Intelligence.](#)

<sup>29</sup> MvT bij artikel 1:23p lid 1 (p. 34): “Opgemerkt wordt dat een eenmalige zoekactie valt onder artikel 1:23o.”



## de Rechtspraak

Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 10 van 14

proportionaliteit/subsidiariteit van de beoogde inzet.<sup>30</sup> Volgens de Raad is opvallend dat artikel 1:23o niet bepaalt dat de proportionaliteit/subsidiariteit door een hogere autoriteit, zoals de rechter-commissaris, wordt getoetst (in tegenstelling tot het voorgestelde artikel 1:23n). Met andere woorden: de kwaliteit van de verslaglegging door de inspecteur wordt op geen enkele wijze getoetst. De Raad acht dit onwenselijk, nu ook de door de (eenmalige) inzet van een webcrawler te verwachten mate van inbreuk op de persoonlijke levenssfeer van de betrokkene(n) per inzet aanzienlijk kan variëren. De Raad adviseert het Wetsvoorstel en de MvT op dit punt te heroverwegen.

Verder merkt de Raad op dat het vanuit systematisch oogpunt logischer zou zijn geweest om artikel 1:23o lid 2 onder te brengen in artikel 1:23n, omdat het in beide gevallen gaat om het verkrijgen van toegang tot besloten gedeelten van sociale media. Het is de Raad niet duidelijk waarom in het geval van artikel 1:23o lid 2 is gekozen voor verplichte toestemming door de Minister van Financiën, terwijl in het geval van artikel 1:23n een bevel van een rechter-commissaris nodig is.

De Raad werpt ten aanzien van artikel 1:23o lid 1 de vraag op in hoeverre toestemming van een hogere autoriteit noodzakelijk is voor het gebruik van een alias/pseudoniem (zolang dat gebruik beperkt blijft tot het verzamelen van gegevens, en zich niet uitstrekt tot bijvoorbeeld contact leggen met een voor het onderzoek relevante persoon). Ter vergelijking: in het kader van het strafprocesrecht wordt algemeen aanvaard dat het onder een pseudoniem aanmaken van een onderzoeksprofiel door een verbalisant kan worden gebaseerd op de algemene taakstellende bevoegdheid ex artikel 3 Politiewet 2012.<sup>31</sup> Los daarvan kan de vraag gesteld worden of een door de Minister van Financiën aangewezen ambtenaar als een (voldoende) onafhankelijke autoriteit kan worden beschouwd.

Tot slot onderschrijft de Raad artikel 1:23o lid 3 en de toelichting in de MvT op dit artikel, waarin staat dat de inspecteur geen individuele ‘internetvriendschappen’ mag aangaan en dat hij vriendschapsverzoeken/contactverzoeken van derden moet negeren of weigeren, of indien het contact eenzijdig tot stand is gebracht dat contact moet ‘ontvrienden’. In strafvorderlijke zin markeert het aangaan van online contact met een verdachte of andere betrokkene in het strafrechtelijk onderzoek de grens tussen online observatie en stelselmatige inwinning van informatie/digitale infiltratie en daartoe gebruikte steunbevoegdheden (zoals pseudokoop/pseudo-dienstverlening). De Raad merkt op dat het vanuit systematisch oogpunt echter logischer zou zijn geweest om ook dit deel van deze bepaling onder te brengen in artikel 1:23n, nu daarin ook voorwaarden aan het verkrijgen van toegang tot besloten gedeelten van sociale media worden gesteld.

---

<sup>30</sup> MvT bij artikel 1:230 lid 1 (p. 32): “Het doorzoeken van het internet geschiedt op een methodische wijze, dat wil zeggen dat voor elke doorzoeking die de inspecteur verricht, dit gebeurt op basis van een welomschreven taakopdracht die is gebaseerd op een handhavingsplan. Daarbij wordt een afweging gemaakt naar de proportionaliteit van de inbreuk van het internetonderzoek op de persoonlijke levenssfeer in relatie tot de noodzaak van het onderzoek.”

<sup>31</sup> Vgl. W. Landman & S. Groothuis, “Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie.”, *Politie & Wetenschap* 2022, p. 32: “(...) het gebruik van een onderzoeksprofiel wil niet direct zeggen dat er een bijzondere opsporingsbevoegdheid nodig is.”



Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 11 van 14

### **Artikel 1:23p**

Deze controlebevoegdheid strekt (kort gezegd) tot de inzet van webcrawlers en tot het ten behoeve van de toezichtstaak opbouwen van een profiel van een individuele internetgebruiker. In het bijzonder de laatstgenoemde vorm van controle/toezicht kan (potentieel) een forse inbreuk op de persoonlijke levenssfeer van de betrokkene opleveren.

Artikel 1:23p lid 1 bepaalt dat de inspecteur (kort gezegd) gebruik kan maken van webcrawlers om doorlopend (dus geen ‘eenmalige zoekactie’) persoonsgegevens van personen die goederen als bedoeld in artikel 1:23n lid 3 voorhanden hebben dan wel aanbieders of afnemers van de voormelde goederen, over te nemen. De formulering “bestanden te gebruiken of te plaatsen op het internet” in artikel 1:23p lid 1 is wat de Raad betreft ongelukkig gekozen. De formulering kan beter worden vervangen door: “op het internet bestanden te gebruiken of te plaatsen”. Daarmee komt duidelijker tot uitdrukking dat het in artikel 1:23p lid 1 gaat om het gebruik van bestaande webcrawlers (zoals de Google zoekmachine) dan wel door de douane aangepaste (instellingen van) bestaande webcrawlers dan wel zelf ontworpen webcrawlers.

Verder heeft de Raad geconstateerd dat de uitoefening van deze controlebevoegdheid niet afhankelijk wordt gesteld van toestemming door een hogere autoriteit. De Raad acht dit onwenselijk nu de door een doorlopende inzet van een webcrawler te verwachten mate van inbreuk op de persoonlijke levenssfeer van de betrokkene(n) per inzet aanzienlijk kan variëren. Daarbij verdient opmerking dat de op voorhand te beoordelen mate van inbreuk op de persoonlijke levenssfeer die door het geautomatiseerd overnemen van gegevens zal ontstaan, afhankelijk is van de wijze waarop de crawler URL’s/hyperlinks verzamelt (het crawling-proces), de wijze waarop gegevens van de betreffende internetbronnen worden overgenomen (gescraped) en de wijze waarop die gegevens vervolgens voor risicoanalyse-doeleinden worden verwerkt (het onderzoek van de overgenomen gegevens). De Raad merkt op dat artikel 1:23p lid 1 de inspecteur niet stimuleert om op voorhand de hiervoor genoemde complexe inschatting van de te verwachten privacyinbreuk te maken. Ondanks dat het om een controlebevoegdheid gaat en niet om een strafvorderlijke bevoegdheid, ziet de Raad geen rechtvaardiging voor het stellen van lichtere eisen aan (de verantwoording van) de inschatting van de te verwachten privacyinbreuk.<sup>32</sup>

Voorts geeft de Raad in overweging om bij het ontwerp van de AMvB zoals genoemd in artikel 1:23t acht te slaan op de ervaringen en ontwikkelingen in verband met de (concept-)AMvB inzake de inzet van webcrawlers in het kader van de strafvorderlijke bevoegdheid tot (geautomatiseerd) stelselmatig openbronnenonderzoek als bedoeld in artikel 2.8.8 Sv nieuw.<sup>33</sup>

---

<sup>32</sup> De MvT bij het toekomstige artikel 2.8.8 Sv (stelselmatig openbronnenonderzoek) bevat een tamelijk uitvoerige catalogus van gezichtspunten die opsporingsdiensten bij de op voorhand te maken inschatting van de privacyinbreuk die door inzet van webcrawlers en andere tools voor het geautomatiseerd overnemen van gegevens uit internetbronnen dienen te betrekken, om te bepalen of een bevel van de officier van justitie nodig is (*Kamerstukken II 2022/23*, 36327, nr. 3, p. 684 t/m 686, 1420).

<sup>33</sup> Zie artikel 2.8.8 lid 3 Sv nieuw: “Bij of krachtens AMvB worden regels gesteld over de geautomatiseerde wijze van overnemen van gegevens” (*Kamerstukken II 2022/23*, 36327, nr. 2, p. 108). Voor zover bekend verkeert deze uitvoeringsregelgeving thans (nog steeds) in de conceptfase.

datum 19 december 2024  
pagina 12 van 14

Daarnaast heeft de Raad een opmerking bij artikel 1:23p lid 2. Dit betreft de controlebevoegdheid om in het kader van de uitoefening van andere controlebevoegdheden (artikelen 1:23i of 1:23j) ‘*analytics codes*’ van een specifieke website/domein te onderzoeken.<sup>34</sup> De term ‘codes’ is kennelijk gebruikt in de betekenis van ‘software’ (zoals: Google Analytics) waarmee van gebruikers van websites/webapplicaties afkomstige (persoons)gegevens kunnen worden geanalyseerd. De term ‘code’ heeft als zodanig evenwel een veel bredere betekenis.<sup>35</sup> Vanuit het oogpunt van rechtszekerheid zou het beter zijn om de beperking van de term ‘code’ tot ‘software’ niet in de MvT, maar in de wettekst zelf op te nemen.

Verder merkt de Raad op dat de strekking van artikel 1:23p lid 3 niet helder uit de wettekst blijkt. Artikel 1:23p lid 3 bevat een (potentieel) vergaande controlebevoegdheid die strekt tot het opbouwen van een profiel van een internetgebruiker (kort gezegd: *online profilering*). Feitelijk betreft *online profilering* een vergaande vorm van online observatie van een persoon. Blijkens de MvT wordt gebruik gemaakt van door sociale media-platforms ontwikkelde ‘algoritmen’ die het browsegedrag van de gebruiker (o.a. zoekopdrachten, ‘gelikete’ posts, gevolgde accounts, bezochte webpagina’s en duur van websitebezoek) registreren. De inspecteur mag op grond van deze controlebevoegdheid de opbouw van het interesseprofiel zodanig beïnvloeden dat dit behulpzaam wordt bij het uitoefenen van de controlebevoegdheid.<sup>36</sup> Artikel 1:23p lid 3 houdt onder meer in: “op sociale media het algoritme dat die media toepast, een gedetailleerd profiel met interesses op te bouwen.” Deze passage is niet alleen taalkundig gebrekkig, maar de strekking ervan stemt niet overeen met de in de MvT gegeven omschrijving van deze controlebevoegdheid. De Raad vermoedt dat de term ‘algoritme’ in dit verband niet adequaat is gekozen, en dat wordt bedoeld op het gebruik van ‘*tracking cookies*’.<sup>37</sup> Kenmerkend voor tracking cookies is dat het browsegedrag van een internetgebruiker vaak over meerdere websites heen wordt gevolgd. De Raad adviseert om het Wetsvoorstel op dit punt aan te passen en de MvT te verduidelijken.

Ten aanzien van artikel 1:23p lid 4 merkt de Raad het volgende op. Het artikel bepaalt (kort gezegd) dat de inspecteur geen tracking cookies op digitale apparaten van derden mag plaatsen. In de MvT wordt opgemerkt dat internettoezicht niet kan strekken tot onderzoekshandelingen die in het kader van de strafvorderlijke netwerkzoeking en de wettelijke hackbevoegdheid alleen onder strikte voorwaarden kunnen worden verricht.<sup>38</sup> Artikel 1:23p lid 3 bepaalt uitdrukkelijk dat persoonsgegevens niet met oog op identificatie van natuurlijke personen mogen worden verwerkt. In de MvT wordt een (ogenschijnlijk vanzelfsprekend) verband gelegd tussen door ‘*tracking cookies*’ verkregen persoonsgegevens en (kort

---

<sup>34</sup> MvT, p. 34

<sup>35</sup> Zie voor de verschillende mogelijke definities van het Engelse woord ‘code’ bijvoorbeeld: <https://www.techtarget.com/whatis/definition/code>.

<sup>36</sup> MvT, 35: “De inspecteur kan gebruik maken van genoemd algoritme door dit te voeden zodat daarmee een profiel gaat ontstaan dat behulpzaam is bij het uitvoeren van de toezichtstaak (...).”

<sup>37</sup> Zie voor een definitie bijvoorbeeld: [Tracking cookies | Autoriteit Persoonsgegevens](#), en voor de privacyrechtelijke aspecten daarvan: [De Autoriteit Persoonsgegevens maakt een einde aan cookiewalls | Considerati](#).

<sup>38</sup> MvT, p. 36



Raad voor de  
rechtspraak

datum 19 december 2024  
pagina 13 van 14

gezegd) het op efficiënte wijze zicht krijgen op activiteiten met betrekking tot goederen als bedoeld in artikel 1:23n lid 3. Nu persoonsgegevens primair dienen ter identificatie van personen, valt wat de Raad betreft niet zonder meer in te zien dat en op welke wijze persoonsgegevens dienstig zouden kunnen zijn voor lokaliseren van activiteiten met betrekking tot goederen als bedoeld in artikel 1:23n lid 3. Met andere woorden: waarom is het noodzakelijk persoonsgegevens van individuen te verzamelen en te verwerken om zicht te krijgen op goederenstromen? Deze vraag dringt zich temeer op nu de ‘persoon die betrokken is bij het goederenvervoer’ weliswaar relevant is voor de risicoanalyse, maar de meeste factoren verband houden met goederen(bewegingen).<sup>39</sup> De Raad adviseert de MvT op dit punt uit te breiden. Ook hier is opvallend dat de uitoefening van deze controlebevoegdheid niet afhankelijk wordt gesteld van toestemming door een hogere autoriteit. Dat is onwenselijk, omdat door profilering van een internetgebruiker al snel een tamelijk volledig beeld van de (activiteiten van die) gebruiker kan ontstaan. Kenmerkend voor profilering is immers dat het surfgedrag van een internetgebruiker doorgaans gedurende een langere periode wordt geregistreerd. De Raad werpt de vraag op of gelet op het (potentieel zeer) ingrijpende karakter van profilering de voorgenomen profilering van een internetgebruiker niet standaard ter toetsing aan een rechter-commissaris (of andere onafhankelijke autoriteit) zou moeten worden voorgelegd.

### **WERKLAST**

De Raad voorziet geen substantiële gevolgen voor de werklast van de Rechtspraak ingevolge het huidige wetsvoorstel. Van uw Ministerie kreeg de Raad informatie dat in een relatief beperkt aantal zaken jaarlijks gebruik zal worden gemaakt van de bevoegdheid ex artikel 1:23n van het wetsvoorstel. De rechter-commissaris behandelt de vordering en neemt gemotiveerd schriftelijk een beslissing, rekening houdend met noodzaak, proportionaliteit, subsidiariteit en gerichtheid van de onderzoekshandelingen in de concrete zaak. De tijd die daarmee is gemoeid is sterk afhankelijk van hoe het verzoek, mede gelet op het uitvoerige toetsingskader, is aangeleverd en is onderbouwd. Het leidt op basis van de huidige tekst van het wetsvoorstel tot de conclusie dat de werklast van de Rechtspraak stijgt, maar niet substantieel, waarbij zij opgemerkt dat ten aanzien van andere controlebevoegdheden de Raad ook een toets door de rechter-commissaris adviseert. Mocht dit advies worden opgevolgd dan levert dit een extra werklastverzwaring op. De Raad wordt dan graag in de gelegenheid gesteld de werklastgevolgen opnieuw te bezien.

### **CONCLUSIE**

De Raad onderkent het belang van de wettelijke normering van controlebevoegdheden die een inbreuk maken op (het recht op) de persoonlijke levenssfeer. De Raad meent echter dat het Wetsvoorstel hierin nog niet ver genoeg gaat. Verder wijst de Raad op een aantal technische punten. De Raad geeft u in overweging om het Wetsvoorstel op de in dit advies genoemde onderdelen te verduidelijken of aan te passen.

---

<sup>39</sup> Zie MvT, p. 5: “(...) het soort goederen die worden vervoerd, de wijze van vervoer, de locatie van de goederen, de herkomst van de goederen, de bestemming van de goederen.”

datum 19 december 2024  
pagina 14 van 14

**TOT SLOT**

Indien na het uitbrengen van dit advies het Wetsvoorstel op belangrijke onderdelen wordt gewijzigd of indien uit nadere uitvoeringsregelgeving belangrijke werklastgevolgen voortvloeien, dan wordt de Raad graag in de gelegenheid gesteld daarover aanvullend te adviseren. Met het oog op de voorbereiding van de gerechten op de invoering van het Wetsvoorstel, stelt de Raad er prijs op als hij geïnformeerd wordt over de indiening van het Wetsvoorstel bij de Tweede en de Eerste Kamer en de plaatsing van de definitieve wetstekst in het *Staatsblad*. Ook eventuele nadere regelgeving volgend op dit Wetsvoorstel met gevolgen voor de rechtspleging valt binnen het adviesrecht van de Raad. Voor zover van toepassing, ontvangt de Raad graag een adviesaanvraag voor deze nadere regelgeving.

Hoogachtend,



Peter Pulles  
Lid Raad voor de rechtspraak