BIJLAGE 4 Ontsleutelplicht

Een decryptiebevel beoogt een oplossing te bieden voor het probleem dat elektronische gegevens op zodanige wijze worden versleuteld dat derden daar geen toegang toe hebben. Met een decryptiebevel kan de weigering van een verdachte om mee te werken aan het ontsleutelen van gegevens strafbaar worden gesteld. Een decryptiebevel is een verstrekkende maatregel die in de afgelopen jaren al vaker is voorgesteld en onderzocht, maar waartoe mijn ambtsvoorgangers na afweging van voor en nadelen, zowel in juridische termen als waar het betreft de praktische haalbaarheid uiteindelijk niet voor hebben gekozen.

Het juridisch instrumentarium is inmiddels veranderd met de inwerkingtreding van de Wet computercriminaliteit. Zoals bekend, voorziet die wet in een sterk geclausuleerde bevoegdheid tot het op afstand en heimelijk binnendringen van een geautomatiseerd werk met het oog op het uitvoeren van specifieke opsporingshandelingen met betrekking tot elektronische gegevens. Dit zou het achterhalen van wachtwoorden en inlogcodes kunnen omvatten, waarmee specifieke versleutelde bestanden kunnen worden ontsleuteld. Als het gaat om ernstige strafbare feiten, en als er geen andere mogelijkheid is, kan deze "nieuwe bevoegdheid" de opsporing helpen om te gaan met het probleem van door versleuteling ontoegankelijke gegevens.

In reactie op de vraag over (on)mogelijkheden met betrekking tot een eventuele ontsleutelplicht worden er, in navolging van wat voorgaande ministers van JenV meldden, overwegend juridische, praktische en technische bezwaren bij een dergelijk bevel gezien. Deze bezwaren zijn reeds tijdens de behandeling van de Wet computercriminaliteit III aan de orde gekomen, en zijn onverminderd valide. Ten eerste is het decryptiebevel moeilijk te verenigen met het nemo tenetur-beginsel (het recht van een verdachte om zichzelf niet te belasten).[1] Hoewel prof. Koops in het WODC rapport getiteld "*Het decryptiebevel en het nemotenetur-beginsel*" tot de conclusie kwam dat een eventueel decryptiebevel niet per definitie in strijd is met het nemotenetur-beginsel, is het zeer de vraag of er een *effectief* decryptiebevel denkbaar is dat verenigbaar is met dit recht. Met name de strafbedreiging is een aandachtspunt. Zo heeft de Afdeling advisering eerder gewezen op jurisprudentie van het EHRM over de druk op terrorismeverdachten om informatie te verstrekken. Volgens het EHRM was de dreiging bij terrorismeverdachten met een gevangenisstraf van 6 maanden om informatie te verstrekken zodanig, dat het recht om zichzelf niet te belasten in de kern was aangetast.[2] Ook prof. Koops stelt in zijn rapport dat in de meeste gevallen waarin het EHRM het aanvaardbaar heeft geacht om onder strafbedreiging medewerking af te dwingen, de dwang uit (niet al te hoge) boetes dan wel maximaal twee dagen gevangenisstraf bestond. Dit betekent dat de maximale strafbedreiging op het weigeren te voldoen aan een eventueel decryptiebevel zeer laag zal zijn ten opzichte van de maximale strafbedreiging voor het achterliggende gronddelict. Dit zal calculerend gedrag van de verdachte in de hand werken. Een verdachte kan dan eerder kiezen voor een veroordeling voor het weigeren te voldoen aan een decryptiebevel dan voor een veroordeling op grond van bijvoorbeeld het bezit van kinderpornografie.

[1] Dit beginsel vloeit voort uit art. 6 EVRM ("right to a fair trial").

[2] EHRM 21 december 2000, Heaney en McGuinness t. Ierland, nr. 34720/97. EHRM 21 december 2000, Quinn t. Ierland, nr. 36887/97.

Naast de spanning met het nemo tenetur-beginsel spelen er nog andere bezwaren. Zo zal het, om te komen tot een veroordeling op grond van het weigeren te voldoen aan een decryptiebevel, noodzakelijk zijn dat bij de verdachte sprake is van opzet. Het College van Procureurs-Generaal en de Nederlandse Vereniging voor Rechtspraak hebben gewezen op de moeilijke bewijslevering ten aanzien van het opzet waardoor met de strafbepaling moeilijk zal kunnen worden gewerkt. Het College heeft opgemerkt dat in "verreweg de meeste gevallen het bewijs van het opzet niet zal zijn te leveren". De verdachte hoeft bijvoorbeeld immers maar te stellen dat hij zich de sleutel niet kan herinneren. Voorts is de situatie denkbaar waarin de verdachte het wachtwoord wel verstrekt maar slechts tot een bepaald deel van het geheugen van het geautomatiseerd werk, waarin alleen 'onschuldige' bestanden zitten (het zgn. 'non-hidden volume') en daarmee voldoet aan het decryptiebevel. Terwijl de incriminerende bestanden kunnen worden opgeslagen in het zgn. 'hidden volume' van het geautomatiseerd werk, waarvan het bestaan niet bewezen kan worden. Om die redenen stelt ook prof. Koops in het eerder genoemde WODC rapport dat juist voor de doorgewinterde zedendelinquenten – voor wie een eventueel decryptiebevel juist bedoeld is –een decryptiebevel weinig effectief zal zijn. Zowel het openbaar ministerie als de politie onderschrijven deze bezwaren waardoor in de opsporingspraktijk evenmin de wens bestaat om een decryptiebevel te introduceren.

Nadat de mogelijke invoering van een decryptiebevel opnieuw is overdacht, zoals hiervoor aangegeven, blijft het standpunt dat ook door eerdere ministers van JenV is ingenomen: de minister van JenV overweegt niet om een decryptiebevel in te voeren. Vooralsnog kunnen politie en justitie met het oog op de opsporing van ernstige misdrijven in specifieke gevallen toegang verkrijgen tot versleutelde gegevens met behulp van de "nieuwe" bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk (art. 126nba Sv). In het Regeerakkoord is afgesproken dat deze nieuwe bevoegdheid 2 jaar na inwerkingtreding van de Wet computercriminaliteit III (per 1 maart jl.) wordt geëvalueerd. Uit die evaluatie zal blijken of de nieuwe bevoegdheid in voldoende mate doeltreffend en effectief is, onder andere bij het verkrijgen van toegang tot versleutelde elektronische gegevens.