BITS OF FREEDOM
Voor jouw internetvrijheid

Datum:
15 augustus 2018

Ons kenmerk:
Inbreng consultatie van de Uitvoeringswet CPC-Verordening

Aan:
Ministerie van Economische Zaken en Klimaat

Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Geachte heer, mevrouw,

Met deze brief reageert Bits of Freedom op het ter consultatie aangeboden wetsvoorstel waarmee enkele aspecten ter uitvoering van de CPC-verordening worden geregeld.[1]

Bits of Freedom heeft met name opmerkingen over de bevoegdheid voor enkele autoriteiten om, kort gezegd, een last aan een aanbieder van een communicatiedienst, de beheerder van een domeinregister of een domeinregistrerende instantie op te leggen met als doel bepaalde informatie ontoegankelijk te maken. Onze kritiek spitst zich toe op een drietal aspecten:

1. een autoriteit mag niet vragen wat het ook kan bevelen,
2. een autoriteit mag niet de vervalsing of filtering van internetverkeer bevelen en
3. een autoriteit moet vooraf inventariseren wat de consequenties zijn van een last voor de toegankelijkheid van andere informatie dan die informatie die beoogd wordt ontoegankelijk te maken.

Deze punten worden hieronder nader toegelicht.

Een autoriteit mag niet vragen wat het ook kan bevelen

1. Het voorstel introduceert een bevoegdheid voor enkele bevoegde autoriteiten om, kort gezegd, een last aan een aanbieder van een communicatiedienst, de beheerder van een domeinregister of een domeinregistrerende instantie (hierna: "aanbieder") op te leggen met als doel bepaalde informatie ontoegankelijk te maken. Het betreft een bevel waaraan de aanbieder verplicht is te voldoen.[2]

2. De beoogde praktijk is dat i) de autoriteit eerst de aanbieder verzoekt om bepaalde informatie ontoegankelijk te maken en ii) als die aanbieder geen gehoor geeft aan

1 https://www.internetconsultatie.nl/uitvoeringswetcpc2017

2 Artikel 2.7, zoals genoemd in onderdeel D van het wetsvoorstel.

dat verzoek de autoriteit het ontoegankelijk maken alsnog afdwingt of af kan dwingen met een last.[3]

3. Het kabinet constateert terecht dat "het hier gaat om een bevoegdheid die potentieel ingrijpende gevolgen [kan] hebben" en dat die "met de nodige terughoudendheid [moet] worden toegepast.".[4] Zij heeft daarom de bevoegdheid van waarborgen voorzien, bedoeld om een zorgvuldige toepassing af te dwingen. Zo mag de bevoegdheid alleen worden ingezet als er vooraf een rechterlijke toetsing heeft plaatsgevonden.

4. Indien de autoriteit de aanbieder slechts verzoekt (en dus geen last oplegt) om bepaalde informatie ontoegankelijk te maken, worden deze waarborgen niet toegepast. Het is in die situatie vertrouwen op een kritische houding van de aanbieder om te voorkomen dat met het ontoegankelijk maken van de informatie een ongeoorloofde inbreuk op de vrijheden en rechten van anderen plaatsvindt. Het is onverstandig om een private partij in een positie te duwen waarin het een afweging moet maken waar fundamentele rechten van anderen op het spel staan, zonder dat hiervoor vergelijkbare waarborgen gelden, zoals een onafhankelijke voorafgaande toets.

5. Daar komt bij dat het voor de aanbieder niet altijd even makkelijk zal zijn om weerstand te bieden tegen de overmacht van een autoriteit. De aanbieder zal vaak het zekere voor het onzekere nemen en derhalve preventief bepaalde informatie ontoegankelijk maken. Daarmee worden de waarborgen, die wel bij het inzetten van de bevoegdheid gelden, buitenspel gezet.

6. Uit de toelichting blijkt bovendien dat het uitvaardigen van een last bij een weigering van honorering van het verzoek optioneel is.[5] Welke waarde kunnen we hechten aan een verzoek tot het ontoegankelijk maken van informatie als dat, bij een weigering, niet altijd wordt opgevolgd door een bevel?

7. Het uitgangspunt moet zijn: de bevoegde autoriteit mag niet vragen wat het ook kan bevelen. Daarin valt eenvoudig te voorzien door in de toelichting expliciet te vermelden dat, indien het beoogde doel van de bevoegde autoriteit is om bepaalde informatie ontoegankelijk te laten maken, dit alleen mag door toepassing van de voorgestelde bevoegdheid.

Een autoriteit mag niet de vervalsing of filtering van internetverkeer bevelen

8. In de toelichting schrijft het kabinet expliciet dat de bevoegde autoriteit "het bevel moet [richten] tot degene die daarvoor het meest in aanmerking komt" en daarbij rekening moet houden met "de eisen van proportionaliteit en subsidiariteit".[6] Het

3 Pagina 26 van de toelichting.
4 Pagina 20 van de toelichting.
5 "Bij verschil van mening kan een zelfstandige last [...] worden opgelegd."
6 Pagina 31 van de toelichting.

kabinet laat expliciet ruimte aan de bevoegde instantie om deze last te richten aan een internettoegangsprovider. Dat zou mogelijk moeten zijn als, bijvoorbeeld, "de gegevens in het buitenland worden gehost."

9. De internettoegangsprovider geeft haar klanten slechts toegang tot het internet en faciliteert een deel van het transport van het internetverkeer tussen haar klant en de aanbieders van diensten op het internet. Zij is meestal niet ook degene bij wie de informatie die ontoegankelijk gemaakt moet is *gehost*. Deze internettoegangs-provider heeft geen kennis van de wijze waarop de hosting provider, bij wie de informatie wel is opgeslagen, haar computersystemen heeft ingericht.

10. In zo'n geval kan de internettoegangsprovider op een beperkt aantal manieren voldoen aan een last om die bedoelde informatie ontoegankelijk te maken. Eén manier is het blokkeren van alle internetverkeer naar het IP-adres van de computer waarop de bedoelde informatie is opgeslagen. Een tweede manier is het vervalsen van de vertaling van de *hostname* van de website met de bedoelde informatie naar het IP-adres van de computer via welke de website toegankelijk is. De provider vervalst of blokkeert hierbij DNS-verkeer.[7]

    Beknopte uitleg. Als een internetgebruiker de website internetconsultatie.nl wil bezoeken, vraagt diens computer aan de DNS-server van zijn internettoegangs-provider op welk IP-adres de server, waarop de website is ondergebracht, te bereiken is. De DNS-server antwoord daarop bijvoorbeeld 62.112.232.243. De computer maakt vervolgens een verbinding met de website op dat adres. Als de internettoegangs-provider gedwongen is de toegang tot de website te blokkeren, zal hij het antwoord op de vraag aan de DNS-server vervalsen en de gebruiker naar een andere server leiden.

11. De eerste methode is zeer onwenselijk omdat de internettoegangsprovider nooit kan overzien welke informatie hierdoor precies ontoegankelijk wordt gemaakt. Via een enkel IP-adres kunnen meerdere websites (of andere diensten) beschikbaar zijn, soms zelfs honderden. Met het blokkeren van dat ene IP-adres, ten einde één enkele website ontoegankelijk te maken, kan goed mogelijk zijn dat een groot aantal andere websites ook ontoegankelijk worden. Dit is voor de internettoegangsprovider niet voorzienbaar.

12. Ook het vervalsen van het DNS-verkeer door internettoegangsproviders is zeer onwenselijk. Het vervalsen of blokkeren van DNS-verkeer ondermijnt het vertrouwen in onze digitale infrastructuur. Immers, door het vervalsen van het internetverkeer wordt de gebruiker misleid. Dat is fundamenteel anders dan het letterlijk laten verwijderen van informatie of het laten de-registreren van een domeinnaam. Het vervalsen van DNS-verkeer is een methode die ook door kwaadwillenden wordt gebruikt. Hoe weet de gebruiker zeker dat niet ook het internetverkeer naar andere websites wordt vervalst en, als het al gebeurt, wie wat met deze vervalsing beoogd?

7 Dit is geen allesomvattende lijst, maar andere methoden zijn meestal erg kostbaar of ineffectief.

13. Bovendien staat de introductie van de bevoegdheid tot het vervalsen en filteren van internetverkeer ook haaks op de inspanning van de overheid om onze digitale infrastructuur zo veel mogelijk te beveiligen en te versterken. Daartoe ondersteunt de overheid de ontwikkeling van nieuwe technologie die tot doel heeft ons internet veiliger te maken, zoals bijvoorbeeld DNSSEC. Een verplichting om DNS-verkeer te filteren zit de ontwikkeling van dit soort technologie in de weg.

14. Bits of Freedom adviseert dan ook om de bevoegdheid tot het vervalsen en filteren van internetverkeer door internettoegangsproviders of aanbieders die enkel en alleen betrokken zijn bij de doorgifte van het internetverkeer uit het wetsvoorstel te halen. We delen het standpunt dat het mogelijk moet zijn om informatie ontoegankelijk te maken, bijvoorbeeld door het ontoegankelijk maken van informatie af te dwingen bij de provider op wiens systemen de informatie is opgeslagen (hostingprovider). Dit kan in het voorgestelde artikel worden opgelost door een zin toe te voegen: "Onder ontoegankelijkmaking wordt niet verstaan het vervalsen of filteren van internetverkeer door internettoegangsproviders of aanbieders die enkel en alleen betrokken zijn bij de doorgifte van het verkeer."

15. Overigens maakt dit niet dat de informatie die is ondergebracht op de computer-systemen in het buitenland altijd buiten bereik van bevoegde autoriteiten valt. Het zou echter meer proportioneel en subsidiair zijn als voor het ontoegankelijk maken van zulke informatie wordt ingezet op samenwerking met buitenlandse autoriteiten. Het ontbreken van samenwerkingsverbanden en/of de traagheid van procedures, mogen geen excuus zijn om dan deze disproportionele maatregelen te treffen.

Een autoriteit moet vooraf een inventarisatie van de consequenties maken

16. Zoals reeds opgemerkt erkent het kabinet dat "het hier gaat om een bevoegdheid die potentieel ingrijpende gevolgen [kan] hebben" en dat die bevoegdheid "met de nodige terughoudendheid [moet] worden toegepast." Het kabinet kiest er daarom onder meer voor dat bij de toepassing van de bevoegdheid een machtiging van een rechter-commissaris vereist is. Dat is een verstandige keuze, vindt Bits of Freedom.

17. Dat neemt niet weg dat het risico bestaat dat met de uitvoering van een last een aanbieder van een communicatiedienst, een beheerder van een domeinregister of een registrerende instantie meer dan alleen de beoogde informatie ontoegankelijk maakt. Het is goed mogelijk dat met het ontoegankelijk maken van een enkele website, honderden andere websites eveneens ontoegankelijk worden. In het verleden is gebleken dat ook de rechter-commissaris dit niet of niet altijd voorziet of kan voorzien. Voorbeeld: terwijl het Openbaar Ministerie de toegang tot één enkele afbeelding wilde blokkeren, werd, na machtiging van een rechter-commissaris de toegang tot een server geblokkeerd waarmee honderden andere sites, emailadressen en mailinglists onbereikbaar werden.[8]

8 https://webwereld.nl/overheid/56727-om-zet-honderden-sites-op-zwart-om-1-fout-plaatje en https://www.bof.nl/2012/05/07/om-negeert-rechter-bij-bevel-blokkeren-website/

18. De wetgever moet daarom afdwingen dat de autoriteit, die wil overgaan tot het opleggen van een last om bepaalde informatie ontoegankelijk te maken, vooraf een inventarisatie maakt van de mogelijke consequenties voor de toegankelijkheid van andere dan de bedoelde informatie. Indien het niet mogelijk blijkt een deugdelijke inventarisatie te maken of indien blijkt dat de last informatie van derden ontoegankelijk maakt, moet de autoriteit afzien van het opleggen van de voorgenomen last. Deze analyse dient te worden voorgelegd aan de rechter-commissaris bij het verzoek om een machtiging.

Vanzelfsprekend is Bits of Freedom graag bereid deze kritiekpunten nader toe te lichten, mocht daartoe behoefte bestaan.

Met vriendelijke groet,