

Je wachtwoord. Of anders...

Wetsvoorstel Computercriminaliteit III dwingt verdachten om versleutelde bestanden toegankelijk te maken voor justitie. De ontsleutelplicht geldt vooralsnog alleen voor verdachten van kinderporno en terreur. Mogelijke uitbreiding van de plicht naar verdachten van andere strafbare feiten en problemen rond de bewijsbaarheid geven te denken.

Peter Hermens en Berfin Yesilgöz¹

Op 2 mei 2013 heeft minister van Veiligheid en Justitie Ivo Opstelten (VVD) het wetsvoorstel Computercriminaliteit III gepresenteerd. In de media werd het wetsvoorstel geduid als het wetsvoorstel waarbij de politie de mogelijkheid krijgt om verdachten (terug) te hacken en waarbij verdachten een ontsleutelplicht opgelegd kunnen krijgen wat wil zeggen dat verdachten hun versleutelde bestanden toegankelijk moeten maken voor justitie. Het wetsvoorstel behelst behalve die bevoegdheden ook nog een zogeheten *Notice and take down*-bevel, wat neerkomt op een bevel tot het ontoegankelijk maken van data op internet.

Het wetsvoorstel van Opstelten zal gelet op de vele recente berichten over DDoS-aanvallen waarbij een computer onbruikbaar wordt gemaakt door andere computers, en digitale identiteitsdiefstal aan maatschappelijke relevantie toemen. Alle onderwerpen die in het wetsvoorstel worden behandeld, zouden dan ook stuk voor stuk bespreking verdienen, maar wij hebben ervoor gekozen in dit artikel alleen de voorgestelde ontsleutelplicht, ook wel het 'decryptiebevel', tegen het licht te houden.

Het is niet voor het eerst dat er een voornemen bestaat tot een decryptiebevel. Ten tijde van de Wet computercriminaliteit II, eind jaren negentig van de vorige eeuw, stond toenmalig minister van Justitie Benk Korthals (VVD) al stil bij de gedachte om een verdachte een bevel tot ontsleuteling te mogen opleggen. Dit werd toen nog een brug te ver gevonden.²

De huidige minister ziet dit anders. In een toegenomen digitalisering van de maatschappij ziet hij problemen bij het opsporen van ernstige strafbare feiten. Niet alleen wordt communicatie standaard versleuteld door gebruikelijke elektronische communicatiediensten zoals Googles Gmail en Twitter. Er is ook een toename van encryptieprogramma's op internet zoals TrueCrypt, waar het zelfs voor een weinig technisch onderlegd persoon mogelijk is bestanden zo te versleutelen dat goede hackers de codes niet kunnen kraken.

In het wetsvoorstel wordt de plicht tot ontsleuteling vooralsnog beperkt tot twee strafbare feiten; het maken van een beroep of gewoonte van het bezit, de vervaardiging of de verspreiding van kinderpornografie en het plegen van terroristische misdrijven. Het publieke belang om dergelijke vormen van criminaliteit aan te pakken zou daartoe nopen. Hoewel de minister zich nu nog niet heeft uitgelaten over de mogelijkheden om het decryptiebevel uit te breiden naar andere strafbare feiten, valt te verwachten dat dit niet lang zal duren. Bevoegdheden die bevallen, worden nu eenmaal van overheidswege veelal uitgebreid.

De minister stelt een aantal procedurele waarborgen voor.³ Allereerst mag een bevel tot ontsleuteling slechts worden gegeven indien het onderzoek dit dringend vordert. Hiermee wordt gestalte gegeven aan de vereisten van proportionaliteit en subsidiariteit. Een andere waarborg zou moeten zijn dat een officier van justitie een dergelijk bevel mag geven na een daartoe

voorafgaande machtiging van de rechter-commissaris. Deze laatste moet voldoen aan de wettelijke voorwaarden, de noodzaak van het bevel, de ongeschreven beginselen van een behoorlijke procesorde en de overige voorwaarden rond het bevel (zoals de termijn voor de uitvoering en de wijze van uitvoering voor de verdachte).

Een derde, aan de vorige voorwaarde gekoppelde, voorwaarde is dat de verdachte in het bijzijn van zijn advocaat wordt gehoord door de rechter-commissaris alvorens de beslissing wordt genomen. Gedurende dat verhoor dient de rechter-commissaris vast te stellen of het klopt dat de verdachte weigert mee te werken. Tegen het bevel om mee te werken aan de ontsleuteling van bestanden staat voor de verdachte een beklagmogelijkheid ex art. 552a Sv open.

Nemo-teneturbeginsel

Het opzettelijk niet-voldoen aan een decryptiebevel wordt, als het aan de minister ligt, strafbaar. Er kan een gevangenisstraf worden opgelegd van ten hoogste drie jaar of een geldboete van de vierde categorie.⁴ Deze sanctie kan een ernstige vorm van dwang opleveren en de vraag doet zich dan ook voor of het decryptiebevel zoals de wetgever dat voor ogen heeft verenigbaar is met het nemo-teneturbeginsel.

Het nemo-teneturbeginsel vormt een essentieel onderdeel van het recht op een eerlijk proces – zoals verwoord in art. 6 EVRM – en houdt in dat niemand gehouden is bewijs tegen zichzelf te leveren. Dit beginsel ziet in eerste lijn op de verklaringsvrijheid van een verdachte. Met

¹ Advocaten in Amsterdam.

² Kamerstukken II, 1998/1999, 26 671, nr. 3, p. 26.

³ Memorie van toelichting bij wijziging WvSr en WvSv in verband met verbetering en versterking opsporing en vervolging computercriminaliteit III, 4.2, p. 51.

⁴ Memorie van toelichting bij wijziging WvSr en WvSv in verband met verbetering en versterking opsporing en vervolging computercriminaliteit III, 4.4., p. 55.

andere woorden, dat de verdachte het recht heeft om te zwijgen. Maar de reikwijdte van nemo tenetur gaat verder dan enkel de verklaringsvrijheid. In zijn arrest van 19 september 2006 legt de Hoge Raad het zwijgrecht ruim uit.⁵ Niet enkel omvat dit het afleggen van een verklaring, maar ook het weigeren om informatie en opheldering te verschaffen. Valt het verstrekken van een wachtwoord dan ook onder het nemo-teneturbeginsel?

Bij het verstrekken van een wachtwoord dient onderscheid te worden gemaakt of het wachtwoord is opgeschreven of (uitsluitend) in het hoofd van de verdachte zit. In het eerste geval gaat het om een vordering tot levering van fysiek bewijs; in het tweede geval is een intellectuele inspanning van de verdachte nodig. Het eerste geval zou opgevat kunnen worden als een kleinere inbreuk op het nemo-teneturbeginsel.

Er wordt algemeen aangenomen dat materiaal dat afhankelijk van de wil bestaat, sterke bescherming geniet van het nemo-teneturbeginsel. Het is betwistbaar of een wachtwoord te kwalificeren is als materiaal afhankelijk van de verdachte. Het wachtwoord bestaat immers, onafhankelijk van de wil van de verdachte. Het materiaal kan echter niet onafhankelijk van de wil van de verdachte worden verkregen. Als de verdachte besluit zijn mond te houden, zal het wachtwoord niet te achterhalen zijn.

De minister onderkent dan ook in het wetsvoorstel dat het nemo-teneturbeginsel bij een decryptiebevel in het gedrang komt.

Desondanks komt hij tot de conclusie dat het decryptiebevel niet in strijd hoeft te zijn met het recht op een eerlijk proces.⁶ Hij ziet zich hierin gesterkt door een lijvig rapport dat in opdracht van het ministerie is opgesteld door hoogleraar regulering van de technologie aan de Universiteit van Tilburg Bert-Jaap Koops.⁷ In dit rapport stelt Koops dat er enige ruimte is binnen de grenzen van het nemo-teneturbeginsel om een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. De hoge sanctie die de wetgever voor ogen heeft op het niet-meewerken zal echter volgens Koops slechts de toets van het EHRM doorstaan indien er aanzienlijke waarborgen tegenover staan: enkel bij aantoonbaar ernstige gevallen, een uitgebreid en afgevoerd stelsel van procedurele waarborgen, en terughoudendheid bij het daadwerkelijk opleggen van een straf voor weigering.⁸ Bovendien zal er voldoende bewijs dienen te zijn dat een verdachte kan ontsleutelen. Alvorens een dergelijke ernstige vorm van dwang toegepast mag worden, zal justitie zelf met voldoende bewijs moeten komen.

Bewijsbaarheid

Het verweer dat naar verwachting het meest zal worden gevoerd, is dat de verdediging aanvoert dat de verdachte wel zou willen meewerken aan het decryptiebevel, maar simpelweg het wachtwoord vergeten

is. Het wachtwoord zal namelijk complexer zijn dan de wachtwoorden die menigeen gebruikt zoals de geboortedatum van zijn ouders, de naam van zijn eerste huisdier of het adres van waar hij woont. Anders zou het Nederlands Forensisch Instituut het wachtwoord immers kunnen kraken. De arrestatie van de verdachte en alle stress die daarmee gepaard gaat, zou het plausibel kunnen maken dat het geheugen hem in de steek laat. Dit wordt nog verergerd indien de verdachte gebruikmaakte van een programma waarbij men slechts drie pogingen heeft om het correcte wachtwoord in te voeren voordat de bestanden definitief worden verwijderd.

Een ander in de rede liggend verweer is dat het Openbaar Ministerie er niet in geslaagd is te bewijzen dat er op de bestanden, waar de verdachte de wachtwoorden niet voor wil verstrekken, materiaal staat dat kinderporno of terrorisme omvat. Men zou zich immers kunnen indenken dat de bij bewijsrechtelijk zwakke zaken – waar met name het decryptiebevel kan bijdragen aan verkrijgen van missend bewijsmateriaal – ook het bewijs zwak is dat een verdachte kan ontsleutelen.

Vooralsnog wordt de plicht tot ontsluiting beperkt tot twee categorieën strafbare feiten. Naar onze mening zal het niet lang duren voordat dit wordt uitgebreid. En dat terwijl er stevige bedenkingen te uiten zijn tegen het voorgenomen decryptiebevel. Vooral vanwege de stevige vorm van dwang in de vorm van de hoge strafbedreiging en de problemen aangaande de bewijsbaarheid. <<

5 HR 19 september 2006, LJN: AV1141.

6 Memorie van toelichting bij wijziging WvSr en WvSv in verband met verbetering en versterking opsporing en vervolging computercriminaliteit III, 4.6.1

7 Koops, B.J., *Het decryptiebevel en het nemo-teneturbeginsel*, Universiteit van Tilburg, 2012.

8 Koops, B.J., *Het decryptiebevel en het nemo-teneturbeginsel*, Universiteit van Tilburg, 2012, p. 105.

(advertentie)

TOGA
atelier
S c h o u t

Kwaliteit met oog voor detail



www.toga-atelierschout.nl
info@toga-atelierschout.nl



Industrieweg 51
3044 AS Rotterdam
Tel.: 010 245 07 66
di t/m vr 9:00 - 17:30

TER VOORTZETTING AANGEBODEN WEGENS PENSIONERING

PASMA ADVOCATENKANTOOR
Compleet met inboedel en inventaris ter voortzetting van de praktijk.

EEN UNIEKE KANS OP EEN PRACHTIGE LOCATIE AAN DE NOORDERHAVEN TE HARLINGEN

Mr T.H. Pasma
Noorderhaven 59
8861 AK HARLINGEN
Tel. 0517-418384
Email: harlingen@pasma-advocatenkantoor.nl