Het decryptiebevel en het nemo-teneturbeginsel

Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?

Bert-Jaap Koops

Dit is de samenvatting van een rapport geschreven in opdracht van het Ministerie van Veiligheid en Justitie. Het rapport, B.J. Koops (2012), *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Tilburg/Den Haag: TILT/ WODC, oktober 2012, is beschikbaar op http://www.wodc.nl/publicaties/.

Samenvatting

Achtergrond en vraagstelling

Wanneer een misdadiger gegevens op zijn computer of zijn communicatie versleutelt, wordt het lastig voor de opsporing om informatie te verzamelen via computeronderzoek en aftappen. Een van de mogelijke oplossingen voor dit probleem is het dwingen van aangewezen personen om versleutelde gegevens te ontsleutelen. Nederland heeft daartoe al bij de Wet computercriminaliteit (1993) een ontsleutelplicht ingevoerd. Het bevel tot ontsleuteling kan momenteel echter niet aan verdachten worden gegeven. De Nederlandse wetgever is er tot nu toe van uitgegaan dat een ontsleutelbevel in strijd is met het beginsel dat verdachten niet aan hun eigen veroordeling hoeven mee te werken, oftewel het nemo-teneturbeginsel. Volgens vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) is het nemo-teneturbeginsel een kernonderdeel van het recht op een eerlijk proces. De precieze reikwijdte van het beginsel is echter niet volledig uitgekristalliseerd en in wetgeving en rechtspraak zijn de nodige uitzonderingen op het beginsel geaccepteerd.

In een onderzoek uit 2000 (B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*) werd geconcludeerd dat een ontsleutelplicht voor verdachten een ingrijpende inbreuk maakt op het beginsel, die niet kon worden gerechtvaardigd door het opsporingsbelang. Sinds 2000 is er echter het nodige gebeurd op het vlak van technologie en rechtspraak over het nemo-teneturbeginsel. Ook is in de Tweede Kamer, naar aanleiding van de Amsterdamse zedenzaak rond Robert M., de vraag opgeworpen of niet alsnog een ontsleutelplicht voor verdachten kan worden ingevoerd. Tegen die achtergrond wordt in dit rapport als hoofdvraag onderzocht in hoeverre, gelet op de ontwikkelingen sinds 2000, een decryptiebevel – een bevel tot het verlenen van medewerking aan het toegankelijk maken van beveiligde gegevens – verenigbaar is met het nemo-teneturbeginsel. Deze vraag is beantwoord aan de hand van literatuuronderzoek, analyse van de buitenlandse rechtsontwikkeling en vijf semi-gestructureerde interviews met deskundigen uit de opsporingspraktijk.

Het nemo-teneturbeginsel

De reikwijdte van het nemo-teneturbeginsel is in de rechtspraak van het Europees Hof (EHRM) niet significant veranderd sinds 2000. De kern van het beginsel ligt nog altijd in de verklaringsvrijheid: op een verdachte mag soms enige druk worden uitgeoefend om verklaringen te verkrijgen, maar die druk mag niet groot zijn en moet omkleed zijn met procedurele waarborgen, zoals de toegang tot een advocaat en het informeren van de verdachte welke gevolgen zijn houding kan hebben op zijn procesgang. Buiten het afleggen van verklaringen geldt dat naarmate de verdachte actiever moet meewerken, en met name als hij daarbij een intellectuele inspanning moet verrichten, een dwang om mee te werken eerder in strijd komt met nemo tenetur. Een ontsleutelplicht ligt dicht aan tegen het afleggen van een verklaring, omdat het wachtwoord in het hoofd van de verdachte zit en niet kan worden verkregen zonder diens

(intellectuele) inspanning. Een decryptiebevel voor verdachten maakt daarom, net als in 2000, nog steeds inbreuk op het nemo-teneturbeginsel.

Deze inbreuk kan echter gerechtvaardigd zijn – er zijn immers uitzonderingen op het beginsel mogelijk. Het Europees Hof kijkt naar vier factoren die tezamen bepalen of een afgedwongen medewerking wel of niet aanvaardbaar is in het licht van het nemo-teneturbeginsel:

1. de aard en mate van dwang;
2. het gewicht van het publiek belang;
3. de aanwezigheid van relevante waarborgen in de procedure;
4. de manier waarop het afgedwongen materiaal wordt gebruikt.

Naarmate de dwang om mee te werken groter is en het afgedwongen materiaal een zwaardere rol heeft bij het bewijs, zal het publiek belang van afgedwongen medewerking des te groter moeten zijn en zullen er meer waarborgen moeten zijn voor rechtsbescherming. Bij een lagere mate van dwang of een ondergeschikte rol van afgedwongen bewijsmateriaal zal een ontsleutelplicht echter eerder de toets doorstaan.

Ook in de Nederlandse rechtsontwikkeling is de rol van het nemo-teneturbeginsel grotendeels hetzelfde gebleven als in 2000. Een decryptiebevel voor verdachten zou nog steeds afwijken van het systeem van de Nederlandse wet, voor zover de weigering mee te werken strafbaar zou zijn. Wel blijkt uit de rechtspraak dat er goede mogelijkheden zijn om ontsleuteling aan verdachten te vragen wanneer zij zich kunnen verschonen van medewerking, vergelijkbaar met de regeling van het verhoor waarbij de verdachte mag zwijgen. De verdachte neemt dan een zeker procesrisico als hij niet meewerkt, omdat onder bepaalde omstandigheden (in situaties waarin de aanwezigheid van beveiligde bestanden duidelijk vragen oproept) de rechter zijn decryptieweigering kan gebruiken bij het bewijs, de straftoemeting of andere beslissingen ten nadele van de verdachte.

Ontwikkelingen in het buitenland

In 2000 waren er geen landen met een ontsleutelplicht voor verdachten, maar dat is inmiddels substantieel gewijzigd. In België mag het decryptiebevel niet aan verdachten worden gegeven, maar Frankrijk en het Verenigd Koninkrijk hebben wel een ontsleutelplicht voor verdachten ingevoerd. Het VK kent een uitgebreide wettelijke regeling wanneer en hoe een decryptiebevel mag worden gegeven, met diverse waarborgen voor rechtsbescherming. In Frankrijk beperkt de wettelijke regeling zich tot strafbaarstelling van het weigeren te ontsleutelen. Australië heeft een wettelijk decryptiebevel ingevoerd dat zich specifiek tot verdachten richt, terwijl in de Verenigde Staten zich een ontsleutelplicht voor verdachten uitkristalliseert in de rechtspraak, die onder bepaalde voorwaarden verenigbaar wordt geacht met (de vergelijkbare Amerikaanse variant van) het nemo-teneturbeginsel.

Uit de Britse en Amerikaanse rechtspraak komt naar voren dat het meewerken aan ontsleuteling lijkt op het afleggen van een verklaring, omdat het impliciet de band van de verdachte met het versleutelde materiaal erkent. Dit maakt inbreuk op nemo tenetur, maar die inbreuk is volgens Amerikaanse rechtspraak gerechtvaardigd a) als het een uitgemaakte zaak is om wat voor bestanden het gaat en dat de verdachte in staat is te ontsleutelen, of b) als er bewijsuitsluiting wordt beloofd voor het (belastende) materiaal dat na ontsleuteling tevoorschijn komt. In het Verenigd Koninkrijk wordt de inbreuk van het decryptiebevel op nemo tenetur aanvaardbaar geacht vanwege de vele *checks and balances* in de Britse regeling en vanwege het feit dat de zittingsrechter altijd de mogelijkheid heeft om afgedwongen bewijs, als dat belastend blijkt, terzijde te leggen. Hoewel de rechtspraak in deze landen nog in ontwikkeling is, blijkt wel dat een ontsleutelplicht voor verdachten onder omstandigheden aanvaardbaar wordt geacht, waarbij in de rechtspraak de grenzen van het nemo-teneturbeginsel nader kunnen worden bepaald. De Britse wetgeving biedt daarmee aanknopingspunten voor de Nederlandse beleidsvorming, maar de regeling kan niet rechtstreeks worden overgezet. Het Verenigd Koninkrijk heeft gekozen voor een hoge mate van dwang (er staat 2-5 jaar gevangenisstraf op het niet meewerken), die alleen kan worden gerechtvaardigd door vergaande waarborgen, waaronder de mogelijkheid van bewijsuitsluiting maar ook enkele waarborgen die Nederland niet kent, zoals een onafhankelijke toezichthouder op de opsporing.

Handhaafbaarheid en ontwikkelingen in techniek

Het gebruik van cryptografie door verdachten is sinds 2000 toegenomen, met name door versleuteling van opgeslagen gegevens. Vooralsnog lijkt het gebruik van sterke encryptie vooral voor te komen bij bepaalde kinderpornonetwerken (die vaak voorop lopen met het gebruik van 'verbergtechnieken'), maar andere groepen misdadigers zouden kunnen volgen. Een belangrijke ontwikkeling is de opkomst van 'anti-forensische' programma's, dat wil zeggen cryptoprogramma's om niet alleen bestanden te versleutelen maar ook om het bestaan van de versleutelde bestanden 'aannemelijk ontkenbaar' te maken. Bij dergelijke programma's is het moeilijk voor justitie om te bewijzen dat er überhaupt versleutelde gegevens op de harde schijf staan.

Aan de andere kant heeft justitie ook ruimere mogelijkheden dan in 2000 het geval leek, om te betogen dat een verdachte wél mogelijk belastend materiaal (zoals binnengehaalde kinderporno) op zijn computer heeft staan en in staat is te ontsleutelen, bijvoorbeeld met aanwijzingen uit een Internettap of verkeersgegevens. Ook de Britse en Amerikaanse rechtspraak toont aan dat er diverse gevallen mogelijk zijn waarin de verdachte 'iets uit te leggen heeft' als hij niet wil ontsleutelen.

Deze twee ontwikkelingen heffen elkaar niet op, maar betekenen eerder dat het sterk van de omstandigheden zal afhangen of een decryptiebevel handhaafbaar is. Anders dan in 2000 hoeft de problematische handhaafbaarheid dan ook niet te leiden tot een categorische afwijzing van een ontsleutelplicht voor verdachten; er kan eerder worden gekozen voor een wettelijke bevoegdheid die afhankelijk van de omstandigheden wel of niet kan worden gebruikt. Vermoedelijk zal een ontsleutelplicht weinig effectief zijn tegen zware en berekenende misdadigers die sowieso niet meewerken met justitie, en vermoedelijk eerder de kleinere of minder slimme misdadigers treffen. De ervaring in het Verenigd Koninkrijk is ook dat een decryptiebevel slechts in een beperkt aantal gevallen wordt opgelegd, waarbij minder dan de helft meewerkt en waarbij in vier jaar tijd slechts zes weigeraars veroordeeld zijn voor niet meewerken.

Conclusies en aanbevelingen

Uit bovenstaande bevindingen blijkt dat een decryptiebevel aan verdachten niet onverenigbaar is met het nemo-teneturbeginsel. Het hangt ervan af hoe het wettelijk wordt vormgegeven (bijvoorbeeld welke soort en mate van dwang kan worden gebruikt) en hoe het in een concreet geval wordt toegepast. Waar de studie uit 2000 concludeerde dat Nederland geen ontsleutelplicht voor verdachten zou moeten invoeren, omdat die alleen effectief zou zijn bij een sterke mate van dwang maar daarmee een onaanvaardbare inbreuk op het nemo-teneturbeginsel zou opleveren, ligt de situatie nu enigszins anders. De ontwikkelingen in het buitenland en in de techniek suggereren dat een ontsleutelplicht voor verdachten wel verenigbaar is met het nemo-teneturbeginsel en – weliswaar voor een beperkt aantal gevallen – effectief zou kunnen zijn, mits de wettelijke regeling en uitvoering met voldoende waarborgen zijn omkleed.

Mocht de wetgever, zoals in het VK, voor een ontsleutelplicht met een hoge mate van dwang kiezen, dan zullen er aanzienlijke waarborgen moeten worden getroffen, zoals een schriftelijk bevel, toegang tot een advocaat, een redelijke bewijsvoeringslast, een discretionaire bevoegdheid voor de rechter om zelfbelastend materiaal alsnog uit te sluiten van bewijs, en toezicht op de praktijk door een onafhankelijk toezichthouder. Het is ook denkbaar om een lagere mate van dwang te kiezen door een weigering te ontsleutelen niet zelfstandig strafbaar te stellen, maar door de rechter te laten meewegen bij beslissingen over bewijs of strafoplegging. Daarnaast kan justitie in voorkomende gevallen ook overwegen om een verdachte bewijsuitsluiting toe te zeggen als hij ontsleutelt; het ontsleutelde materiaal kan dan niet tegen de verdachte worden gebruikt, maar wel tegen anderen of bijvoorbeeld voor het identificeren (of uitsluiten) van slachtoffers, wat in kinderpornozaken een belangrijk aspect kan zijn.

Wanneer de verschillende opties in samenhang wordt bekeken, zijn er grofweg drie mogelijkheden voor de Nederlandse wetgever ten aanzien van de ontsleutelplicht voor verdachten.

1. **De huidige situatie handhaven**. Een ontsleutelbevel mag dan niet worden gegeven aan verdachten, maar politie en justitie kunnen verdachten wel verzoeken om vrijwillige medewerking. Onder omstandigheden kan de rechter binnen de huidige wet tot op zekere hoogte rekening houden met het feit dat een verdachte niet ontsleutelt, in de bewijsconstructie of bij de strafoplegging.

2. **Een decryptieregeling conform de regeling van het verhoor**. De praktijk van het vragen om ontsleuteling wordt geformaliseerd, in de wet of in lagere regelgeving, waarbij het verzoek wordt genormeerd op dezelfde wijze als het verhoor (art. 29 Sv). Dit zal voor de praktijk op zich niet veel verschil maken, maar het past beter in het systeem van de wet omdat het meewerken aan ontsleuteling meer lijkt op het afleggen van een verklaring dan op het uitleveren van voorwerpen. De normering van een decryptieverzoek conform de regeling van het verhoor heeft als voordeel dat de bijbehorende waarborgen van toepassing zijn, zoals de toegang tot een advocaat en de cautie. Dit kan de mogelijkheden versterken om binnen de grenzen van het nemo-teneturbeginsel negatieve conclusies te verbinden aan de proceshouding van de niet-meewerkende verdachte.
3. **Een decryptiebevel aan verdachten met strafbaarstelling van weigering.** Het niet-meewerken aan een decryptiebevel wordt strafbaar gemaakt op basis van artikel 184 Sr (maximaal drie maanden gevangenisstraf) of met een zelfstandige strafbaarstelling met een hogere maximumstraf. Vanuit de EHRM-eisen zal een zwaardere straf eerder aanvaardbaar zijn als die zich beperkt tot specifieke delicttypen waarbij versleuteling aantoonbaar een groot maatschappelijk probleem veroorzaakt. Een dergelijke wetswijziging maakt een grotere inbreuk op het nemo-teneturbeginsel dan de vorige mogelijkheid en zal met veel waarborgen moeten worden omkleed en zorgvuldig moeten worden gemotiveerd. Om het recht zichzelf niet te belasten niet van zijn betekenis te ontdoen, zal daarbij in elk geval altijd de zittingsrechter de mogelijkheid moeten hebben om alsnog de onder dwang ontsleutelde gegevens uit te sluiten van het bewijs.

De analyse van de EHRM-rechtspraak en het systeem van de Nederlandse wet wijst uit dat de tweede mogelijkheid te prefereren is boven de eerste mogelijkheid. Anders dan in 2000 hoeft de derde mogelijkheid echter niet op voorhand te worden afgewezen. Er is enige ruimte binnen de grenzen van het nemo-teneturbeginsel om een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. De effectiviteit daarvan zal gezien de zware eisen niet groot zijn, maar kan in incidentele gevallen wel aanwezig zijn. Het is daarom vooral een beleidsafweging of een strafbaarstelling van decryptieweigering – die binnen de grenzen van het nemo-teneturbeginsel mogelijk is als er voldoende waarborgen zijn – te prefereren is boven een decryptieregeling conform de regeling van het verhoor.

Gegeven deze conclusie, verdient het aanbeveling dat de wetgever een hernieuwde afweging maakt of en onder welke omstandigheden een decryptiebevel aan verdachten zou kunnen worden gegeven. In elk geval zou de wetgever serieus de tweede mogelijkheid moeten overwegen. De keuze tussen de tweede en derde mogelijkheid (oftewel tussen weinig of veel dwang) komt vooral neer op een beleidsafweging. Het gaat daarbij niet om een zwart-wit-afweging tussen legitimiteit en effectiviteit; belangrijk is vooral dat bij een ontsleutelplicht voor verdachten een zorgvuldige combinatie wordt gekozen van uit te oefenen dwang, de manier waarop afgedwongen materiaal wordt gebruikt en procedurele waarborgen, en dat vanuit het publiek belang zorgvuldig wordt gemotiveerd waarom een gekozen regeling een aanvaardbare inbreuk op het nemo-teneturbeginsel oplevert.

Bij de beleidsafweging is het belangrijk om geen wonderen te verwachten van een decryptiebevel. Het zal alleen effect kunnen sorteren in een beperkt aantal gevallen waarin een verdachte duidelijk ‘iets uit te leggen heeft’ en waarin er al veel bewijs tegen de verdachte bestaat. De wetgever moet ook terughoudend zijn met een instrumentele inzet van het strafrecht; de bedoeling is immers om misdadigers te straffen voor feiten die zij hebben begaan, niet om verdachten te straffen voor het niet meewerken aan bewijsgaring. Verder verdient het aanbeveling om bij de beleidsvorming rond de ontsleutelplicht te kijken naar het bredere perspectief van problemen waar de digitale opsporing tegenaan loopt (zoals cloud computing) en naar alternatieve manieren om het probleem van encryptie aan te pakken, zoals Trojaanse politiepaarden die wachtwoorden of sleutels heimelijk kunnen onderscheppen.