ANNOTATIE

Breyer t. Duitsland (EHRM, nr. 50001/12) – Verplichte registratie van prepaid simkaarthouders in overeenstemming met het EVRM?

H. Kranenborg

Annotatie bij Europees Hof voor de Rechten van de Mens, 30-01-2020, ECLI:CE:ECHR:2020:0130JUD005000112 (EHRC-2020-0078)

Introductie

1. De bewaarplicht van telefoongegevens is een onderwerp dat met name het Hof van Justitie van de EU al vele jaren bezighoudt. De onderhavige uitspraak van het EHRM, waarin uitgebreid verwezen wordt naar deze jurisprudentie van het HvJ EU, betreft een nieuw element in de onderliggende discussie. Tot dusver zagen de uitspraken van het HvJ EU op de bewaarplicht van gegevens die de telefoonmaatschappijen in de normale uitoefening van hun dienstverlening al verzamelen.[1] Gegoten in gegevensbeschermingstermen: de verwerking van de persoonsgegevens werd door de telefoonmaatschappij al noodzakelijk geacht voor het door haar gestelde commerciële doel. De maatregelen die in de jurisprudentie van het HvJ EU centraal stonden, betroffen Europese en nationale wetgeving die telefoonmaatschappijen de plicht oplegde deze commercieel gegenereerde gegevens langer te bewaren, om beschikbaar te zijn voor strafrechtelijke handhavingsdoeleinden.

2. De onderhavige zaak wijkt hiervan af omdat Duits recht telefoonmaatschappijen allereerst verplicht om bepaalde gegevens te genereren die zij voor haar commerciële doeleinden normaal gesproken *niet* noodzakelijk acht. Het gaat hier om de identificatiegegevens van personen die een prepaid simkaart aanschaffen. Voordat verder wordt ingegaan op de relevantie van dit verschil voor de benaderingen van het EHRM en het HvJ EU, volgt

hieronder een beknopte beschrijving van de discussie zoals deze zich binnen de Europese Unie en voor het HvJ EU afspeelt.

De bewaarplicht van telefoongegevens in het Unierecht

3. Na de aanslagen in Madrid en Londen in 2004 en 2005 werd door de Uniewetgever in recordtempo een richtlijn aangenomen waarin lidstaten telefoonmaatschappijen moesten verplichten telefoongegevens te bewaren van al hun klanten voor een periode van tussen de zes maanden en twee jaar.[2] Het betrof zogenaamde verkeers- en locatiegegevens (ook wel: metadata). Dit zijn telefoongegevens zoals tijdstip en duur van een gesprek, maar niet de inhoud van de communicatie. De gegevens moesten bewaard worden om beschikbaar te zijn voor de bestrijding van ernstige criminaliteit.

4. Na het overleven van een eerste rechtsgang vanwege een vermeende verkeerde rechtsgrondslag in het voormalige EG-Verdrag[3], verklaarde het HvJ EU in *Digital Rights Ireland* de richtlijn in 2014 alsnog ongeldig, vanwege strijd met het recht op privacy en het recht op bescherming van persoonsgegevens zoals neergelegd in art. 7 en 8 van het Grondrechtenhandvest.[4] Het HvJ hekelde met name het algemene karakter van de gegevensopslag; het betrof alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder onderscheid.[5] Daarnaast bevatte de richtlijn volgens het HvJ geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. Ook kende de richtlijn geen verdere materiële en procedurele voorwaarden voor toegang en gebruik.[6]

5. Hoewel de richtlijn ongeldig was verklaard, gingen niet alle lidstaten ertoe over de nationale omzettingswetgeving aan te passen of in te trekken. In de zaak *Tele2 Sverige en Watson* werd het HvJ EU gevraagd of de vereisten uit *Digital Rights Ireland* ook van toepassing waren op de bestaande nationale wetgeving.[7] Het antwoord daarop was bevestigend. In zijn uitspraak ging het HvJ EU nog verder dan in *Digital Rights Ireland* in het formuleren van de vereisten waaraan de dataretentie-wetgeving moest voldoen.

6. De meest controversiële van deze vereisten betrof de overweging dat een algemene bewaarplicht als zodanig niet kon worden toegestaan.[8] Volgens het HvJ maakten de bewaarde gegevens, in hun geheel beschouwd, profilering mogelijk en konden zeer precieze conclusies worden getrokken over het privéleven van de betrokken personen.[9] Hierdoor was sprake van een bijzonder ernstige inbreuk op de fundamentele rechten van de betrokkenen. Hoewel de bestrijding van ernstige criminaliteit een rechtmatig doeleinde was, ging een algemene bewaarplicht volgens het HvJ EU verder dan strikt noodzakelijk.[10] Volgens het HvJ EU was een *gerichte* bewaarplicht eventueel wél mogelijk, waarbij er een verband moet

bestaan tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare orde.[11]

7. Meerdere lidstaten hadden kritiek op het vereiste van gerichte bewaring. Het voornaamste bezwaar was dat een gerichte bewaarplicht onbruikbaar was, omdat het moeilijk vooraf is te bepalen van wie de telefoongegevens nodig zijn om een misdrijf op te lossen. Bovendien, mocht dit al mogelijk zijn, dan zou dit stigmatisering en discriminatie in de hand kunnen werken. Het gevolg was: vijf nieuwe prejudiciële procedures voor het HvJ EU waarin de *Tele2 Sverige en Watson* uitspraak expliciet ter discussie werd gesteld.[12] Gevraagd werd ook of een algemene bewaarplicht wél mogelijk was als het doel het handhaven van de nationale veiligheid betreft, of de bestrijding van alleen *bijzonder* ernstige criminaliteit. Op het moment van schrijven waren deze zaken nog aanhangig.[13]

8. Een tweede opzienbarend element uit de uitspraak in *Tele2 Sverige en Watson* was dat het HvJ EU een onderscheid maakte tussen enerzijds de beoordeling of het *bewaren* van de gegevens als zodanig rechtmatig was, en anderzijds of *toegang* tot de gegevens met voldoende waarborgen was omgeven (o.a. voorafgaande rechterlijke toestemming). Met andere woorden: de rechtmatigheid van de *bewaar*plicht was niet afhankelijk van hoe *toegang* tot de gegevens was geregeld. Aangevoerd zou kunnen worden dat het risico van profilering bij een algemene bewaarplicht zich alleen materialiseert als de gegevens ook daadwerkelijk voor die doeleinden toegankelijk zijn. Als toegang restrictief is geregeld, waarbij profilering wettelijk onmogelijk wordt gemaakt, dan zou de impact van een algemene bewaarplicht minder groot zijn. Deze redenering, die in *Tele2 Sverige en Watson* aan het HvJ EU was voorgelegd, nam het HvJ echter niet over.[14] De bewaarplicht, met de theoretische mogelijkheid van profilering, was volgens het HvJ EU op zichzelf in strijd met het Grondrechtenhandvest.

9. Toegang tot telefoongegevens voor strafrechtelijke handhaving stond ook centraal in de zaak *Ministerio Fiscal*.[15] De vraag was of autoriteiten toegang kon worden verleend tot bepaalde identiteitsgegevens van een klant van een telefoonmaatschappij in het kader van een strafrechtelijk onderzoek dat een niet ernstig delict betrof. De toegang betrof dus niet de eerder beschreven locatie- en verkeersgegevens, maar de meer ‘statische’ gegevens die de klant identificeren (ook wel: *subscriber data*). *Ministerio Fiscal* wijkt in zoverre af van de eerder besproken zaken, dat niet aan de orde was of de gegevens onderwerp waren van een wettelijke bewaarplicht. Identificatiegegevens (van ‘vaste’ klanten) worden immers door de telefoonmaatschappij normaal gesproken voor de duur van het contract bewaard voor de eigen commerciële doeleinden. Het HvJ EU kon zich daardoor beperken tot een analyse van de regels omtrent *toegang* tot de informatie. Omdat de gevraagde informatie louter de identificatie van de klant betrof en geen informatie omvatte waaruit zeer precieze conclusies konden worden getrokken over het privéleven van de betrokken personen, achtte het Hof de

inmenging met de fundamentele rechten van de betrokken persoon niet heel vergaand, waardoor de gegevens ook voor niet ernstige misdrijven toegankelijk konden zijn.[16]

De Breyer*-uitspraak van het EHRM*

10. De onderhavige uitspraak in *Breyer t. Duitsland* is de eerste waarin het EHRM met de materie in aanraking komt. Het bewaren van persoonsgegevens door bevoegde autoriteiten zélf is wel al vaker ter sprake gekomen. In 2000, in de zaak *Amann t. Zwitserland*, overwoog het EHRM dat het louter bewaren door autoriteiten van gegevens die het privéleven van individuen betreft een inmenging met het recht op bescherming van de persoonlijke levenssfeer oplevert.[17] Het meest bekend is wellicht de uitspraak in *S. en Marper t. Verenigd Koninkrijk*, waarin het EHRM oordeelde dat het bewaren van vingerafdrukken en DNA-materiaal van personen die waren veroordeeld en personen die verdacht waren geweest van een misdrijf in strijd was met art. 8 EVRM.[18]

11. De *Breyer*-zaak ziet op de wettelijke verplichting om de identiteitsgegevens van een prepaid-simkaarthouder te registreren en te bewaren tot één jaar na beëindiging van de contractuele relatie. Wat betreft de aard van de gegevens heeft de *Breyer*-zaak het meest weg van de gegevens die onderwerp vormden van de *Ministerio Fiscal*-uitspraak van het HvJ EU. Dit overweegt het EHRM ook met zoveel woorden.[19] Echter, zoals gezegd, de *Breyer*-zaak wijkt af van *Ministerio Fiscal* en de andere zaken voor het HvJ EU omdat in die eerdere zaken geen sprake was van een wettelijke plicht tot het vastleggen van de gegevens: het betrof door de telefoonmaatschappij reeds gegenereerde gegevens. Dit is een belangrijk punt in de zaak, waarover later meer. Eerst volgt een korte bespreking van de verschillende stappen in de redenering van het EHRM.

12. Het EHRM heeft weinig woorden nodig om te concluderen dat sprake is van een inmenging met art. 8 EVRM, dat er een wettelijke basis is voor die inmenging en dat sprake is van een legitiem doel. De voornaamste vraag is of de maatregel noodzakelijk is in een democratische samenleving.

13. Het EHRM stelt vast dat de registratie van gebruikers van mobiele telefoons het werk van wethandhavingsautoriteiten sterk versimpelt en versnelt. Dat de registratiemaatregel eventueel omzeild kan worden, zoals de klagers aanvoerden, kan volgens het Hof niet het algemene nut en de effectiviteit van een wettelijke bepaling in twijfel trekken. Volgens het EHRM is de maatregel een passend antwoord op de veranderingen in communicatiegedrag en gebruik van communicatiemiddelen.

14. Om vervolgens te beoordelen of sprake is van een redelijke balans tussen de verschillende private en publieke belangen, beoordeelt het EHRM eerst hoe ernstig de inmenging met het

recht op privéleven van de gebruikers is. Het EHRM constateert dat de gegevens geen hoogst persoonlijke informatie omvatten en dat de gegevens het niet mogelijk maken profielen van gebruikers op te stellen of hun bewegingen te volgen. Bovendien wordt geen informatie over de communicatie zelf opgeslagen. In die zin wijkt de zaak volgens het EHRM af van *Tele2 Sverige en Watson*, en lijkt zij meer op *Ministerio Fiscal*. Het EHRM concludeert dat hoewel de inmenging niet triviaal is, zij van beperkte aard is. De bewaartermijn van één jaar na beëindiging van de contractuele relatie is volgens het EHRM passend.

15. Hoewel de klagers alleen over de registratieplicht hebben geklaagd, moet volgens het EHRM voor de beoordeling van de proportionaliteit van de inmenging ook worden gekeken naar de manier waarop de mogelijke toegang tot de opgeslagen gegevens en het verdere gebruik ervan is geregeld. Hiermee lijkt het EHRM een andere benadering te kiezen dan het HvJ EU in *Tele2 Sverige en Watson*. In *Tele2 Sverige en Watson* speelden de regels over toegang, zoals uitgelegd, geen rol in de beoordeling van de proportionaliteit van de bewaarplicht. Anders gezegd, een algemene bewaarplicht kon niet worden 'gecompenseerd' met strikte regels voor toegang. Een verschil met de *Tele2 Sverige en Watson*-zaak is echter, dat in de onderhavige zaak het EHRM op zichzelf met de bewaarplicht geen probleem lijkt te hebben, waar het HvJ EU dat in *Tele2 Sverige en Watson* duidelijk wél had. Het EHRM ziet zich vervolgens genoodzaakt te toetsen hoe toegang tot de bewaarde gegevens is gereguleerd om te kunnen beoordelen of de nationale maatregel in z'n geheel in overeenstemming is met art. 8 EVRM. Daarmee is niet per se gezegd dat het EHRM de regels over toegang tot de gegevens ook een rol laat spelen als de beoordeling van de bewaarplicht op zichzelf negatief is.

16. Als het EHRM vervolgens naar de regels voor toegang tot de bewaarde gegevens kijkt, concludeert het dat er voldoende grenzen worden gesteld aan de bevoegdheid om gegevens op te vragen en dat toezicht door een onafhankelijke instantie (de Duitse gegevensbeschermingsautoriteiten) is gegarandeerd. Verder hebben betrokken personen algemene middelen om tegen informatieverzoeken in rechte op te treden, in het bijzonder in combinatie met rechtsmiddelen tegen uiteindelijke besluiten van de bevoegde instanties.

17. Ten aanzien van de vereisten van rechterlijke controle en onafhankelijk toezicht contrasteert het EHRM de *Breyer*-zaak met eerdere jurisprudentie, waarin onder meer geheime toezichtsmaatregelen ten behoeve van de nationale veiligheid centraal stonden. Het EHRM stelt vast dat in al die eerdere zaken sprake was van een meer serieuze en ingrijpende inmenging in het privéleven van betrokken personen en dat de vereisten van controle en toezicht niet zomaar overgedragen kunnen worden naar de toegang tot de gegevens in de onderhavige zaak. Het EHRM overweegt dat voor de onderhavige zaak het niveau van controle en toezicht een belangrijk maar niet beslissend element is in de beoordeling van de proportionaliteit van de nationale maatregel.

18. Deze versoepeling van de criteria staat het EHRM toe te accepteren, dat geen sprake is van voorafgaande rechterlijke controle, en dat de beoordeling van de noodzaak in beginsel door de autoriteit wordt uitgevoerd die de gegevens opvraagt. De betrokken telefoonmaatschappij is niet bevoegd de eventuele noodzaak van de toegang tot de gegevens in een concreet geval te beoordelen. Het vereiste van voorafgaande controle door een rechter of een onafhankelijke autoriteit was in de *Tele2 Sverige en Watson*-uitspraak van het EU HvJ een belangrijk criterium voor de rechtmatigheid van toegang tot bewaarde gegevens. Daarbij moet wel worden opgemerkt dat de aard van de persoonsgegevens in *Tele2 Sverige en Watson* van andere orde was dan in de onderhavige zaak. In *Ministerio Fiscal*, dat toegang tot gelijkaardige gegevens betrof, kwam de vraag of toegang tot dergelijke gegevens aan voorafgaande controle moet onderworpen niet ter sprake. Het is dus niet duidelijk of het HvJ EU in een vergelijkbaar geval, vast zou blijven houden aan het vereiste van voorafgaande controle.[20]

De dissenting opinion van rechter Ranzoni

19. Het EHRM komt tot de slotsom dat geen sprake is van een schending van art. 8 EVRM. Deze uitspraak werd door zes rechters ondersteund; één rechter stemde tegen. In zijn *dissenting opinion* legt rechter Ranzoni uit waarom hij vindt dat wél sprake is van een schending van art. 8 EVRM. Hij verschilt van mening over de waarde van de verschillende waarborgen waarmee toegang tot de opgeslagen gegevens is omgeven. Hij acht deze onvoldoende om verkeerd gebruik en misbruik van de gegevens te voorkomen, waarbij hij met name het ontbreken van voorafgaande rechterlijke controle of controle door een onafhankelijke autoriteit hekelt.

20. Rechter Ranzoni heeft echter ook moeite met de constatering dat de inmenging in het privéleven van de betrokken personen gering is. Hoewel hij het ermee eens is dat de bewaarde informatie op zichzelf niet als gevoelig is aan te merken, wijst hij erop dat identiteitsgegevens het mogelijk maken verdere informatie aan de geïdentificeerde persoon te koppelen. Hij verwijst daarbij naar de eerdere EHRM-uitspraak in *Benedik t. Slovenië*, waarin het Hof zich uitsprak over de inzage van de politie in de identiteitsgegevens van een gebruiker van een dynamisch IP-adres.[21] Vastgesteld was dat het dynamische IP-adres gebruikt was voor het online delen van kinderpornografie. Ten aanzien van die inzage overwoog het EHRM: '[…] what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data'.[22]

21. Rechter Ranzoni snijdt hier een belangrijk punt aan. De verplichting om de identificatiegegevens van prepaid-simkaarthouders vast te leggen en te bewaren dient uiteraard om de persoon achter een bepaald telefoonnummer te vinden. Welke informatie

daarmee aan de geïdentificeerde persoon gekoppeld kan worden, is contextafhankelijk. Het is daarom moeilijk in algemene zin iets over de ernst van de inmenging met het recht op privéleven te zeggen. Het vastleggen en bewaren van de identiteitsgegevens van een prepaid-simkaarthouder zorgt er bovendien voor dat de gegevens over het gebruik van de simkaart (de locatie- en verkeersgegevens) meerwaarde krijgen. Hoewel er ten tijde van de feiten in de onderhavige *Breyer*-zaak geen aanvullende verplichting gold ten aanzien van het bewaren van locatie- en verkeersgegevens, zal een wettelijke regeling die een bewaarplicht van dergelijke gegevens in het leven roept, bij een registratie van de prepaid-simkaarthouders, normalerwijs ook de gegevens van deze gebruiker omvatten.

22. En inderdaad, de Duitse telecommunicatiewet is in 2015 gewijzigd en heeft een algemene bewaarplicht van locatie- en verkeersgegevens in het leven geroepen. In vergelijking met de nationale wetgeving die centraal stond in *Tele2 Sverige en Watson*, is de bewaartermijn echter vrij kort: vier weken voor locatiegegevens en tien weken voor verkeersgegevens. De vraag of een dergelijke bewaarplicht, hoewel niet gericht, toch mogelijk is onder EU recht, vormt het onderwerp van een van de meest recente prejudiciële procedures voor het EU HvJ.[23]

Tot slot

23. Het EHRM navigeert met de onderhavige uitspraak tussen de verschillende uitspraken van het HvJ EU door. Daarbij lijkt het zich onvoldoende bewust van het speciale karakter van de plicht tot registratie van de prepaid-simkaarthouders en van het feit dat in de omvangrijke jurisprudentie van het HvJ over de bewaarplicht juist dit element nog niet is beoordeeld. De *dissenting opinion* van rechter Ranzoni legt de vinger op deze zere plek. Bij de beoordeling van de mate van inbreuk op het recht van betrokkenen, lijkt het EHRM bovendien onvoldoende rekening te houden met het feit dat de registratie van de identiteit van een prepaid-simkaarthouder het mogelijk maakt ook de locatie- en verkeersgegevens van de gebruiker te 'ontsluiten'. Het is daarmee niet gezegd dat het EHRM de Duitse registratieplicht in strijd met art. 8 EVRM had moeten verklaren. De constatering dat de inmenging in het privéleven van de betrokken personen *niet* gering was, had ertoe moeten leiden dat de rechtvaardiging van deze inmenging met een strengere blik beoordeeld werd.

H.R. Kranenborg is lid van de Juridische Dienst van de Europese Commissie en verbonden aan de K.U. Leuven en de Universiteit Maastricht. Deze bijdrage is op persoonlijke titel geschreven.

[1] Zie o.a. *Digital Rights Ireland Ltd*, HvJ EU (GK) 8 april 2014, gevoegde zaken C-293/12 en C-

594/12, ECLI:EU:C:2014:238, «EHRC» 2014/140 m.nt. Koning en *Tele2 Sverige en Watson*, HvJ EU (GK) 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, «EHRC» 2017/79 m.nt. Koning, waarover hieronder meer.

[2] Richtlijn 2006/24, OJ L 105, 13.4.2006, p. 54-63.

[3] *Ierland t. Europees Parlement en Raad*, HvJ EU (GK) 10 februari 2009, zaak C-301/06, ECLI:EU:C:2009:68.

[4] *Digital Rights Ireland*, *supra* noot 1.

[5] *Digital Rights Ireland*, punt 57.

[6] *Digital Rights Ireland*, punt 60-61. Dit is enigszins ironisch omdat het ontbreken van regels over toegang en verder gebruik door de autoriteiten juist de reden was dat de richtlijn de eerste rechtsgang over de juiste rechtsgrondslag overleefde.

[7] *Tele2 Sverige en Watson*, *supra* noot 1.

[8] Na de *Digital Rights Ireland*-uitspraak was er discussie of het HvJ een algemene bewaarplicht categorisch uitsloot.

[9] *Tele2 Sverige en Watson*, punt 99.

[10] *Tele2 Sverige en Watson*, punt 102 en 107.

[11] *Tele2 Sverige en Watson*, punt 108.

[12] Zie resp. zaak C-623/17, gevoegde zaken C-511/18 en C-512/18, zaak C-520/18 en gevoegde zaken C-793/19 en C-794/19. Een nieuw verzoek van een Ierse rechter was op het moment van schrijven nog niet officieel door het EU HvJ geregistreerd.

[13] Op 15 januari 2020 publiceerde Advocaat-Generaal Campos Sánchez-Bordona zijn conclusies, zie ECLI:EU:C:2020:5 tot en met 7.

[14] Zie conclusie van Advocaat-Generaal Saugmandsgaard Øe van 19 juli 2016 in *Tele2 Sverige en Watson*, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:572, punt 193 en verder.

[15] *Ministerio Fiscal*, HvJ EU (GK) 2 oktober 2018, zaak C-207/16, ECLI:EU:C:2018:788, «EHRC» 2019/18 m.nt. Van der Sloot.

[16] *Ministerio Fiscal*, pt. 56 tot en met 61. In een nog aanhangige prejudiciële procedure, ingesteld door een Estse rechter, wordt de vraag gesteld of toegang tot verkeers- en

locatiegegevens die een korte periode betreffen (bijv. een paar uur, één dag) ook als een niet ernstige inbreuk moet worden gezien. Zie zaak C-746/18, en de conclusie van Advocaat-Generaal Pitruzzella van 21 januari 2020, ECLI:EU:C:2020:18.

[17] *Amann t. Zwitserland*, EHRM (GK) 16 februari 2000, nr. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, «EHRC» 2000/31 m.nt. Brems, par. 69.

[18] *S. en Marper t. Verenigd Koninkrijk*, EHRM (GK) 4 december 2008, nrs. 30562/04, 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, «EHRC» 2009/13 m.nt. Koops. Zie voortbouwend op *S. en Marper* recentelijk: *Gaughran t. Verenigd Koninkrijk* en *Trajkovski en Chipovski t. Noord-Macedonië*, EHRM 13 februari 2020, resp. nr. 45245/15 en nrs. 53205/13 en 63320/13, ECLI:CE:ECHR:2020:0213JUD004524515 en ECLI:CE:ECHR:2020:0213JUD005320513, «EHRC Updates» 2020-0086 en «EHRC Updates» 2020-0093.

[19] Zie *Breyer t. Duitsland*, par. 94.

[20] Zie over het vereiste van voorafgaande goedkeuring door een gerechtelijke instantie of een onafhankelijke bestuurlijke autoriteit bij toegang tot gegevens bewaard door private entiteiten ook Advies A-1/15 van het HvJ EU over de voorgenomen overeenkomst tussen de EU en Canada over de doorgifte van passagiersgegevens (PNR), ECLI:EU:C:2016:656, pt. 262 en verder.

[21] *Benedik t. Slovenië*, EHRM 24 april 2018, nr. 62357/14, ECLI:CE:ECHR:2018:0424JUD006235714, «EHRC» 2018/154 m.nt. Van der Sloot.

[22] *Benedik t. Slovenië*, par. 109.

[23] Zaken C-793/19 en C-794/19.