Redactioneel

arsaequi.nl/maandblad AA20230395

GEKRAAKTE CRYPTOCOMMUNICATIE ALS BEWIJS IN STRAFZAKEN

Bram Groothoff & Yong Yong Hu

Het OM gebruikt de laatste jaren in toenemende mate ontsleutelde cryptocommunicatie als bewijs in grote strafzaken. Onderzoeken naar servers met versleutelde berichten worden steevast gepresenteerd met de implicatie dat de servers enkel berichten van criminelen bevatten. Maar klopt deze redenering: worden systemen voor versleutelde berichten enkel door criminelen gebruikt? En rechtvaardigt dat deze vorm van opsporing?

PGP staat voor *Pretty Good Privacy.* Dit systeem biedt gebruikers de mogelijkheid om versleutelde (mail)berichten te sturen via cryptotelefoons. PGP was daarmee het eerste bekende systeem voor cryptotelefoons. Tot 2016 waren deze telefoons nauwelijks te kraken. Daar kwam verandering in toen het Team High Tech Crime, een speciale eenheid van de Landelijke Recherche, twee servers in Costa Rica en Canada wist te ontsleutelen en zo toegang kregen tot meer dan een miljoen PGP-berichten (*Om.nl* 9 maart 2017). Nadien ondergingen verschillende andere aanbieders van versleutelde cryptocommunicatie eenzelfde lot als PGP.

De ontsleutelde berichten werden vervolgens gebruikt als bewijsmateriaal in strafzaken. Vast staat dat dergelijke berichten als bewijsmateriaal mogen worden gebruikt. De Hoge Raad heeft dat bepaald in zijn arrest van 28 juni 2022 (ECLI:NL:HR:2022:900) De berichten hebben geleid tot een veelvoud aan succesvolle vervolgingen voor ernstige strafbare feiten. Zo vormen de berichten een belangrijk onderdeel van het bewijs tegen Omar L. (ECLI:NL:GHARL:2021:11610) voor het aansturen van meerdere liquidaties. Doordat L. en zijn medeverdachten (onterecht) vertrouwden op de versleuteling van hun berichten kon de gang van zaken rond de moorden van minuut tot minuut gereconstrueerd worden. Deze zaak is exemplarisch voor veel andere strafzaken waarin bewijs middels cryptocommunicatie centraal staat en illustreert de enorme waarde die deze bewijsvergaring kan hebben bij de bestrijding van ernstige criminaliteit.

Er is echter ook kritiek op deze vorm van opsporing, die ook wel bulkbevoegdheden worden genoemd (Galič *TBS&H* 2022, afl. 2). Kenmerkend voor deze opsporingsmethode is dat er eerst een enorme hoeveelheid data wordt verzameld en vervolgens verdachten worden gevonden door de communicatie te doorzoeken. Hierbij hanteert justitie een veronderstelde verdenking voor alle gebruikers van cryptotelefoons. Het feit dat het gaat om dure telefoons met ingewikkelde beveiligingssystemen en dat dit soort telefoons vaak bij criminelen worden aangetroffen wijzen tezamen op een predispositie van de gebruikers om misdrijven te plegen.

De keerzijde van de medaille is dat ook burgers die extra gesteld zijn op hun privacy – denk bijvoorbeeld aan journalisten – gebruikmaken van cryptotelefoons. Het is van groot belang dat journalisten veilig kunnen communiceren met bronnen. Vanwege hun taak als *public watchdog* krijgen ze vaak vertrouwelijke en/of belastende informatie van andere burgers en daarbij is het waarborgen van de privacy cruciaal. Daarnaast is de veronderstelling – een overgrote meerderheid van de gebruikers is betrokken bij misdrijven – moeilijk te bewijzen (Galič *TBS&H* 2022, afl. 2). Tevens rijst de vraag wanneer dat wel lukt: hoe groot moet het percentage criminele gebruikers zijn om een algemene veronderstelde verdenking voor de hele dataset aan te nemen? Tegelijkertijd kan de waarde van het bewijs niet onderschat worden. Het ontsleutelde berichtenverkeer heeft geleid tot succesvolle vervolgingen in een groot aantal strafzaken die gaan om ernstige misdrijven.

Wanneer het gaat om het strafproces zelf, leidt deze vorm van opsporing ook tot uitdagingen, in het bijzonder voor de advocaten die de verdachten bijstaan. De zoekmachines die de politie gebruikt om verdachte berichten te zoeken, is niet gebruiksvriendelijk voor advocaten die ontlastende berichten zoeken in de database. Het is lastig in te schatten of het OM al het beschikbare bewijs heeft opgenomen in het dossier. Bovendien oordeelde de Hoge Raad in het hiervoor aangehaalde arrest dat het OM in beginsel geen inzage in de gehele dataset aan de verdediging hoefde te geven. Hiermee wordt de verdediging in dit soort zaken behoorlijk bemoeilijkt.

Al met al is de conclusie gerechtvaardigd dat ontsleutelde cryptocommunicatie van onschatbare waarde is voor de opsporing en vervolging van ernstige criminaliteit, maar dat tegelijkertijd de redenering die schuilgaat achter de veronderstelde verdenking van alle gebruikers van cryptotelefoons vragen oproept. Hetzelfde geldt voor de beperkte mogelijkheden voor de verdediging om de betrouwbaarheid van de berichten te controleren. De komende jaren zal de rechtspraktijk op dit vlak nog voor de nodige uitdagingen komen te staan.