Internetcensuur

Groothuis, M.M.; Visser E., Weij M.

5 Internetcensuur

M.M. Groothuis[162]

5.1 Inleiding

Ingevolge artikel 7 Grondwet heeft niemand vooraf verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet. Wanneer 'drukpers' ruim wordt geïnterpreteerd, in de zin dat daaronder ook het internet wordt verstaan, zou men kortweg kunnen concluderen dat internetcensuur in strijd is met deze grondwetsbepaling en dus niet is toegestaan.
Toch is er de afgelopen jaren gedebatteerd over de wenselijkheid en mogelijkheden van een vorm van censuur op Internet in het belang van de staatsveiligheid, meer in het bijzonder het beschermen van de samenleving tegen de dreiging van terrorisme. Het debat begon na de aankondiging van het Tweede Kamerlid Wilders van zijn film *Fitna*.[163] In reactie hierop pleitte Minister van Staat Van den Broek er in maart 2008 voor dat de Nederlandse regering een kort geding zou aanspannen tegen het Tweede Kamerlid, om, met het oog op de staatsveiligheid, de rechter (vooraf) te laten bepalen of uitzending van de film verantwoord was.[164] De discussie naar aanleiding van deze gebeurtenissen spitste zich toe op de vraag of er, ondanks het in artikel 7 Grondwet geformuleerde censuurverbod, niet toch onder bijzondere omstandigheden ruimte is, of zou moeten komen, voor een vorm van censuur op internet.

In dit hoofdstuk worden de juridische mogelijkheden en grenzen van internetcensuur onderzocht. Onder internetcensuur wordt daarbij verstaan: een vorm van toezicht van overheidswege op de inhoud van een uiting op Internet alvorens deze uiting digitaal wordt gepubliceerd. In de paragrafen 5.2 en 5.3 staat de vraag centraal of, en zo ja onder welke voorwaarden internetcensuur mogelijk is onder

162 De auteur dankt L.E. Visser, student-stagiaire bij SOLV Advocaten, voor haar bijdrage aan het literatuuronderzoek voor deze publicatie.

163 Deze film kan worden gedownload op: http://www.liveleak.com/view?i=216_1207467783.

164 Interview met minister van Staat Hans van den Broek 24 maart 2008 in het televisieprogramma 'Het Gesprek', te downloaden op www.hetgesprek.nl. Zie over dit interview ook: NRC Handelsblad, 'Provider wil anti-koran film vooraf zien', 25 maart 2008, te downloaden op www.nrc.nl.

de Nederlandse Grondwet en het Europees Verdrag voor de Rechten van de Mens (EVRM).[165] Vervolgens worden in paragraaf 5.4 enkele praktische aspecten van internetcensuur en 'informele internetcensuur' belicht. In paragraaf 5.5 ten slotte worden conclusies geformuleerd over de mogelijkheden en grenzen van internetcensuur op Nederlands- en Europeesrechterlijk niveau.

5.2 Internetcensuur en de Nederlandse Grondwet

In een debat over de mogelijkheden en grenzen van internetcensuur rijst in de eerste plaats de vraag hoe de term 'drukpers' in het eerste lid van artikel 7 Grondwet moet worden uitgelegd in een digitale omgeving. Valt onder 'drukpers' ook het Internet? Medio jaren negentig, toen het gebruik van Internet en het Web in opkomst was, was er onder Internetgebruikers en juristen discussie over deze vraag.[166] Thans, ruim tien jaar later, is er geen twijfel meer over de vraag òf de vrijheid van meningsuiting van toepassing is op Internet: die vraag wordt zonder meer bevestigend beantwoord.[167] Het juridische debat spitst zich nu toe op de vraag hoe de verschillende leden van artikel 7 Grondwet moeten worden geïnterpreteerd wanneer zij worden toegepast in een digitale omgeving, alsmede op de

165 Naast de Grondwet en het EVRM is in dit kader ook het Internationaal Verdrag inzake Burgerlijke en Politieke Rechten (IVBPR) van belang. In artikel 19, tweede lid, van dit verdrag is bepaald dat een ieder het recht heeft op vrijheid van meningsuiting. De inhoud van dit artikel overlapt inhoudelijk grotendeels het – hierna te bespreken – artikel 10 EVRM. Door het ontbreken van een internationaal hof dat bindende uitspraken kan doen speelt art. 19 IVBPR in de praktijk een kleine rol. Zie in deze zin ook: J.A. Peters en I.J. de Vré, *Vrijheid van meningsuiting. De betekenis van een grondrecht in tijden van spanning,* Preadvies voor de Vereniging voor de Vergelijkende Studie van het Recht van Nederland en België, Kluwer: Deventer 2005, p. 9. Om deze reden zal deze verdragsbepaling in deze bijdrage verder buiten beschouwing blijven.

166 Zie in dit verband de regeringsnota *Wetgeving voor de elektronische snelweg (*1998), Kamerstukken II, 1997/1998, 25 880, nrs. 1-2.

167 Zie (o.m.) HR 25 november 2005, LJN AU4019 (anonieme uiting op Internet), *Mediaforum* 2006, nr. 1, *m.nt.* A.H. Ekker; Gerechtshof Amsterdam 17 november 2006, LJN AZ3011 (discriminerende uitingen op Internet); Rechtbank 's-Hertogenbosch 21 december 2004, LJN AR7891 (ontkennen van de Holocaust op internet).

vraag of aanvullende – specifiek op de *online* omgeving gerichte – normen nodig zijn.[168]

Een kernpunt in dit verband is de vraag hoe het in artikel 7, eerste lid, neergelegde censuurverbod moet worden geïnterpreteerd: staat deze bepaling in de weg aan elke vorm van internetcensuur of is er onder bijzondere omstandigheden toch ruimte voor het tevoren verbieden van een publicatie of vertoning op Internet?

Artikel 7, eerste lid, Grondwet verbiedt censuur van overheidswege expliciet.[169] Censuur is per definitie preventief. Toezicht op de inhoud van een uiting vormt de harde kern van het censuurverbod.[170] Krachtens artikel 7, eerste lid, Grondwet, kan de formele wetgever wel grenzen stellen aan de inhoud van uitingen (dit volgt uit de woorden 'behoudens ieders verantwoordelijkheid volgens de wet'), maar die grenzen kunnen uitsluitend achteraf – dus nadat de uiting is gedaan – worden gesteld. Zodanige grenzen achteraf zijn te vinden in het Wetboek van Strafrecht, waarin onder meer smaad, belediging, opruiing, en aanzet tot haat en discriminatie strafbaar zijn gesteld.[171] Aangenomen moet worden dat het censuurverbod bij uitingen op Internet op dezelfde wijze geldt als bij uitingen in een niet-digitale omgeving.

Betekent dit dat er geen enkele mogelijkheid voor de overheid is om vooraf een publicatie van een tekst of film op Internet te verbieden? In dit verband is ook artikel 103 van de Grondwet van belang. Volgens dit artikel bepaalt de wet in welke gevallen ter handhaving van de uit- of inwendige veiligheid bij koninklijk besluit een door de wet als zodanig aan te wijzen *noodtoestand* kan worden afgekondigd (eerste lid). Daarbij kan worden afgeweken van onder meer artikel 7 Grondwet (tweede lid). Het uitroepen van de noodtoestand is geregeld in de Coördinatiewet Uitzonderingstoestanden. Krachtens deze wet kan de regering een noodtoestand uitroepen wanneer 'buitengewone omstandigheden dit noodza-

168 Een uitgebreide analyse van deze vraagstukken is te vinden in het rapport van de Commissie Grondrechten in het Digitale Tijdperk, *Grondrechten in het digitale tijdperk*, Kamerstukken II, 2000/01, 27 460 nr. 1, bijlage I. Een wetsvoorstel tot wijziging van art. 7 Gw werd na een kritisch advies van de Raad van State niet ingediend bij de Tweede Kamer. In 2005 heeft de minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aangekondigd dat, in verband met de technologische ontwikkelingen, een nieuw voorstel tot wijziging van artikel 7 Gw zal worden voorbereid, waarbij de internationaalrechtelijke ontwikkelingen zullen worden betrokken (brief van 28 november 2005, Kamerstukken II, 2005/06, 30 300 VII, nr. 35). In de periode 2006-2008 is echter geen wetsvoorstel ingediend. Begin 2009 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aangekondigd dat het onderwerp 'Grondrechten in het digitale tijdperk' wordt opgenomen in de opdrachtverlening aan de nieuwe Staatscommissie Grondwet (brief van 26 januari 2009, Kamerstukken II, 2008/09, 31 570, nr. 8, p. 1).

169 Peters en De Vré a.w. 2005, p. 24; G.A.I. Schuijt, 'Het Censuurverbod in de Nederlandse Grondwet en Rechtspraak', in: *Censures/Censuur*, Referaten van het colloquium van 16 mei 2003 – Actes du colloque du 16 mai 2003, Uitgeverij Larcier: Brussel 2003, te downloaden op http://www.ivir.nl/publicaties/schuijt/censuurverbod.pdf.

170 J.A. Peters en I.J. de Vré, a.w. 2005 p. 24. Zie hierover ook: J.M. De Meij, *Uitingsvrijheid: de vrije informatiestroom in grondwettelijk perspectief*, Amsterdam: Cramwinckel 2000, p. 93-98.

171 Zie hierover: A.I.J Janssens en A.J. Nieuwenhuis, *Uitingsdelicten*, Kluwer: Deventer 2008, p. 29-84 en 146-171.

kelijk maken ter handhaving van de uitwendige of inwendige veiligheid' (art. 1). Volgens de memorie van toelichting bij deze wet moet het gaan om feitelijke gebeurtenissen van zodanige aard dat de veiligheid niet meer kan worden gewaarborgd zonder gebruik te maken van de buitengewone bevoegdheden die door het uitroepen van de noodtoestand ter beschikking komen.[172] Indien aan deze voorwaarde wordt voldaan, zou het (theoretisch) mogelijk zijn om bijvoorbeeld de vertoning van een film op Internet tevoren te verbieden.
Het uitroepen van de noodtoestand door de regering dient onmiddellijk ter kennis te worden gebracht van de Staten-Generaal. De Eerste en Tweede Kamer dienen vervolgens in gezamenlijke vergadering te besluiten of de noodtoestand mag voortduren. Aldus is er een parlementaire waarborg tegen het inperken van artikel 7 Grondwet wegens een noodtoestand.
Uit het vorenstaande kan worden geconcludeerd dat er weliswaar een uitzondering op het censuurverbod van artikel 7 Grondwet bestaat, maar dat deze uitzondering zeer restrictief dient te worden uitgelegd.

Een afzonderlijke vraag is nog of een rechterlijk publicatieverbod onder het censuurverbod valt. De Hoge Raad heeft bepaald dat dit niet het geval is.[173] Wil een publicatieverbod niet in strijd komen met artikel 7 Grondwet, dan moet de inhoud van de publicatie concreet bekend zijn. De rechter heeft vele malen een verbod tot publicatie afgewezen omdat het verbod dat was gevraagd te weinig concreet was.[174]

5.3 Internetcensuur en het EVRM

Ingevolge artikel 10, eerste lid, van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) heeft een ieder het recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. Ingevolge het tweede lid van artikel 10 EVRM kunnen beperkingen aan de vrijheid van meningsuiting worden gesteld. Deze beperkingen dienen 'noodzakelijk te zijn in het belang van een democratische samenleving' (de noodzakelijkheids- en proportionaliteitseis) in het belang van de nationale veiligheid, het voorkomen van wanordelijkheden

172 Kamerstukken II, 1993/94, 23 790, nr. 3, p. 4.
173 HR 2 maart 2003, *Mediaforum* 2003, 6, m.nt Schuijt. Zie hierover ook: Peters en De Vré a.w. 2005, p. 24.
174 Peters en De Vré, a.w., p. 24. Zie voor een voorbeeld: Voorzieningenrechter Rechtbank Den Haag 15 maart 2005, LJN AT0303, Mediaforum 2005, 4, p. 178 e.v., m.nt G.A.I. Schuijt.

en strafbare feiten, voor de bescherming van de gezondheid of de goede zeden of de bescherming van de rechten en vrijheden van anderen.
Het Europees Hof voor de Rechten van de Mens heeft in zijn uitspraak in de zaak Perrin tegen Verenigd Koninkrijk (2005) bepaald dat uitingen op Internet onder de reikwijdte van artikel 10, eerste lid, EVRM vallen.[175] Ook het Comité van Ministers van de Raad van Europa heeft expliciet erkend dat digitale uitingen beschermd worden door deze verdragsbepaling. In de *Declaration on Human Rights and the Rule of Law in the Information Society* (2005)[176] verklaarde het Comité dat "freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form."
In hoeverre biedt artikel 10 EVRM ruimte voor censuur van overheidswege? De tekst van artikel 10, tweede lid, sluit censuur niet uit. Wel vloeit uit die bepaling de eis voort dat elke preventieve maatregel noodzakelijk zal moeten zijn in een democratische samenleving.[177] Het Europees Hof voor de Rechten van de Mens (verder: het Hof) beschouwt voorafgaande toestemming als uiterst verdacht.[178] In het Sunday Times No. 2-arrest overwoog het Hof hierover: "[T]he dangers inherent in prior restraints are such that they call for most careful scrutiny on the part of the Court."[179]
Uit het voorgaande kan worden geconcludeerd dat internetcensuur in de jurisprudentie van het Hof niet wordt uitgesloten, maar wel aan een strikte noodzakelijkheids- en proportionaliteitstoets wordt onderworpen. Dit betekent dat een overheid, indien deze internetcensuur wil toepassen, zal moeten aantonen met het oog op welk doel het voorafgaand toezicht nodig is, dat er geen alternatief middel is om dit doel te bereiken en dat het gekozen middel (de censuur) evenredig is ten opzichte van het te bereiken doel.

175 EHRM 18 oktober 2005, Perrin t. Verenigd Koninkrijk, nr. 5446/03, *EHRC* 2006, 12, m.nt. MMG.
176 Declaration CM(2005)56 final, 13 mei 2005, gepubliceerd op de website van de Raad van Europa, www.coe.int.
177 EHRM 26 april 1979, Sunday Times t. Verenigd Koninkrijk, nr. 6538/74, *NJ* 1980, 146, m.nt. EAA. Zie ook EHRM 26 november 1991, Sunday Times t. Verenigd Koninkrijk (No. 2), nr. 13166/87, *NJ* 1992, 457, m.nt. EJD; EHRM 13 juli 1995, Miloslavsky t. Verenigd Koninkrijk, 18139/91, *NJ* 1996, 544, m.nt. EJD en EHRM 17 juli 2001, Ekin Association t. Frankrijk, nr. 39288/98, *NJ* 2002, 444, m.nt. EJD.
178 J.A. Peters en I.J. de Vré, a.w. 2005 p. 25.
179 EHRM 26 november 1991, Sunday Times t. Verenigd Koninkrijk (No. 2), nr. 13166/87, r.o. 51.

5.4 De praktijk: censuur, zelfregulering en co-regulering

In deze paragraaf staan twee vormen van censuur centraal: formele en informele censuur.[180] *Formele censuur* is censuur in de traditionele betekenis: toezicht door de overheid op de inhoud van uitingen alvorens deze worden gepubliceerd. Onder *informele censuur* wordt verstaan: informeel toezicht door media- en telecommunicatieondernemingen op de inhoud van uitingen, al dan niet op verzoek van een overheidsinstelling.[181] Terwijl formele internetcensuur vooral plaatsvindt in staten met een autoritair of repressief regime, is informele internetcensuur in opkomst in democratische staten, waaronder ook Nederland. In het onderstaande worden formele en informele censuur belicht aan de hand van enkele praktijkvoorbeelden.

Formele censuur

Op 19 september 2006 vond in Thailand een militaire coup plaats tegen de regering van de democratisch gekozen premier Thaksin Shinawatra. Na de coup rapporteerden internetgebruikers dat een aantal Thaise websites onbereikbaar was geworden. Dit betrof in het bijzonder websites van organisaties en personen die kritisch waren over de militaire coup.[182]

Reeds in 2002 rapporteerde Amnesty International over grootschalige internetcensuur in China door middel van het blokkeren van buitenlandse nieuwsorganisaties, politiekgevoelige binnenlandse websites, het blokkeren van e-mailverkeer, het verstoren van search engines en de introductie van een filtersysteem dat webverkeer met bepaalde – verboden – trefwoorden kon tegenhouden.[183] Terwijl deze vormen van internetcensuur in de periode rondom de Olympische Spelen in

180 Het hier gemaakte onderscheid is gebaseerd op: E. Dommering, *Gevangen in de waarneming. Hoe de burger de communicatiemiddelen overnam en zelf ook de bewaking ging verzorgen,* Rede uitgesproken op 25 april 2008 in de Aula van de Universiteit van Amsterdam: Otto Cramwinckel Uitgever 2008, p. 39-41.

181 Hierbij wordt onderscheid gemaakt tussen zelfregulering en co-regulering. Zelfregulering is het resultaat is van een afspraak tussen (uitsluitend) marktpartijen; co-regulering is het resultaat van samenwerking tussen marktpartijen en een overheidsinstelling.

182 Bron: nieuwsbericht Human Rights Watch, 'Thailand: Military-Backed Government Censors Internet Blocking Cyber Dissidents Obstructs Return to Democracy', 22 mei 2007, gepubliceerd op: http://www.hrw.org/en/news/2007/05/22/thailand-military-backed-government-censors-internet. Zie over deze en andere praktijkvoorbeelden van internetcensuur: J.L. Goldschmidt en T. Wu, *Who controls the Internet: Illusions of a Borderless World,* New York: Oxford Universiy Press 2006, p. 65-86, aangehaald in R. Faris en N. Villeneuve, 'Measuring Global Internet Filtering', in: R. Deibert et al 2008. *Access Denied. The Practice and Policy of Global Internet Filtering,* MIT Press: Cambridge Massachusetts 2008, p. 9.

183 Zie het rapport *State Control of the Internet in China,* te dowloaden op: http://www.amnestyusa.org/document.php?lang=e&id=50A38A55EB758C0C80256C72004773CD.

augustus 2008 korte tijd leken te zijn verminderd, zijn er diverse aanwijzingen dat de toen vrijgegeven sites sindsdien weer worden geblokkeerd.[184]

Wat zijn de motieven voor overheden wereldwijd om internetcensuur toe te passen? Uit empirisch onderzoek van Faris en Villeneuve (2008)[185] blijkt dat drie hoofdmotieven kunnen worden onderscheiden: 1) politieke- en machtsoverwegingen, 2) het handhaven van sociale normen en 3) veiligheidsoverwegingen.
Politiek gemotiveerde vormen van internetcensuur werden door Faris en Villeneuve waargenomen in staten met een autoritair of repressief regime, waaronder China, Vietnam, Iran, Myanmar, Pakistan, Thailand, Uzbekistan, Saudi-Arabië, Syrië en Lybië.[186]
Internetcensuur gericht op het handhaven van sociale normen komt voor in een groot aantal landen. Een bekend voorbeeld is Saoedi-Arabië, waar het publiceren en het bezoeken van websites met informatie over (onder meer) alcohol, drugs, gokken alsmede seksueel-expliciete informatie is verboden bij ministeriële regeling.[187] De Saoedische staat gebruikt geavanceerde filtertechnieken, zoals *Secure Computing's SmartFilter software*, om websites met de verboden informatie op te sporen en te blokkeren.[188]
Ook internetcensuur ten behoeve van de staatsveiligheid is wereldwijd een veel voorkomend fenomeen. Een voorbeeld is Zuid-Korea, waar 'het verspreiden van informatie over staatsondermijnende activiteiten' is verboden en de *Korean Internet Safety Commission* bevoegd is te bepalen welke websites illegaal materiaal bevatten en moeten worden geblokkeerd.[189]

Hoe werkt internetcensuur in de praktijk? Hoewel de technieken voortdurend veranderen, parallel aan de ontwikkelingen van het internet zelf, is het toch moge-

---

184 Bron: Keith Brashner, 'After brief Olympic thaw, China steps up Web censorship', *International Herald Tribune* 16 december 2008, http://www.iht.com/articles/2008/12/16/asia/china.php.

185 R. Faris en N. Villeneuve, 'Measuring Global Internet Filtering', in: R. Deibert et al a.w. 2008, p. 5-27.

186 Nederland heeft in 2007 de internetcensuur in China en Vietnam aan de orde gesteld in de VN Mensenrechtenraad. Zie hierover de brief van de Minister van Buitenlandse Zaken Verhagen aan de Tweede Kamer van 18 april 2007, Kamerstukken II 2006/07, 30 800 V, nr. 86, p. 4. Nederland en de EU hebben in de Mensenrechtenraad ook aandacht gevraagd voor internetcensuur in Pakistan. Zie hierover de antwoorden van de minister van Buitenlandse Zaken op Kamervragen (1297) van het Lid Peters, Kamerstukken II 2006/2007, Aanhangsel van de Handelingen 2758.

187 Council of Ministers Resolution van 12 februari 2001. Een Engelse vertaling van deze ministeriële regeling is gepubliceerd op: http://www.al-bab.com/media/docs/saudi.htm.

188 Zie hierover uitgebreid: J. Zittrain and B. Edelman, *Documentation of Internet Filtering in Saudi Arabia,* Harvard Law School: Berkman Center for Internet & Society 2002, http://cyber.law.harvard.edu/filtering/saudiarabia/ en R. Deibert et al a.w. 2008, p. 363 (Country Summary Saudi Arabia).

189 Deze wet, de National Security Law, is in Zuid-Korea controversieel: zie hierover: *The Korea Herald*, 8 september 2004, 'A nation-splitting law', http://www.asiamedia.ucla.edu/article.asp?parentid=14429. Bron: R. Deibert et al a.w. 2008, p. 369-373 (Country Summary Saudi Arabia).

lijk vier thans veel voorkomende technieken te benoemen (aansluitend bij de vakterminologie worden de Engelse termen gebruikt): *IP blocking*, *DNS tampering, proxy-based blocking methods* en *server take down.*[190]
Onder *IP blocking* wordt verstaan het blokkeren van IP-adressen[191] zodat internetgebruikers de aan deze adressen verbonden webpages niet meer kunnen bezoeken.
DNS tampering, ofwel DNS vervalsing, is het verstoren van DNS-servers, de netwerkcomputers op internet die domeinnamen (bijvoorbeeld bureaujansen.nl) koppelen aan IP-adressen. Door het verstoren van de DNS-servers verbinden deze servers de domeinnamen aan verkeerde IP-adressen, waardoor websites onbereikbaar worden.
Proxy-based blocking methods zijn filtermethodes waarbij het internetverkeer langs een computersysteem wordt geleid met het doel het te bezoeken http-adres[192] te vergelijken met een lijst van te blokkeren sites. Dit kunnen individuele domeinen zijn (bijvoorbeeld bureaujansen.nl) maar ook subdomeinen (bijvoorbeeld .nl). Ook kan worden gefilterd op bepaalde woorden in het domein (bijvoorbeeld falung gong[193]). Wanneer een internetgebruiker een domein op de lijst probeert te bezoeken, wordt de site geblokkeerd. Soms verschijnt in dat geval een formele mededeling dat de site is geblokkeerd; in andere gevallen verschijnt een leeg scherm of een storingsmelding.
Server take down ten slotte is het fysiek loskoppelen van een server van het internet (letterlijk: de stekkers lostrekken) zodat deze niet meer is verbonden met internet. Dit kan geschieden door overheidsfunctionarissen, bijvoorbeeld politie- of veiligheidsdiensten die het kantoor van een internet service provider bezoeken, of door de eigenaar of beheerder van een internet service provider op bevel van een overheidsfunctionaris.

Informele censuur: zelfregulering en co-regulering
Naast internetcensuur in de strikte betekenis van het woord (van overheidswege) hebben zich het afgelopen jaar ook verscheidene vormen van informele internetcensuur ontwikkeld. De belangrijkste vormen zijn zelfregulering en co-regulering door internet service providers.

---

190 De nu volgende beschrijving is gebaseerd op: R. Faris en N. Villeneuve a.w. 2008, p. 13-15 en S.J. Murdoch en R. Anderson, 'Tools and Technology of Internet Filtering', in: R. Deibert et al a.w. 2008, p. 58-64.

191 IP adres: Internet Protocol adres: nummer waarmee een met het internet verbonden computer geïdentificeerd kan worden door andere computers (te vergelijken met een telefoonnummer).

192 HTTP: HyperText Transfer Protocol. Http-adres: adres van een webpagina op het World Wide Web (internet).

193 Falung Gong is een in China verboden levensovertuiging. Websites met de woorden 'falung gong' worden in China geblokkeerd.

Zelfregulering betreft afspraken tussen internet service providers, search engines (zoals Google) of andere telecommunicatiebedrijven onderling over het filteren van informatie met een bepaalde inhoud. Een voorbeeld is het samenwerkingsverband tussen zeven *search engines* (zoekmachines) in Duitsland – Google, Lycos Europe, MSN Deutschland, AOL Deustchland, Yahoo, T-online en t-info – met het doel informatie die schadelijk is voor minderjarigen op gecoördineerde wijze te filteren. De filtering vindt plaats op basis van een index, de *Bundesprüfstelle für Jugendgefährdende Medien*[194], die wordt opgesteld en gepubliceerd door het Duitse federale Ministerie voor Media.[195]

Deze vorm van *informele controle vooraf* gaat in de praktijk dikwijls gepaard met *informele repressie achteraf* zonder rechterlijke tussenkomst door middel van een zogeheten 'notice and take down procedure'[196]: het op eerste aanmaning door de beheerder van het internetplatform (of de internet service provider) verwijderen van informatie die in de aanmaning als schadelijk en/of onrechtmatig wordt aangemerkt. In Nederland is in dit kader artikel 6:196c van het Burgerlijk Wetboek van belang.[197] In het vierde lid van deze bepaling wordt aangegeven dat een 'hosting provider' [198] niet aansprakelijk is als hij a) niet wist of behoorde te weten dat er sprake was van een activiteit of informatie met een onrechtmatig karakter, dan wel b) zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt. Door het toepassen van *notice and take down procedure*s kunnen hosting providers in Nederland aansprakelijkheid op grond van art. 6:196c, vierde lid, BW voorkomen.

Van co-*regulering* is sprake als een regeling of afspraak berust op samenwerking tussen marktpartijen enerzijds en een overheidsinstelling anderzijds. De grens tussen zelf-regulering en co-regulering is niet altijd scherp te trekken. In dit kader kan worden gewezen op het samenwerkingsverband tussen een aantal Nederlandse internet service providers en het Korps Landelijke Politiediensten (KLPD)

194 Deze index is gepubliceerd op: http://www.bundespruefstelle.de/bmfsfj/generator/bpjm/die-bundespruefstelle.html.

195 Zie over de inhoud van deze index en de toepassing ervan door de zeven Duitse search engines: M. Ermert en R.W. Smith, 'Search engine providers practice self-regulation', *Heise Online* 25 februari 2005, http://www.heise.de/english/newsticker/news/56817.

196 Dommering a.w. 2008, p. 39. Zie over de praktijk van *notice and take down procedures* in Nederland: Peters en De Vré a.w. 2005 p. 58-66.

197 Deze bepaling is in 2004 in het Burgerlijk Wetboek opgenomen door de inwerkingtreding van de Aanpassingswet richtlijn inzake elektronische handel. Die wet vormt de implementatie van de Richtlijn Elektronische Handel: Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, Pb EG 17 juli 2000, L178/1-16.

198 Hosting provider: provider die informatie van een ander op verzoek opslaat.

met het doel de toegang tot websites met kinderpornografisch materiaal te blokkeren.[199] Het KLPD houdt een 'zwarte lijst' bij van webpages met kinderpornografisch materiaal. De samenwerkende internet service providers passen vervolgens filtertechnieken toe om de toegang tot deze webpages te blokkeren.
In opdracht van het ministerie van Justitie (WODC) is in 2008 een onderzoek uitgevoerd naar (o.m.) de juridische grondslag van deze samenwerking tussen de KLPD en de internet service providers.[200] De onderzoekers concluderen dat de juridische grondslag voor het blokkeren van de webpages op basis van de zwarte lijst van de KLPD problematisch is. De KLPD heeft geen bevoegdheid tot het (doen) filteren en blokkeren van websites met kinderpornografisch materiaal. Een dergelijke activiteit kan niet worden gebaseerd op artikel 2 Politiewet 1993, maar vereist een expliciete wettelijke basis vanwege de mogelijke beperking van het uitoefenen van het grondwettelijk beschermde recht op de vrijheid van meningsuiting. De onderzoekers wijzen op de mogelijkheid van zelfregulering en analyseren in dat verband ervaringen in andere Europese landen, waaronder Noorwegen en Zweden.
In reactie op dit onderzoeksrapport schreef de Minister van Justitie op 15 september 2008 aan de Tweede Kamer (o.m.): "Ik onderschrijf dat de mogelijkheden om te filteren en te blokkeren kleiner worden wanneer de overheid dit doet of laat doen; de mogelijkheden van de overheid om informatie te blokkeren worden immers begrensd door Grondwet en EVRM. Ik onderschrijf ook de mening van de onderzoekers dat er juridische mogelijkheden zijn voor providers, netwerkbeheerders of particulieren om hun internetverkeer zelf te filteren."[201] De minister geeft aan van mening te zijn dat de werkwijze die nu door het KLPD samen met een aantal internet service providers wordt gevolgd niet moet worden voortgezet. Hij heeft overleg gevoerd met vertegenwoordigers van de internet service providers om alternatieve mogelijkheden te onderzoeken. Afgesproken is dat de internet service providers de techniek van het ontdekken van kinderporno zullen proberen te verfijnen en die te gebruiken voor het ontwikkelen van kinderpornofilters, zo blijkt uit de brief van de minister aan de Kamer. Voorts zullen de internet

199 Zie hierover (o.m.) de brief van de Minister van Justitie van 15 september 2008 aan de Tweede Kamer, Kamerstukken II 2007/08, 28 684 en 31 200 VI, nr. 166.

200 De onderzoeksopdracht was verstrekt in reactie op de motie Van der Staaij–Rouvoet (TK 2005–2006, 30 300 VI, nr. 160), waarin de regering was verzocht 'verdere uitbouw en toepassing van de technische mogelijkheden tot het blokkeren, filteren of afsluiten van kinderpornografisch materiaal op internet en andere media te bevorderen en de Kamer daarover nader te berichten'. De resultaten van dit onderzoek zijn gepubliceerd in: W.Ph.Stol, H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt en A.R. Lodder, *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland,* bijlage bij Kamerstukken II 2007/08, 28 684 en 31 200 VI, nr. 166. Dit rapport is tevens gepubliceerd bij Uitgeverij Boom te Den Haag.

201 Kamerstukken II 2007/08, 28 684 en 31 200 VI, nr. 166, p. 4.

service providers zelf een voorziening treffen voor het bijhouden en actualiseren van de zwarte lijst en zullen zij, gezamenlijk met de overheid, werken aan de ontwikkeling van een platform voor de internationale uitwisseling van gegevens.[202]

5.5 Conclusie

In deze bijdrage zijn de juridische mogelijkheden en grenzen van internetcensuur onderzocht. Daarbij is een onderscheid gemaakt tussen internetcensuur in de strikte betekenis van het woord en 'informele internetcensuur'. Onder *formele internetcensuur* is verstaan: een vorm van toezicht van overheidswege op de inhoud van een uiting op Internet alvorens deze uiting wordt gepubliceerd. Onder *informele censuur* is verstaan: informeel toezicht door media- en telecommunicatieondernemingen op de inhoud van uitingen, al dan niet op verzoek van een overheidsinstelling.

Eerst is onderzocht of internetcensuur mogelijk is onder de Nederlandse Grondwet. Artikel 7, eerste lid, Gw verbiedt censuur van overheidswege expliciet. Toezicht op de inhoud van een uiting vormt de harde kern van het censuurverbod. Aangenomen moet worden dat het censuurverbod bij uitingen op Internet op dezelfde wijze geldt als bij uitingen in een niet-digitale omgeving.
Vervolgens is de vraag behandeld of artikel 10 EVRM ruimte biedt voor internetcensuur. Geconcludeerd werd dat internetcensuur in de jurisprudentie van het Hof niet wordt uitgesloten, maar wel aan een strikte noodzakelijkheids- en proportionaliteitstoets wordt onderworpen. Dit betekent dat een overheid, indien deze internetcensuur wil toepassen, zal moeten aantonen met het oog op welk doel het voorafgaand toezicht nodig is, dat er geen alternatief middel is om dit doel te bereiken en dat het gekozen middel (de censuur) evenredig is ten opzichte van het te bereiken doel.

In het tweede deel van deze bijdrage stond de praktijk van formele en informele internetcensuur centraal. Onderzocht is welke vormen van formele en informele internetcensuur wereldwijd, in Europa en in Nederland voorkomen, welke motieven daaraan ten grondslag liggen en hoe internetcensuur in technische zin werkt.

202 Kamerstukken II 2007/08, 28 684 en 31 200 VI, nr. 166, p. 5.

Geconcludeerd is dat *formele internetcensuur* vooral plaatsvindt in staten met een autoritair of repressief regime, terwijl informele internetcensuur in opkomst is in democratische staten, waaronder ook Nederland. In het onderzoek naar de motieven voor formele internetcensuur werden drie hoofdmotieven gevonden: 1) politieke- en machtsoverwegingen, 2) het handhaven van sociale normen en 3) veiligheidsoverwegingen.

Bij *informele internetcensuur* is een onderscheid gemaakt tussen zelfregulering en co-regulering. In het onderzoek naar de praktijk van informele internetcensuur kwam een grote variatie aan toepassingsvormen naar voren. Een in het oog springend voorbeeld betrof het samenwerkingsverband tussen een aantal Nederlandse internet service providers en het Korps Landelijke Politiediensten (KLPD) met het doel de toegang tot websites met kinderpornografisch materiaal te blokkeren. De Nederlandse minister van Justitie heeft recent erkend dat de juridische grondslag voor het blokkeren van de webpages op basis van de zwarte lijst van de KLPD problematisch is. Hij heeft aangegeven dat de werkwijze die nu door het KLPD samen met de internet service providers wordt gevolgd niet zal worden voortgezet en is in overleg getreden met de internet service providers om te bezien of het filteren op basis van de zwarte lijst kan worden voortgezet op basis van een vorm van zelfregulering door de betrokken internet service providers. Uit deze casus blijkt dat de Grondwet en het EVRM duidelijke grenzen stellen aan het filteren van internetverkeer en dat zelfregulering mogelijk een oplossing kan zijn om de met het filteren beoogde doelen te bereiken zonder over de grondwettelijke en verdragsrechtelijke grenzen heen te gaan.