ANNOTATIE

Akgün t. Turkije (EHRM, 19699/18) – Gebruik van cryptocommunicatieapplicatie als voldoende grond voor redelijk vermoeden van schuld

D.A.G. van Toor

Annotatie bij Europees Hof voor de Rechten van de Mens, 20-07-2021, ECLI:CE:ECHR:2021:0720JUD001969918 (EHRC-2021-0202)

1. Na de mislukte couppoging in Turkije zijn vele mensen opgepakt, vervolgd en veroordeeld voor deelname aan een terroristische organisatie (in dit geval de *Fetullahist Terrorist Organization* (afgekort met FETÖ), zoals de Turkse autoriteiten de organisatie van aanhangers van de Gülen-beweging noemt). Al eerder publiceerde *EHRC Updates* annotaties over klachten van mensenrechtenschendingen naar aanleiding van het optreden van de autoriteiten tegen de vermeende organisatie en haar leden die verantwoordelijk zou zijn voor de couppoging.[1] In zowel de geannoteerde zaken *Hakan Bas* en *Sabuncu e.a.*[2] als de onderhavige zaak gaat het om de vraag of het voorarrest van vermeende leden van de FETÖ gerechtvaardigd was. In de onderhavige zaak staat enkel die vraag centraal, en dan vooral of klagers gebruik van de cryptocommunicatieapplicatie *ByLock* bewezen kan worden en, zo ja, of dat voldoende is om een redelijk vermoeden van schuld in de zin van art. 5 lid 1 sub c EVRM aan te nemen.[3] Deze vraag is in de eerdere annotaties niet aan bod gekomen, terwijl die absoluut relevant is gezien de vele ontmantelingen van cryptocommunicatieaanbieders de laatste tijd.[4]

2. In de onderhavige zaak wordt klager op 17 oktober 2016, zo'n drie maanden na de couppoging, aangehouden en verhoord vanwege een gerezen "verdenking" dat hij – een oud

politieagent – lid is van FETÖ. Hij wordt direct ondervraagd over het gebruik van *ByLock*, maar verklaart die applicatie nooit te hebben gebruikt en hij ontkent elke betrokkenheid bij de couppoging (par. 10-11). Hij wordt in voorarrest genomen enkel op de basis van het gebruik van de cryptocommunicatieapplicatie (par. 16; 130).

3. Volgens de Turkse autoriteiten wordt *ByLock* namelijk alleen door leden van de FETÖ gebruikt. Dit wordt bevestigd na onderzoek verricht door de *High Council of Judges and Prosecutors* (HSYK) (par. 38) en de Nationale Veiligheidsdienst (MIT) (par. 53). Twee IT-consultatiebedrijven beschrijven verder dat *ByLock* voor een besloten groep is ontwikkeld (par. 57 e.v.). Daarnaast blijkt uit de analyse van de applicatie dat de Turkse taal is gebruikt in de broncode, dat in een bepaalde periode voorafgaand aan de couppoging veelvuldig is gegoogled naar *ByLock* in Turkije, dat de applicatie alleen via een *Virtual Private Network* (VPN) toegankelijk was waardoor de applicatie een hoge mate van identiteitsafscherming biedt en dat *ByLock* op geen enkele wijze commercieel succes heeft getracht te bereiken (par. 57 e.v.). Dit alles leidt de autoriteiten ertoe te concluderen dat *ByLock* een cryptocommunicatieproduct is *van* en *voor* FETÖ-leden. Deze analyse wordt geaccepteerd door het Turkse Constitutionele Hof (par. 83 e.v.), dat daarmee de deur opent om het *enkele* gebruik van *ByLock* als voldoende redengevend te achten voor deelname aan FETÖ.

4. Klager zou *ByLock* bijna 5.000 maal hebben geraadpleegd in de periode van augustus 2014 tot mei 2015 (par. 29) (en de oplettende lezer merkt dat dit meer dan een jaar voor de couppoging is). Daarmee is voor de autoriteiten zonneklaar dat hij onderdeel uitmaakt van FETÖ. De Turkse overheid stelt zich in Straatsburg dan ook op het standpunt dat het enkele gebruik van *ByLock* voldoende grond voor het voorarrest van klager vormt (par. 130) en gaat uitvoering in op de analyse van de applicatie (par. 133 e.v.), zoals die is geaccepteerd door het Turkse Constitutionele Hof.

5. Gezien de context van de onderhavige zaak – de al veelvuldig bekritiseerde willekeurige arrestaties en veroordelingen van vermeende leden van FETÖ door de Turkse autoriteiten – is het lastig om de kern van de rechtsvraag serieus te nemen. Er is zoveel onduidelijk over *ByLock* en er gaan geruchten de ronde dat de gebruikersdata van *ByLock* zijn gemanipuleerd[5] dat het, gezien de situatie in Turkije, moeilijk is voor te stellen dat alle opgepakte personen, die *ByLock* gebruikten, terroristen zijn. Dat laat echter onverlet dat de rechtsvraag van groot belang is. Is, en zo ja onder welke voorwaarden, is het gebruik van een cryptocommunicatieapplicatie of -product voldoende voor het aannemen van een redelijk vermoeden van schuld?

6. Het EHRM lijkt dit niet in algemene zin uit te willen sluiten (par. 167). Versleutelde communicatie speelt een grote rol binnen criminele netwerken en het EHRM is zich bewust

van de realiteit dat opsporingsdiensten wereldwijd inzetten op het ontmantelen van aanbieders van *deviant security* producten en diensten,[6] zoals de overname en ontmanteling van *Encochat*[7] en *SkyECC*[8] en de undercoveroperatie *ANOM*[9] laten zien. Het Hof stelt dan ook dat het aanpakken van communicatiestromen een belangrijke tool is in de strijd tegen georganiseerde criminaliteit (par. 167). *Onvoldoende* voor het aannemen van een redelijk vermoeden van schuld is echter het enkele downloaden van een cryptocommunicatie*applicatie* (par. 173). Ten minste moet vaststaan dat de applicatie wordt *gebruikt* en daarnaast dienen nog andere aanwijzingen aanwezig te zijn dat de gebruiker betrokken is bij criminaliteit, zoals bijvoorbeeld de inhoud van de ontsleutelde berichten (par. 173). Omdat het in de onderhavige zaak om een *applicatie* gaat, en niet om een *product* zoals een *cryptophone* – een speciaal voor versleutelde communicatie geprepareerde *smartphone*, waarmee niets anders kan worden gedaan dan versleutelde berichten versturen en ontvangen –, is het onduidelijk of het voorgaande voor beide geldt.

7. Voor applicaties die downloadbaar zijn via de gangbare portalen staat namelijk niet bij voorbaat vast dat die alleen beschikbaar zijn voor besloten groepen. Dit is anders voor producten of diensten waarvoor flink, in cash, moet worden betaald (*Encrochat*) of die alleen verkrijgbaar zijn op voorspraak van andere (criminele) bezitters (*ANOM*). De uitgangspositie van een openbare applicatie zoals *ByLock* is daarmee anders, en het is logisch dat het EHRM meer bewijzen verlangt voordat kan worden geconcludeerd dat het enkele gebruik van een openbare applicatie voldoende is voor een redelijk vermoeden van schuld.

8. Hiermee is niet gezegd dat het uitgangspunt moet zijn dat het gebruik van de eerder genoemde *deviant security*-producten of diensten *ipso facto* tot het aannemen van een redelijk vermoeden van schuld leidt of moet leiden, maar wel dat daarvoor de deur openstaat.[10] De karakteristieken van het product of de dienst lijken mij voldoende redengevend te kunnen zijn om te concluderen dat sprake is van een redelijk vermoeden van schuld van deelname aan een criminele organisatie. Het gebruik van een kostbare *cryptophone* door alle leden van de organisatie – want met een *cryptophone* kan alleen met een andere *cryptophone* worden gecommuniceerd – is dan het bewijs voor de duurzaamheid en beslotenheid van de organisatie.

9. Terug naar de onderhavige zaak. Het EHRM hoeft zich uiteindelijk niet in scherpe bewoordingen uit te laten over de redenering van de Turkse autoriteiten dat het gebruik van *ByLock* gelijkstaat aan deelname aan een terroristische organisatie. De “bewijzen” dat *ByLock* een dienst van en voor leden van FETÖ is, wordt namelijk pas maanden na klagers arrestatie en voorarrest bekend (par. 171). Dit betekent dat ten tijde van de arrestatie en het voorarrest nog niets bekend was over *ByLock*, althans dat dit niet blijkt uit de stukken. Het EHRM concludeert dan ook dat de rechtbank van Ankara, ten tijde van de beslissing over het

voorarrest van klager, geen toereikende informatie voorhanden had om te concluderen dat *ByLock* enkel door leden van FETÖ werd gebruikt (par. 174; 179).

D.A.G. van Toor

Universitair docent Straf(proces)recht (Willem Pompe Instituut voor Strafrechtswetenschappen (UU))

[1] EHRM 3 maart 2020, ECLI:CE:ECHR:2020:0303JUD006644817, *Hakan Baş t. Turkije* (EHRM, nr. 66448/17) – Hoe bijzonder is noodrecht?, «EHRC Updates» juni 2020, m.nt. De Lange; EHRM 10 november 2020, ECLI:CE:ECHR:2020:1110JUD002319917, *Sabuncu e.a. t. Turkije* (EHRM, nr. 23199/17) – Een redelijke verdenking?, «EHRC Updates» april 2021, m.nt. Ten Voorde.

[2] EHRM 3 maart 2020, ECLI:CE:ECHR:2020:0303JUD006644817, *Hakan Baş t. Turkije* (EHRM, nr. 66448/17) – Hoe bijzonder is noodrecht?, «EHRC Updates» juni 2020, m.nt. De Lange; EHRM 10 november 2020, ECLI:CE:ECHR:2020:1110JUD002319917, *Sabuncu e.a. t. Turkije* (EHRM, nr. 23199/17) – Een redelijke verdenking?, «EHRC Updates» april 2021, m.nt. Ten Voorde.

[3] Ook in de twee eerder genoemde zaken speelt *ByLock* een belangrijke rol. Daarnaast levert het invoeren van *ByLock* veel treffers op in HUDOC. Zie bijvoorbeeld ook EHRM 16 april 2019, ECLI:CE:ECHR:2019:0416JUD001277817, *Alparslan Altan t. Turkije*; EHRM 19 februari 2021, zaaksnr. 15669/20, *Yalcinkaya* t. *Turkije* (*communicated case*), waarin door het EHRM vele vragen worden gesteld over *ByLock* (bijv. over de betrouwbaarheid en de wettelijke grondslag van het onderzoek naar de applicatie).

[4] Bijvoorbeeld https://www.nrc.nl/nieuws/2021/03/14/grote-rol-politie-bij-encro-hack-a4035545, laatst geraadpleegd op 27 januari 2022; https://www.politie.nl/nieuws/2021/maart/9/nieuwe-klap-voor-georganiseerde-misdaad.html, laatst geraadpleegd op 27 januari 2022.

[5] https://blog.fox-it.com/2017/09/13/fox-it-debunks-report-on-bylock-app-that-landed-75000-people-in-jail-in-turkey/, laatst geraadpleegd op 27 januari 2022.

[6] E.H.A. van de Sandt, *Deviant Security: The Technical Computer Security Practices of Cyber Criminals*, Bristol: University of Bristol 2019.

[7] https://www.nrc.nl/nieuws/2021/03/14/grote-rol-politie-bij-encro-hack-a4035545, laatst geraadpleegd op 27 januari 2022.

[8] https://www.politie.nl/nieuws/2021/maart/9/nieuwe-klap-voor-georganiseerde-misdaad.html, laatst geraadpleegd op 27 januari 2022.

[9] C.M. Taylor Parkins-Ozephius, I.N. de Wit, D.A.G. van Toor & T. Beekhuis, 'De politie als winkelier van smartphones met "versleutelde" communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel', *TBS&H* 2021, 5, p. 322-333.

[10] Zie uitgebreider D.A.G. van Toor, 'Het enkele gebruik van *cryptophones* als basis voor procesrechtelijke concepten', *TBS&H* 2022, 2 (*in press*).