ANNOTATIE

Podchasov t. Rusland (EHRM, 33696/19) – Biedt artikel 8 EVRM een recht op end-to-end encryptie?

J.H.L. van Banning

Annotatie bij Europees Hof voor de Rechten van de Mens, 13-02-2024, ECLI:CE:ECHR:2024:0213JUD003369619 (EHRC-2024-0077)

1. Het opleggen van verplichtingen aan communicatieaanbieders om gegevens over gebruikers te bewaren ten behoeve van de nationale veiligheid of het bestrijden van (zware) criminaliteit staat al geruime tijd onder de aandacht. Het belang van digitaal bewijs in strafzaken, bijvoorbeeld in de vorm van historische verkeers- en locatiegegevens, heeft geleid tot een toenemende druk op communicatieaanbieders om deze gegevens te bewaren voor eventueel later gebruik in strafzaken. Tegelijk staat regelgeving die verplichtingen tot het bewaren van deze gegevens oplegt op gespannen voet met de privacy van gebruikers. In een steeds groter wordend aantal zaken hebben zowel het Hof van Justitie als het Europees Hof voor de Rechten van de Mens zich uitgelaten over deze spanning.[1] Tot voor kort stond daarbij, ondanks aandacht daarvoor in de literatuur[2] en het belang dat aan encryptie in verschillende Europese richtlijnen en verordeningen wordt toegekend,[3] een verplichting van communicatieaanbieders om ondersteuning te bieden bij het ontsleutelen van gegevens nog niet centraal. In de zaak *Podchasov t. Rusland* is daar op 13 februari 2024 verandering in gekomen.

2. De feiten van de zaak kunnen als volgt worden samengevat. Telegram Messenger LLP (hierna: Telegram) biedt in Rusland een gratis chatapplicatie aan, die onder andere de mogelijkheid biedt om end-to-end versleutelde berichten te versturen. Vanaf 28 juni 2017 kwalificeert Telegram als een "*Internet Communications Organizer*" (ICO) voor de Russische telecommunicatiewet. Daarmee ontstaat voor Telegram de verplichting om alle metadata van

berichtenverkeer een jaar te bewaren, de inhoud van alle communicatie voor zes maanden te bewaren, en opsporingsautoriteiten onder omstandigheden toegang te geven tot deze gegevens in combinatie met informatie die nodig is voor het ontsleutelen van eventuele end-to-end versleuteling. Kort daarna krijgt Telegram van de Russische autoriteiten het bevel om het berichtenverkeer van een zestal gebruikers te ontsleutelen. Telegram weigert aan dit bevel te voldoen, met het argument dat ontsleuteling niet mogelijk is zonder een kwetsbaarheid in het encryptiemechanisme van alle Telegramgebruikers te creëren. Na het opleggen van een boete naar aanleiding van deze weigering wordt Telegram op 13 april 2018 in heel Rusland verboden.[4] De klager vecht zonder succes met vierendertig anderen (allemaal gebruikers van Telegram, maar geen onderwerp van het oorspronkelijke decryptiebevel) het bevel aan tot aan het Russisch Hooggerechtshof. Vervolgens wendt de klager zich tot het EHRM, met de klacht dat de bewaarplicht, de toegang tot de gegevens door de autoriteiten, en de verplichting aan ICO's om mee te werken aan decryptie in strijd met art. 8 EVRM zijn. Het EHRM benadert deze klacht niet alleen vanuit de zojuist aangehaalde rechtspraak inzake verplichtingen aan communicatieaanbieders, maar verwijst ook naar de bredere internationale discussie over de wenselijkheid van het inperken van end-to-end encryptie. In deze annotatie wordt daarom eerst ingegaan op enkele technische en historische aspecten van deze discussie. Daarna wordt het oordeel van het EHRM besproken. Tot slot zal kort worden ingegaan op de mogelijke betekenis van de overwegingen van het EHRM voor het Nederlandse en Europese beleid ten aanzien van end-to-end versleuteling.

3. Encryptie, in de meer algemene zin van het woord, betreft het omzetten van de inhoud van een leesbare tekst (*plaintext*) naar een codetekst (*ciphertext*) die zonder het terugzetten naar *plaintext* niet begrijpelijk is. Encryptie heeft verschillende voorkomens, maar voor de hier te bespreken zaak is dus met name de zogenaamde *end-to-end-encryption* (E2EE) van belang. Bij E2EE wordt een bericht bij het versturen daarvan met een zogenaamde *public key* omgezet naar *ciphertext*. De *public key* is, zoals de naam al suggereert, publiekelijk beschikbaar. Deze *public key* werkt evenwel slechts één kant op: een tekst kan ermee versleuteld worden, maar niet weer ontsleuteld worden. Daarvoor moet gebruik worden gemaakt van een *private key*, die enkel op het apparaat van de ontvanger staat. Eventuele onderscheppers van het berichtenverkeer kunnen daardoor niet bij de inhoud van de berichten komen. Ook de aanbieder van de communicatiedienst heeft bij deze vorm van encryptie geen mogelijkheid om de inhoud van de verstuurde berichten, bijvoorbeeld op vordering van opsporingsautoriteiten, te ontsleutelen.[5]

4. Sinds de opkomst van gemakkelijk toegankelijke en technisch hoogwaardige encryptie heeft een serie discussies plaatsgevonden over de vraag of communicatieaanbieders niet verplicht zouden moeten worden om een 'achterdeur' in te bouwen, bijvoorbeeld door slechts

versleuteling aan te bieden die ook door de communicatiebieder (al dan niet op bevel van opsporingsautoriteiten) ontsleuteld kan worden, of de versleuteling makkelijker te maken om te kraken. In deze discussies (die in de literatuur de naam "*Cryptowars*" hebben gekregen[6]) hebben opsporingsautoriteiten steeds gewezen op het risico dat een deel van de georganiseerde criminaliteit zich definitief aan het zicht van opsporingsdiensten zou onttrekken. Tegenstanders van een achterdeur wijzen er daarentegen op dat het verzwakken van de E2EE voor een enkele gebruiker niet mogelijk is zonder de encryptie voor alle gebruikers te verzwakken. Dit maakt dat een verplichting tot het ontsleutelen van specifieke berichten noodzakelijkerwijs het verzwakken van de encryptie van alle gebruikers inhoudt (en deze gebruikers dus kwetsbaar maakt voor cybercriminaliteit, de communicatieaanbieder, of kwaadwillende overheden). Bovendien bestaat er volgens tegenstanders een groot aantal meer gerichte alternatieven voor het confisqueren van communicatie (daarbij kan gedacht worden aan het hacken van het apparaat, om berichten voor de versleuteling of na de ontsleuteling te achterhalen, of infiltratie) of kan gebruik worden gemaakt van onderdelen van de communicatie die niet versleuteld zijn, zoals de bijbehorende metadata.[7]

5. Het EHRM vangt zoals gebruikelijk aan met de vraag of sprake is van een inbreuk. Met betrekking tot de opslag van de communicatie stelt het EHRM vast dat alleen de opslag van gegevens al een inbreuk op het privéleven en de correspondentie van de klager is. Met betrekking tot de toegang door de autoriteiten ontstaat het uit de rechtspraak van het EHRM bekende probleem dat er geen bewijs is dat de autoriteiten ook toegang hebben gehad tot de gegevens van de klager. Onder verwijzing naar het toetsingskader dat voor toetsing van wetgeving *in abstracto* is geformuleerd in *Roman Zakharov t. Rusland*[8] is het EHRM hier kort over. In die zaak oordeelde het EHRM al dat de relevante bepalingen in de Russische telecommunicatiewet inzake toegang tot gegevens van communicatieaanbieders te weinig waarborgen bevatte, en alleen het bestaan daarvan al een inbreuk vormt. Omdat Rusland sinds *Roman Zakharov* de wet niet gewijzigd heeft is dat dus ook in deze zaak het geval. De verplichting voor de communicatieaanbieder om mee te werken aan ontsleuteling, tot slot, is voor het EHRM eveneens een inbreuk. De verplichting om desgevraagd mee te werken aan ontsleuteling dwingt de communicatieaanbieder om het encryptiemechanisme in het algemeen te verzwakken. Daarmee worden dus alle gebruikers getroffen, waaronder de klager.

6. De vraag is vervolgens of deze inbreuk gerechtvaardigd is op grond van lid 2 van art. 8 EVRM. Daarvoor moet de vraag beantwoord worden of de inbreuk in *accordance with law* is, een *legitimate aim* heeft, en of deze *necessary in a democratic society* is. Zoals gebruikelijk is het EHRM kort over de vraag of sprake is van een *legitimate aim*: het bestrijden van de nationale veiligheid, de openbare orde, en de bestrijding van criminaliteit zijn legitieme doeleinden voor het maken van een inbreuk. De vraag is vervolgens hoe de inbreuk zich verhoudt tot deze

doelen. Het EHRM beschouwt de inbreuk die gemaakt wordt door de automatische ongerichte retentieverplichting als "*exceptionally wide-ranging and serious*".[9] Anders dan het Hof van Justitie (en in een recente eigen uitspraak),[10] toetst het EHRM de retentie niet afzonderlijk aan artikel 8 EVRM, maar tezamen met de waarborgen waarmee de toegang tot die gegevens door de autoriteiten gepaard gaan. Deze waarborgen schieten volgens het EHRM tekort: de Russische opsporingsautoriteiten moeten weliswaar een rechterlijke machtiging verkrijgen alvorens de gegevens te kunnen raadplegen, maar er bestaat geen verplichting om die machtiging ook aan de communicatieaanbieder te tonen. Daarnaast verplicht de Russische wetgeving communicatieaanbieders tot het installeren van technieken die directe toegang door de Russische veiligheidsdiensten tot de communicatie mogelijk maken. Gezien het risico van misbruik dat een dergelijke regeling in het leven roept, moet de wet voldoende waarborgen bevatten tegen willekeur en misbruik. Omdat het hier in feite dus om dezelfde regeling gaat die in *Roman Zakharov* onvoldoende waarborgen bleek te bevatten, komt het EHRM onder verwijzing naar die laatste uitspraak in *Podchasov* tot dezelfde conclusie.

7. Bezien in het licht van de reeds bestaande rechtspraak van zowel het EHRM als het Hof van Justitie over het bewaren en vorderen van gegevens komen deze conclusies niet als een verrassing. Wel nieuw is wat het EHRM vervolgens bepaalt over de verplichting tot medewerking aan het ontsleutelen van de communicatie. Na het belang van encryptie voor verschillende fundamentele rechten en beveiliging benadrukt te hebben, constateert het EHRM onder verwijzing naar Europese en internationale aanbevelingen en deskundigen dat "(t)hese measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications."[11] Hoewel encryptie ook door criminele organisaties gebruikt kan worden, concludeert het EHRM onder verwijzing naar diezelfde aanbevelingen dat er alternatieven beschikbaar zijn. De verplichting om *end-to-end* versleutelde communicatie te ontsleutelen is daarom disproportioneel.

8. Er valt een aantal zaken op aan de redenering van het EHRM. De redenering bevat, afgezien van de conclusie, geen verwijzing naar waarborgen (of het gebrek daaraan) of doelstellingen in de Russische wetgeving. De premisse dat de verplichting om mee te werken aan ontsleutelingsbevelen een inbreuk op de veiligheid en privacy van alle gebruikers noodzakelijk maakt, bestaat voor een groot deel uit verwijzingen naar internationale documentatie en (overigens niet nader gespecificeerde) deskundigen. De argumentatie heeft daardoor een vrij algemeen karakter: ongeacht de mogelijke waarborgen of doelstellingen is een verplichting die neerkomt op het afzwakken van encryptie disproportioneel zolang meer

gerichte alternatieven voorhanden zijn. Daarnaast valt op hoe weinig woorden het EHRM uiteindelijk besteedt aan dit laatste onderdeel van de klacht (het EHRM komt tot zijn conclusie in slechts vier korte paragrafen). Mogelijk heeft het stilzitten van de Russische autoriteiten in deze procedure daarbij een rol gespeeld. De Russische Federatie – inmiddels geen lid meer van de Raad van Europa – heeft nauwelijks geprobeerd de bewering van de klager tegen te spreken, en het EHRM heeft dus mogelijk ook weinig reden gehad om dieper op deze materie in te gaan.[12]

9. De vraag is of de zaak verregaande gevolgen moet hebben voor de Nederlandse praktijk. Vooralsnog bevat de Nederlandse Telecommunicatiewet noch het Wetboek van Strafvordering een expliciete verplichting om encryptie te verzwakken. Art. 126m lid 6 Sv bevat een verplichting tot medewerking aan het ontsleutelen van de communicatie, maar deze verplichting geldt slechts voor zover de communicatieaanbieder toegang heeft tot de mogelijkheid om de communicatie te ontsleutelen. De aanbieder hoeft de communicatie dus niet ontsleutelbaar aan te bieden.[13] De Wet op de Inlichtingen- en Veiligheidsdiensten 2017 bevat een vergelijkbare verplichting om mee te werken aan ontsleuteling voor communicatieaanbieders (art. 57), waarin evenwel is geëxpliciteerd dat dit bevel niet kan zien op het afzwakken van de encryptie of het inbouwen van toegang.[14] Voorts zijn zogenaamde '*over-the-top*' (OTT) communicatiediensten – communicatiediensten die (kort gezegd) berichtenverkeer via het internet aanbieden – uitgezonderd van de aftapbaarheidsverplichting uit hoofdstuk 13 van de Telecommunicatiewet.[15] Belangrijke aanbieders van E2EE in Nederland, zoals WhatsApp, Signal en Telegram, vallen daardoor niet onder de aftapbaarheidsverplichting die is neergelegd in de Telecommunicatiewet. In een kabinetsstandpunt uit 2016 komt het kabinet bovendien nog tot de conclusie dat "(…) het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland."[16]

10. Dat laat onverlet dat er de afgelopen jaren door de Minister van Justitie en Veiligheid onderzoek is gedaan naar de mogelijkheid om de aftapbaarheidsverplichting in de Telecommunicatiewet uit te breiden naar OTT-communicatiediensten. Vooralsnog lijkt dit niet te hebben geleid tot een mogelijke uitbreiding van de aftapbaarheidsverplichting die niet eveneens een verzwakking van E2EE in zou houden.[17] Ook in Europees verband is E2EE geen rustig bezit. Op het moment van schrijven wordt gewerkt aan een (controversieel) voorstel dat het, kort gezegd, mogelijk maakt om verleners van (onder andere) interpersoonlijke communicatiediensten te verplichten om detectiemechanismen in te zetten om berichtenverkeer te controleren op beeldmateriaal van seksueel kindermisbruik en *grooming*.[18] Hoewel de tekst van het voorstel niet expliciet over encryptie spreekt en de considerans het belang van encryptie benadrukt (overweging 26), is in de literatuur

gesignaleerd dat een dergelijke verplichting de noodzaak creëert berichten ofwel voorafgaand aan de versleuteling te scannen (het zogenaamde *client side scanning*), dan wel de versleuteling te verzwakken zodat deze '*in transit*' gescand kunnen worden.[19] Wel verdient vermelding dat in theorie slechts de laatste variant impliceert dat E2EE verzwakt zou moeten worden (het scannen van tekst of afbeeldingen op het apparaat nog voordat ze versleuteld zijn, kan immers zonder dat de encryptie zelf verzwakt wordt).[20] Niet onbelangrijk is, tot slot, dat het Zweedse presidentschap van de Raad van de Europese Unie in 2023 heeft voorgesteld om een *High Level Expert Group* in te stellen om onderzoek te doen naar uitdagingen voor de toegang tot gegevens van communicatieaanbieders, waaronder E2EE.[21]

11. Mede dankzij de opkomst van de hackbevoegdheid als alternatief voor het verzwakken van encryptie hebben sommige auteurs de laatste jaren gesproken over "een (al dan niet langdurige) wapenstilstand in de *Cryptowars*."[22] De hierboven besproken initiatieven en discussies laten echter zien dat 'de achterdeur' bij E2EE voor zowel de Nederlandse als Europese wetgever geen afgeronde discussie is. In dit licht zijn de algemene doch spaarzame overwegingen van het EHRM over het belang van encryptie onverminderd relevant; wie E2EE wil verzwakken, zal voldoende moeten onderbouwen dat er geen alternatieven zijn die een meer gerichte oplossing bieden.

J.H.L. van Banning

Promovendus straf(proces)recht aan de Vrije Universiteit Amsterdam

[1] Zie o.a. *Breyer t. Duitsland*, EHRM 30 januari 2020, nr. 50001/12, ECLI:CE:ECHR:2020:0130JUD005000112, EHRC Updates april 2020, m.nt. Kranenborg; *Ekimdzhiev e.a. t. Bulgarije*, EHRM 11 januari 2022, nr. 70078/12, ECLI:CE:ECHR:2022:0111JUD007007812, EHRC Updates 29 januari 2023, m.nt. Van Toor; *Digital Rights Ireland*, HvJ EU (GK) 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, «EHRC» 2014/140, m.nt. Koning; *Tele2*, HvJ EU (GK) 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, «EHRC» 2017/79, m.nt. Koning; *La Quadrature du Net*, HvJ EU (GK) 6 oktober 2020, C-511/18 e.a., ECLI:EU:C:2020:791, EHRC Updates januari 2021, m.nt. Schroers; *G.D. t. the Commissioner of the Garda Síochána e.a.*, HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, EHRC Updates november 2022, m.nt. Jansen en Te Molder; *Prokuratuur*, HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, EHRC Updates mei 2021, m.nt. Van Toor.

[2] Zie bijvoorbeeld O.L. van Daalen, 'The right to encryption: Privacy as preventing unlawful access', *Computer Law & Security Review*, Volume 49, 2023, 105804, p. 1-19.

[3] Zie bijvoorbeeld Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), art. 32; Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), overweging 20 considerans; Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie, overweging 97 considerans en art. 40.

[4] Het EHRM merkt op dat Telegram desondanks nog steeds publiekelijk in Rusland beschikbaar en in gebruik is, *Podchasov t. Rusland,* par. 14. In reactie op het verbod is door Telegram eveneens een klacht bij het EHRM ingediend, zie EHRM, 29 oktober 2020, nr. 13232/18.

[5] Zie voor een toegankelijke bespreking J.H. Hoepman, *Privacy is hard and seven other myths. Achieving privacy through careful design*, Cambridge: MIT Press 2023, p. 74-78.

[6] Zie voor een korte geschiedenis B.J. Koops & E. Kosta, 'Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"', *Computer Law & Security Review*, 34(4), p. 890-900.

[7] Ibid. Zie ook, met verdere bronverwijzing, de interventies in de onderhavige zaak van Privacy International (https://privacyinternational.org/legal-action/podchasov-v-russia, geraadpleegd op 6 maart 2024) en het European Information Society Institute (https://www.lse.ac.uk/law/news/2021/echr-clinic, geraadpleegd op 6 maart 2024).

[8] *Roman Zakharov t. Rusland*, EHRM, 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.

[9] *Podchasov t. Rusland,* par. 70.

[10] *Škoberne t. Slovenië*, EHRM, 15 februari 2024, nr. 19920/20, ECLI:CE:ECHR:2024:0215JUD001992020, par. 139-146.

[11] *Podchasov t. Rusland*, par. 77. Het EHRM verwijst onder andere naar de gezamenlijke verklaring van Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging (20 mei 2016), *On lawful criminal investigation that respects 21st Century data protection*; Europees Comité voor gegevensbescherming en Europees Toezichthouder voor

gegevensbescherming (28 juli 2022), *Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*; Resolutie 47/16 van de VN Mensenrechtenraad (26 juli 2021), *The promotion, protection and enjoyment of human rights on the Internet*, UN Doc. A/HRC/RES/47/16.

[12] Zie *Podchasov t. Rusland*, par. 57.

[13] Zie *Kamerstukken II* 1998/99, 26671, 3, p. 24-25.

[14] Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 123-124.

[15] Hoofdstuk 13 ziet enkel op aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. Omdat berichtendiensten als WhatsApp, Signal en Telegram een communicatiedienst aanbieden over de infrastructuur (het internet) heen zonder het gebruik van de infrastructuur zelf aan te bieden, vallen zij hier niet onder. Zie *Kamerstukken II*, 2020/21, 35 865, nr. 3 (MvT), p. 4.

[16] *Kamerstukken II*, 2015/16, 26 643, nr. 383, p. 4.

[17] Zie bijvoorbeeld de brief van de Minister van Justitie en Veiligheid d.d. 28 april 2022 inzake Wob-verzoek inzake encryptie, aftapbaarheid van OTT-communicatiediensten (Kamerstuk 26 643, nr. 844). Zie ook de discussie daarover in *Kamerstukken II*, 2022/23, 26 643, nr. 918.

[18] Voorstel van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, COM(2022)209, 11 mei 2022. Zie daarover uitgebreid A. de Hingh, 'De preventie en bestrijding van seksueel misbruik van kinderen in de online omgeving: een controversieel Europees voorstel', *Tijdschrift voor Internetrecht*, *2023*(2), p. 53-65.

[19] O.L. van Daalen, *Fundamental rights assessment of the framework for detection orders under the CSAM proposal*. Instituut voor Informatierecht, 22 april 2023.

[20] Dit lijkt ook de positie van het kabinet te zijn, zie *Kamerstukken II*, 2022/23, 26643, nr. 968, p. 11. *Client side scanning* kent echter eigen bezwaren, en er is voor gewaarschuwd dat het voorstel communicatieaanbieders zou kunnen bewegen tot het afzwakken van E2EE om aan de nieuwe verplichtingen te kunnen voldoen. Zie Europees Comité voor gegevensbescherming en Europees Toezichthouder voor gegevensbescherming (28 juli 2022), *Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, p. 27-29.

[21] *"Going dark": will the next assault on privacy take place behind closed doors?*, Statewatch, 19 april 2023.

[22] B.J. Koops & J.J. Oerlemans, 'Formeel strafrecht en ICT', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT, derde druk*, Den Haag: Sdu Uitgevers 2019, p. 139. Zie ook Koops & Kosta 2018, p. 900.