Reactie Vrijschrift op het voorstel voor de Wet Computercriminaliteit III

Inleiding

Over Vrijschrift

Vrijschrift werkt aan bewustwording van de economische en maatschappelijke betekenis van vrije kennis en cultuur voor onze samenleving. Vrijschrift heeft een beschermende en bevorderende rol voor informatievrijheid.

Adres:

Stichting Vrijschrift

Trekwei 7, 8711 GR Workum

Opbouw

Deze positiebepaling is verdeeld in algemene observaties over het wetsvoorstel in zijn algemeenheid en de vier nieuwe bevoegdheden die hiermee worden geïntroduceerd:

- heimelijk binnendringen in een geautomatiseerd werk;
- ontoegankelijkmaking van gegevens of afstand;
- decryptiebevel aan de verdachte;
- heling van gegevens.

Deze worden bezien in hun algemeenheid en per bevoegdheid in hun verhouding tot de uitingsvrijheid, de vrijheid om informatie te vergaren en overige grondrechten.

Algemene observaties

In zijn algemeenheid valt op dat geen van de voorgestelde bevoegdheden in reikwijdte een relatie hebben met computercriminaliteit in de zin van criminaliteit die betrekking heeft op computersystemen of die zonder computersystemen niet gepleegd zou kunnen worden. Dit maakt nut en noodzaak van de voorgestelde bevoegdheden moeilijk te beoordelen en alleen al daarom roept dit vragen van proportionaliteit op. De Memorie van Toelichting (MvT) begint evenwel met:

"Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken."

Een belofte die helaas niet waargemaakt wordt, het valt te voorzien dat het in de praktijk vooral om inzet bij andere criminaliteit dan computercriminaliteit zal gaan. De MvT spreekt met name over misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Vanuit de gedachte dat wat offline geldt ook online moet gelden lijkt het logisch dat dat de waarborgen bij de inzet van de voorgestelde bevoegdheden aansluiten bij die voor de bijzondere opsporingsbevoegdheden voor bijvoorbeeld georganiseerde criminaliteit.

Iedere analogie met de offline wereld gaat echter per definitie mank nu het in het bijzonder om geautomatiseerde werken gaat waarvan de locatie en de beoogde inzet onbekend is. Het wetsvoorstel doet dit onvoldoende recht. Het is bijvoorbeeld zeer wel denkbaar dat een computer

waar de bijzondere bevoegdheden uit dit wetsvoorstel tegen worden ingezet eigendom is van een organisatie te goeder trouw maar door kwaadwillenden overgenomen is. Dit kan betekenen dat een computer die enerzijds een vitale rol speelt in bijvoorbeeld een ziekenhuis anderzijds hulpmiddel is bij ernstige misdrijven. Het is dan heel wel denkbaar dat het handelen van opsporingsambtenaren juist leidt tot onoverzienbare "collateral damage" die mogelijk evenveel of meer maatschappelijke impact heeft dan het misdrijf. Vooropgesteld dat de voorgestelde bevoegdheden überhaupt in termen van proportionaliteit verdedigbaar zijn is het alleen al vanwege deze risico's zonder meer noodzakelijk dat zij met meer waarborgen omkleed worden dan bij de reeds bestaande bijzondere opsporingsbevoegdheden het geval is. Het gaat hier om vergaande inbreuken op de persoonlijke levenssfeer, de uitingsvrijheid en het recht op een eerlijk proces. De afweging van de betrokken belangen kan niet aan een officier van justitie worden overgelaten, zelfs niet in dringende gevallen, maar vereist rechterlijk toezicht.

Vrijschrift betwijfelt echter in zijn algemeenheid of de voorgestelde bevoegdheden wel proportioneel kunnen zijn, ongeacht het niveau van de waarborgen waarmee zij omkleed zijn.

Heimelijk binnendringen van een geautomatiseerd werk

Het voorstel lijkt op meerdere gedachten te hinken met betrekking tot het onderzoek in een geautomatiseerd werk. Enerzijds wordt er gesproken van een noodzaak vanwege het niet langs andere wegen kunnen achterhalen van de identiteit van gebruikers of de locatie van een computer, anderzijds zijn de gegeven voorbeelden meerdere malen duidelijk op andere situaties van toepassing. Zo is bijvoorbeeld in het geval van een smartphone die door een crimineel gebruikt wordt duidelijk wie de gebruiker is en zijn op basis van de verkeersgegevens die voorhanden zijn bij de netwerkexploitant (waar in de praktijk veelvuldig gebruik van wordt gemaakt) de locatie én de communicatiepartners van de verdachte bekend.

Zoals al in zijn algemeenheid opgemerkt gaat het wetsvoorstel voorbij aan de eventuele onbedoelde neveneffecten. Het voorstel maakt onvoldoende duidelijk waarom de voordelen van een zó ingrijpend optreden van opsporingsdiensten opwegen tegen de nadelen, al was het maar omdat veel van de nadelen in het geheel niet genoemd worden.

Daarnaast worden opsporingsdiensten belanghebbenden bij het in stand houden van beveiligingsproblemen in (consumenten)apparatuur en wellicht zelfs actieve afnemer op de reeds bestaande zwarte markt voor beveiligingslekken.

Ook gaat het wetsvoorstel onvoldoende in op de mate waarin computers, in het bijzonder smartphones, een dusdanig integraal onderdeel uitmaakt van het leven van burgers dat een dergelijke heimelijke observatie een veel grotere inbreuk op de persoonlijke levenssfeer maakt dan een traditionele inkijkoperatie. Een smartphone heeft een verdachte immers vrijwel altijd bij zich en bevat zijn of haar e-mail geschiedenis, SMS-berichten, bezochte locaties, voicemailberichten en veelal ook alle ingangen in sociale media.

Daar komt nog bij dat het binnendringen, zelfs verkennend, van een computersysteem niet mogelijk is zonder dit systeem te wijzigen. Zeker niet in het geval van het heimelijk aftappen van communicatie vereist dit diepgaande veranderingen in computersystemen. Wie zoveel aan de situatie in een computersysteem verandert zal ook bewijsmateriaal op die computer kunnen manipuleren. Als zodanig is het een middel dat zijn doelen voorbij lijkt te schieten.

Ontoegankelijk maken van gegevens op afstand

Het ontoegankelijk maken van gegevens op afstand is gelijk te stellen met het vernietigen van bewijsmateriaal, zowel belastend als ontlastend. Zelfs als het gepaard gaat met het maken van een kopie voor vervolgingsdoeleinden is het door het buiten de feitelijke macht brengen van de verdachte van gegevens intrinsiek onverenigbaar met diens recht op verdediging.

Zeker met het oog op de uitingsvrijheid is het onverteerbaar dat het voorstel zwijgt over de situatie die ontstaat in het geval gegevens ontoegankelijk zijn gemaakt en vervolgens het strafrechtelijk onderzoek wordt gestaakt of opgeschort. Dit zou de facto in censuur uitmonden die onverenigbaar is met art. 10 EVRM.

Decryptiebevel aan de verdachte

De strafbaarstelling van de weigering van een verdachte van het produceren of stelselmatig verspreiden van kinderporno om een decryptiesleutel af te staan is, hoe onsympathiek deze groep van criminelen ook is, per definitie onverenigbaar met het beginsel dat een verdachte niet aan zijn of haar eigen veroordeling hoeft mee te werken. Daar komt nog bij dat het in de praktijk onmogelijk kan zijn aan een dergelijk bevel gehoor te geven. Bijvoorbeeld omdat de data die voor versleutelde data wordt gehouden niet versleuteld is maar statistische ruis en als zodanig niet te onderscheiden is van versleutelde data. Op vrijwel iedere hedendaagse computer zijn bijvoorbeeld zogenaamde entropiepools aanwezig van dergelijke ruis om willekeurige getallen te kunnen genereren die een rol spelen bij de normale beveiliging van internetverbindingen etc.

Heling van gegevens

Het strafbaarstellen van de heling van gegevens lijkt ingegeven door een incident: de openbaarmaking van zeer persoonlijke foto's van een bekende Nederlander door haar buurman die op haar huisnetwerk was binnengedrongen. Voorzover incidenten al tot wetgeving moeten leiden is het zeer de vraag of dit geen goede aanleiding was geweest om bijvoorbeeld het lekken van persoonsgegevens niet strafbaar te stellen. In dit voorstel wordt en passant een niet onbelangrijke pijler onder de (onderzoeks)journalistiek weggeslagen: informatie die als gevolg van een strafbaar feit voorhanden is gekomen. Men denke bijvoorbeeld aan klokkenluiders die, al dan niet terecht, als staatsgeheime informatie geclassificeerde informatie aan een journalist ter hand stellen. De praktijk leert dat zelfs indien aangenomen wordt dat er in zo'n scenario sprake is van een strafuitsluitingsgrond, zoals de MvT suggereert, een eventueel strafrechtelijk onderzoek zeer belastend is voor de journalist in kwestie. Hier komt nog bij dat de beroepsgroep van journalist steeds diffuser wordt.

Los hiervan kan de vraag gesteld worden of deze strafbaarstelling zich ook uitstrekt tot gegevens die afkomstig zijn van een strafbaar feit in een andere jurisdictie. Het voorstel zwijgt hierover.