EHRC EUROPEAN HUMAN RIGHTS CASES UPDATES

ANNOTATIE

P.N. t. Duitsland (EHRM, nr. 74440/17) – Opsporing met behoud van privacy

B.H.M. Custers

Annotatie bij Europees Hof voor de Rechten van de Mens, 11-06-2020, ECLI:CE:ECHR:2020:0611JUD007444017 (EHRC-2020-0170)

Feitenrelaas

1. De heer P.N., Duits staatsburger, kocht medio 2011 een fiets op de vlooienmarkt voor 29 euro. Die fiets was gestolen en daardoor kwam P.N. in beeld van de politie van Dresden op verdenking van heling. Bij de opsporing en vervolging werden identificerende gegevens van de verdachte verzameld, waaronder foto's van gezicht en lichaam van de verdachte, en vinger- en handpalmafdrukken. Verdachte had een strafblad. In 2010 kreeg hij een strafrechtelijke boete opgelegd omdat hij iemand valselijk had beschuldigd van een delict. In de jaren 2002-2009 was verdachte op het rechte pad gebleven, maar daarvoor was hij een veelpleger, die in de periode 1986-2001 dertien keer werd veroordeeld, waaronder vijf keer tot een gevangenisstraf, variërend van twee tot dertig maanden, voor uiteenlopende delicten, waaronder belaging, vandalisme en fraude. Voor de vermeende fietsheling, de aanleiding van deze zaak, is verdachte vrijgesproken.

2. In deze zaak staat centraal of bovengenoemde identificerende gegevens mochten worden afgenomen bij verdachte. Hiertegen maakt hij administratief bezwaar bij de politie, met als argument dat dit een schending is van zijn recht op privacy (art. 8 EVRM) en dat het verzamelen van deze gegevens niet noodzakelijk en disproportioneel is. De politie wijst het bezwaar af op 24 augustus 2011, zich op het standpunt stellend dat het aannemelijk is dat verdachte in de toekomst opnieuw zou kunnen recidiveren. De zaak komt op 15 juni 2012 voor bij de rechtbank in Dresden, die eveneens het verzoek van de heer P.N. afwijst, omdat de afname van de gegevens door de politie noodzakelijk, relevant en proportioneel is. Op 7

oktober 2016 wijst ook het gerechtshof van Saksen, de Duitse deelstaat waarin Dresden ligt, het hoger beroep af, met verwijzing naar de redenen die de rechtbank eerder al opgaf. Op 10 mei 2017 geeft het federale constitutionele hof (Bundesverfassungsgericht) zonder verdere toelichting aan, dat de klacht van P.N. niet ontvankelijk is. Het EHRM stelt dat daarmee alle nationale rechtsmiddelen zijn uitgeput en neemt de zaak in behandeling.

Rechtsvragen en wettelijke kaders

3. De rechtsvraag die in deze zaak centraal staat is of het afnemen van identificerende persoonsgegevens, zoals foto's, vingerafdrukken en handpalmafdrukken is toegestaan. Het belangrijkste wettelijke kader is art. 8 EVRM, dat het recht op privacy waarborgt. Het recht op privacy is niet absoluut, er zijn uitzonderingen die een (beperkte) inbreuk op de privacy rechtvaardigen. De centrale rechtsvraag valt daarmee uiteen in verschillende deelvragen, zoals: (1) is hier sprake van een inbreuk op art. 8 EVRM en zo ja, (2) is die inbreuk gerechtvaardigd, want (2a) bij wet voorzien, (2b) voor een legitiem doel en (2c) in een democratische samenleving noodzakelijk? Zoals hieronder wordt besproken, loopt het Hof deze stappen systematisch en zorgvuldig na in deze uitspraak. Met name de proportionaliteitsvraag is daarbij interessant. De proportionaliteitsvraag geeft niet alleen de meeste ruimte voor verschillende afwegingen en interpretaties, maar moet bovendien speculatief beantwoord worden, omdat in belangrijke mate wordt meegewogen de kans dat verdachte (opnieuw) zal recidiveren. Deze zaak is vooral interessant omdat getoond wordt dat privacy en opsporing wel degelijk hand in hand kunnen gaan. Regelmatig wordt het recht op privacy gezien als een hindernis voor opsporingsautoriteiten (privacy versus opsporing/veiligheid), als iets waardoor ze hun werk minder doelmatig en doeltreffend zouden kunnen doen. In deze zaak wordt getoond dat als de autoriteiten de privacyregels zorgvuldig betrachten, er geen dergelijke hindernis hoeft te zijn.

4. De relevante nationale wettelijke kaders in deze zaak zijn het Duitse wetboek van strafvordering (Strafprozessordnung), in het bijzonder art. 81b dat de afname van foto's en vingerafdrukken regelt, en de politiewet in de deelstaat Saksen, in het bijzonder art. 43 dat de opslag en het gebruik van gegevens regelt (vergelijkbaar met de Wet politiegegevens in Nederland). De relevante Europese wettelijke kaders in deze zaak zijn, naast art. 8 EVRM, het Verdrag van Straatsburg en EU-richtlijn 2016/680. Het Verdrag van Straatsburg (Conventie 108) is een verdrag van de Raad van Europa uit 1981 op het terrein van bescherming van persoonsgegevens. Op de beginselen in dit verdrag heeft de EU haar wetgeving op het gebied van bescherming van persoonsgegevens ontwikkeld, waaronder de huidige Algemene Verordening Gegevensbescherming (AVG). EU-richtlijn 2016/680 is tegelijk met de AVG aangenomen door de EU en biedt een kader voor de bescherming van persoonsgegevens in het strafrecht.[1] Richtlijn 2016/680 en de AVG zijn elkaar wederzijds uitsluitende regimes. In

Duitsland is richtlijn 2016/680 geïmplementeerd in nationale wetgeving in de Duitse federale politiewet (Bundespolizeigesetz 1994) en op deelstaatniveau.[2]

Analyse

5. Het recht op privacy zoals geformuleerd in art. 8 EVRM is niet absoluut. Inbreuken op dit recht kunnen toegestaan zijn, volgens het tweede lid van dit artikel. Daarvoor moet aan drie voorwaarden zijn voldaan: de inbreuk moet (1) zijn voorzien bij wet, (2) een legitiem doel dienen en (3) noodzakelijk zijn in een democratische samenleving. Het is vaste rechtspraak van het EHRM om niet te definiëren wat privacy is – dat werd in de jaren negentig zelfs onmogelijk en onnodig geacht.[3] In plaats daarvan wordt volgens bovenstaand stramien steeds vastgesteld of sprake is van een (toegestane) inbreuk op het recht op privacy.

6. Het Hof stelt in deze uitspraak eerst vast of er sprake is van een inbreuk op het recht op privacy en vervolgens of deze inbreuk is toegestaan. Het nemen van een foto en het vastleggen van de foto in een politiedatabank met de mogelijkheid dat deze vervolgens geautomatiseerd wordt verwerkt, is een inbreuk op art. 8 EVRM.[4] Het afnemen van vingerafdrukken is eveneens een inbreuk op het recht op privacy.[5] Het vastleggen van persoonlijke gegevens, zoals contactgegevens van veroordeelden is ook een inbreuk op art. 8 EVRM.[6] In deze zaak zijn verder handpalmafdrukken afgenomen en is een beschrijving van verdachte opgesteld en in de politiedatabanken opgenomen, hetgeen een verdere inbreuk op art. 8 EVRM is. Alles bij elkaar is er geen twijfel dat in deze zaak sprake is van een inbreuk op het recht op privacy.

7. De volgende vraag is of die inbreuk op art. 8 EVRM gerechtvaardigd is. Daarvoor moet aan drie voorwaarden zijn voldaan. De eerste voorwaarde is dat de inbreuk bij wet moet zijn voorzien. De betreffende wetgeving moet voldoende toegankelijk en voorzienbaar zijn en met voldoende nauwkeurigheid zijn geformuleerd voor rechtssubjecten.[7] Dit wordt marginaal getoetst door het EHRM. In het geval van opslag van gegevens van een verdachte komt daar bij dat er in minimum waarborgen moet zijn voorzien, waaronder beperkingen in duur, opslag en gebruik van de gegevens en toegang door derden, procedures voor integriteit en vertrouwelijkheid van de gegevens en procedures voor het vernietigen van de gegevens. Dit alles om misbruik te voorkomen.[8]

8. De wet die in deze zaak de uitzondering op art. 8 EVRM zou moeten rechtvaardigen is het Duitse wetboek van strafvordering, in het bijzonder art. 81b. Dit artikel is zonder meer goed toegankelijk voor burgers en is volgens het Hof geformuleerd met een hoge mate van nauwkeurigheid. Het artikel is expliciet in het benoemen foto's en vingerafdrukken van verdachten en noemt ook andere metingen en vergelijkbare maatregelen. Hieronder kunnen de handpalmafdrukken en persoonsbeschrijvingen worden geschaard. Volgens het Hof is dit

voldoende voorzienbaar.

9. De tweede voorwaarde is dat de inbreuk een legitiem doel dient. De mogelijke legitieme doelen zijn uitputtend opgesomd in art. 8 EVRM: nationale veiligheid, openbare veiligheid, economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden en de bescherming van de rechten en vrijheden van anderen. *In casu* worden de gegevens afgenomen en vastgelegd om het opsporen van toekomstige delicten te faciliteren. Daarmee wordt het voorkomen van strafbare feiten en het beschermen van rechten van anderen gediend, hetgeen beide legitieme doelen zijn.

10. De derde voorwaarde is dat de inbreuk noodzakelijk is in een democratische samenleving. Het noodzakelijkheidscriterium kan op verschillende manieren worden ingevuld. Op grond van EHRM-rechtspraak moet hierbij gekeken worden naar de vraag of sprake is van een dringende maatschappelijke behoefte en de vraag of de maatregel proportioneel is in verhouding tot het doel dat wordt nagestreefd.[9] Soms wordt de noodzakelijkheidstoets daarom ook wel aangeduid als een proportionaliteitstoest, omdat de nadruk ligt op het afwegen van verschillende belangen.[10] Echter, het EHRM gebruikt doorgaans weinig tot geen verdere structurering bij de nadere invulling van de noodzakelijkheidstoets.[11] De meest heldere jurisprudentie op dit punt stelt in elk geval dat de onderbouwing door de autoriteiten relevant en voldoende moet zijn.[12]

11. Een heldere en algemeen geaccepteerde structurering van het noodzakelijkheidscriterium is die van Alexy, die drie toetsen onderscheidt om dit te beoordelen.[13] Ten eerste is dat effectiviteit, waarbij moet worden onderzocht of de maatregel kan bijdragen aan het beoogde doel. In feite gaat het dan om bruikbaarheid: kan de maatregel überhaupt iets bijdragen en, zo ja, is dat substantieel? Ten tweede gaat het om subsidiariteit, waarbij moet worden onderzocht of er alternatieven zijn die minder of geen inbreuk maken op het recht op privacy. Als hetzelfde doel ook op minder ingrijpende wijze (voor verdachte) bereikt kan worden, dan heeft dat de voorkeur. Dit criterium ligt vaak lastig, omdat andere methoden doorgaans ook een andere effectiviteit met zich brengen. Ten derde moet gekeken worden naar proportionaliteit *strictu sensu*, waarbij moet worden afgewogen of de impact van een maatregel proportioneel is in verhouding tot de doelen waaraan de maatregel moet bijdragen.

12. Als het gaat om persoonsgegevens, biedt richtlijn 2016/680 verdere aanknopingspunten voor de invulling van het noodzakelijkheidscriterium. Zo is in artikel 4 van de richtlijn onder meer geregeld dat de gegevens rechtmatig en eerlijk worden verwerkt, voor welbepaalde, uitdrukkelijk omschreven en legitieme doelen, toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot die doelen. De gegevens dienen juist en actueel te zijn en

onverwijld te kunnen worden gewist of gerectificeerd. Betrokkenen moeten niet langer geïdentificeerd kunnen worden dan noodzakelijk voor de betreffende doelen. De gegevens moeten middels passende technische en organisatorische middelen voldoende beveiligd zijn tegen ongeoorloofde of onrechtmatige toegang en tegen onopzettelijk verlies, vernietiging of beschadiging. Conform art. 5 van de richtlijn moeten lidstaten passende termijnen vastleggen voor het wissen van de gegevens.

13. Hoewel het EHRM in deze zaak niet al deze criteria stapsgewijs naloopt, wordt de noodzakelijkheidstoets uitgebreid in ogenschouw genomen. Het vormt de kern van deze uitspraak. In de noodzakelijkheidstoets die het Hof uitvoert in deze zaak, lopen bovengenoemde criteria door elkaar heen.

14. Wat betreft de opslag en verwerking van de gegevens stelt het Hof dat de Duitse wetgeving afdoende waarborgen biedt, waaronder specifieke termijnen voor het beoordelen of de gegevens nog steeds nodig zijn en de vuistregel dat gegevens na vijf jaar worden gewist. Ook kunnen betrokkenen verzoeken de gegevens te laten verwijderen als ze kunnen aantonen dat hun gedrag toont dat de gegevens niet langer nodig zijn.

15. Het Hof gaat nauwelijks in op de effectiviteit van de gegevens en lijkt dit impliciet aan te nemen. Het beoogde doel van de gegevens is het kunnen identificeren van de verdachte in geval van toekomstige delicten (en daarmee het voorkomen danwel opsporen van die toekomstige delicten). Het ligt voor de hand dat foto's, persoonsbeschrijvingen, vingerafdrukken en handpalmafdrukken daaraan bijdragen.

16. Op het subsidiariteitscriterium gaat het Hof wel uitgebreid in, iets dat doorgaans niet gebeurt. Zo stelt het Hof dat identificatie en het opsporen van toekomstige delicten ook zou kunnen plaatsvinden via het afnemen van celmateriaal en de opslag van DNA-profielen, maar dat dit veel ingrijpender zou zijn voor de privacy van betrokkene, omdat dit aanzienlijk meer en gevoeligere informatie zou omvatten.[14]

17. Bij het proportionaliteitscriterium weegt het Hof af dat de ernst en omvang van de eerdere delicten waarvoor verdachte is veroordeeld doorslaggevend zijn. Hoewel de meeste delicten op diens strafblad van langer geleden dateren, recidiveerde verdachte ook recenter. Het Hof leidt daaruit af dat verdachte mogelijk weer kan recidiveren en dat rechtvaardigt de opslag van de identificerende gegevens door de politie. Het feit dat verdachte niet is veroordeeld voor het feit dat aanleiding vormde voor deze zaak (de fietsenheling in 2011) doet volgens het Hof daar niets aan af.

18. De proportionaliteitsafweging van het Hof is het punt dat de meeste twijfels oproept. Hoewel het goed na te volgen is dat verdachte weer zou kunnen recidiveren, beklijft het gevoel

dat verdachte op deze manier nooit met een schone lei kan beginnen. De kans dat iemand een delict begaat wordt bij uitstek bepaald door de factor of iemand eerder een delict heeft begaan.[15] Bovendien kunnen, naarmate meer gegevens worden verzameld, meer en betere voorspellingen worden gedaan, hetgeen een grotere inbreuk op de privacy kan vormen.[16] Het zou betekenen dat gegevens van iedereen met een strafblad in de politiedatabanken moeten blijven met het oog op potentiële toekomstige misdrijven, maar dat zou disproportioneel zijn.

19. Om deze redenering de pas af te snijden, vergelijkt het Hof deze zaak expliciet met de *landmark cases S. en Marper t. Verenigd Koninkrijk* en *M.K. t. Frankrijk*.[17] In die zaken was geen sprake van eerdere veroordelingen, stelt het Hof, hetgeen maakt dat in deze zaak de proportionaliteitsafweging anders ligt. Bovendien was in de *Marper*-zaak sprake van gegevensopslag met onbepaalde termijn en in de *M.K.*-zaak sprake van opslagtermijnen van 25 jaar. In een andere zaak, *Trajkovski en Chipovski t. Noord-Macedonië*, achtte het Hof opslag van DNA-gegevens voor onbepaalde termijn disproportioneel.[18] Het Hof acht onbepaalde of zeer langer opslagtermijn disproportioneel, maar een vijfjaarstermijn dus niet.

Conclusie

20. Alles bij elkaar zou geredeneerd kunnen worden dat dit geen bijzondere uitspraak is: het Hof loopt, zoals in zovele zaken, de criteria na of een inbreuk op art. 8 EVRM gerechtvaardigd is en de afwegingen bij elke stap zijn niet nieuw. Toch is deze uitspraak interessant, omdat getoond wordt dat privacy en opsporing niet lijnrecht tegenover elkaar hoeven te staan, zoals soms onterecht wordt verondersteld.[19] Zoals opsporingsdiensten bij de invoering van de cautie of na het *Salduz*-arrest[20] dachten dat het hun werk lastig of onmogelijk zou maken, zo werd ook bij de invoering van steeds gedetailleerdere wetgeving op het gebied van privacy en gegevensbescherming gedacht dat dit contraproductief zou werken.[21] In feite laat het Hof nu zien dat het naleven van privacy in de opsporing dus gewoon kan, mits dit zorgvuldig is geregeld. Het is pas zorgvuldig als enerzijds steeds een afweging wordt gemaakt of gegevens mogen worden verzameld en verwerkt en anderzijds als daarbij de beginselen voor eerlijke gegevensverwerking worden nageleefd.

21. Het Hof lijkt met deze uitspraak een (kleine) correctie aan te brengen op de zaken *Marper* en *M.K.*. In die zaken werd de autoriteiten de wacht aangezegd en een stevige lijn in het zand getrokken, terwijl in deze zaak weer enige ruimte wordt geboden. Zonder af te doen aan de eerdere uitspraken, wordt hier (bijna als een *best practice*) geformuleerd hoe privacy en opsporing wel degelijk goed samen kunnen gaan. Het Hof lijkt deze zaak zelfs hierop geselecteerd te hebben, want de zaak was nauwelijks ontvankelijk: alle eerdere nationale rechters hadden hetzelfde oordeel en de hoogste nationale rechter vond het niet de moeite

waard de zaak in behandeling te nemen.

22. Het is niet geheel toevallig dat dit een Duitse zaak is. Uit vergelijkend empirisch onderzoek blijkt dat de bescherming van de privacy in Duitsland aanzienlijk beter geregeld is dan in de meeste andere lidstaten.[22] Dit lijkt sterk verbonden met de teleologische benadering van het privacy- en gegevensbeschermingsrecht in Duitsland, voortkomend uit de nationale geschiedenis van het land, in tegenstelling tot de veel meer positiefrechtelijke benadering in Frankrijk en Italië of de pragmatische instelling in het Verenigd Koninkrijk.[23] Het Hof laat in elk geval doorschemeren dat de aanpak in het Verenigd Koninkrijk (de *Marper*-zaak) en Frankrijk (de *M.K.*-zaak) niet de juiste balans wist te treffen.

Bart Custers[24]

[1] Leiser M.R. & Custers B.H.M. (2019), The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *European Data Protection Law Review* 5(3): 367-378.

[2] https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html. Deel 1 gaat over het verzamelen van gegevens, deel 2 gaat over het verwerken en gebruik van gegevens.

[3] *Niemietz t. Duitsland*, EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088.

[4] *Gaughran t. Verenigd Koninkrijk*, EHRM 13 februari 2020, nr. 45245/15, ECLI:CE:ECHR:2020:0213JUD004524515, par. 65-70, «EHRC Updates» 2020-86 m.nt. B. van der Sloot.

[5] *S. en Marper t. Verenigd Koninkrijk*, EHRM (GK) 4 december 2008, nrs. 30562/04 en 30566/04, par. 78-86, «EHRC» 2009/13 m.nt. B.J. Koops; *M.K. t. Frankrijk*, EHRM 18 april 2013, nr. 19522/09, ECLI:CE:ECHR:2013:0418JUD001952209, par. 26, «EHRC» 2013/187; *Gaughran t. Verenigd Koninkrijk*, par. 65-70.

[6] *Gardel t. Frankrijk*, EHRM 17 december 2009, nr. 16428/05, ECLI:CE:ECHR:2009:1217JUD001642805, par. 58.

[7] *Malone t. Verenigd Koninkrijk*, EHRM 2 augustus 1984, nr. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, par. 66-68, Series A no. 82; *Rotaru t. Roemenië*, EHRM (GK) 4 mei 2000, nr. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, par. 55, «EHRC» 2000/53 m.nt. E. Brems; *S. en Marper*, par. 95; *M.K.*, par. 30. *Sunday Times t. Verenigd Koninkrijk*, EHRM 26 april 1979, nr. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874.

[8] *Rotaru*, par. 56-59; Association for European Integration and Human Rights en Ekimdzhiev t. Bulgarije, EHRM 28 juni 2007, nr. 62540/00, ECLI:CE:ECHR:2007:0628JUD006254000, par. 75-77.

[9] *Sunday Times*.

[10] P. Craig and G. De Burca, *eu Law* (Oxford: Oxford University Press, 2011).

[11] J. Gerards, 'How to improve the necessity test of the European Court of Human Rights', 11 *International Journal of Constitutional Law* (2013) 466–490.

[12] *S. en Marper*, par. 101; *M.K.*, par. 33.

[13] R. Alexy, 'Constitutional Rights, Balancing and Rationality', 16 *Ratio Juris* (2003) 131–140. Zie ook Pool R.L.D & Custers B.H.M. (2017), The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European journal of crime, criminal law and criminal justice*25(2): 123-144.

[14] Cf. *Trajkovski en Chipovski t. Noord-Macedonië*, EHRM 13 februari 2020, nrs. 53205/13 and 63320/13, ECLI:CE:ECHR:2020:0213JUD005320513, «EHRC Updates» 2020/93 m.nt. B. van der Sloot.

[15] Dressel, J., and Farid, H. (2018) The accuracy, fairness and limits of predicting recidivism, *Science Advances*, Vol. 4, No. 1.

[16] Custers B.H.M. (2012), Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination, *Privacy Observatory Magazine* 2012(3).

[17] *S. en Marper*, *M.K.*.

[18] *Trajkovski en Chipovski*.

[19] Cf. Wely, M. van (2019) 'Ik word echt verdrietig van corruptiezaken', *Telegraaf*, 14 maart 2019.

[20] Salduz t. Turkije, EHRM 26 April 2007, nr. 36391/02, ECLI:CE:ECHR:2007:0426JUD003639102,

[21] Cf. Krebs, C. (2018) Who is afraid of more spams and scams? Krebs on Security, 16 March 2018, https://krebsonsecurity.com/2018/03/who-is-afraid-of-more-spams-and-scams/

[22] Custers, B.H.M., Sears A.M., Dechesne F., Georgieva I.N., Tani T. & Hof S. van der (2019),

EU Personal Data Protection in Policy and Practice. Information technology & law series nr. 29. Heidelberg: Asser/Springer.

[23] Mulligan, D.K. and Bamberger, K.A. (2015) *Privacy on the Ground in the United States and Europe*, MIT Press.

[24] Prof.mr.dr.ir. B.H.M. (Bart) Custers is hoogleraar Law & Data Science em directeur van eLaw, het centrum voor recht en digitale technologie van de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden.