

ANNOTATIE

# Glukhin t. Rusland (EHRM, 11519/20) – Gezichtsherkenning alleen in uitzonderlijke gevallen

**B. van der Sloot**

*Annotatie bij Europees Hof voor de Rechten van de Mens, 04-07-2023,  
ECLI:CE:ECHR:2023:0704JUD001151920 (EHRC-2023-0183)*

1. De zaak betreft een veroordeling van de klager omdat hij de Russische autoriteiten niet in kennis had gesteld van zijn voornemen om een solodemonstratie te houden. Tijdens het strafrechtelijk onderzoek zou de politie gezichtsherkenningstechnologie hebben gebruikt om zijn identiteit te achterhalen. Hij klaagt over een schending van de art. 6, 8 en 10 EVRM. Het EHRM velde een oordeel over de laatste twee bepalingen en stelt dat het derhalve onnodig is om de klacht onder het recht op een eerlijk proces op zijn eigen merites te beoordelen.

2. Wat art. 10 EVRM betreft, stelt het EHRM vast dat er duidelijk sprake was van een inmenging. Vervolgens wijst het EHRM er op dat de rechtsgrondslag op basis waarvan verzoeker werd gearresteerd was dat hij een "snel (de)gemonteerd voorwerp" bij zich had. Tegelijkertijd wijst het Hof erop dat de wet geen criteria bevatte die iemand in staat stelden te voorzien welk soort voorwerpen onder die bepaling zouden vallen. Het EHRM wijst op de aard van de solodemonstratie van de verzoeker, op het gebrek aan juridische helderheid op nationaal niveau, zoals aangaande de werkingssfeer en de wijze van toepassing van de relevante bepalingen door hogere Russische rechtscolleges en op het ontbreken van een gedetailleerde analyse in het specifieke geval van de verzoeker. Daarom oordeelt het EHRM dat er reden is of de juridische praktijk in Rusland voldoende voorzienbaar was om aan het vereiste van de kwaliteit van wet (*quality of law*) te voldoen. Interessant is dat het Hof vervolgens voor een dubbele voorwaardelijke benadering kiest als het stelt dat zelfs als de inmenging aan het 'voorgeschreven bij wet'-criterium zou voldoen en zelfs als de maatregel de

legitieme doelen van "het voorkomen van wanordelijkheden" en "de bescherming van de rechten van anderen" nastreefde, de inmenging niet noodzakelijk in een democratische samenleving zou zijn. De autoriteiten legden namelijk niet de vereiste mate van tolerantie aan de dag ten aanzien van de vreedzame solodemonstratie van verzoeker.

3. Het gebruik van gezichtsherkenningstechnologie beoordeelt het EHRM onder art. 8 EVRM. Daarover stelt het Hof vast dat de politie tijdens routinematige controle van het internet foto's en een video ontdekte van verzoeker die een solodemonstratie hield, gepubliceerd op een openbaar Telegram-kanaal. De politie maakte vervolgens screenshots van het Telegram-kanaal, sloeg deze op en paste naar verluidt gezichtsherkenningstechnologie toe om verzoeker te identificeren, te lokaliseren en te arresteren. Naar verluidt, omdat de regering niet wilde reageren op het vermoeden van het gebruik van gezichtsherkenningssoftware en de politie niet verplicht was om registers bij te houden van hun gebruik van dergelijke technologie. De overheid heeft volgens het Hof echter wel impliciet het gebruik ervan erkend, onder andere toen zij verwees naar de juridische grondslag voor het gebruik van deze technologie. Daarom vindt het Hof het aannemelijk dat deze technologie werd gebruikt en dat er sprake was van een inbreuk op het recht op privacy van verzoeker.

4. Wat de legitimiteit van de inmenging betreft, betwijfelt het Hof sterk of de nationale wettelijke bepalingen voldoen aan het vereiste van *quality of law*, omdat de nationale wetgeving de verwerking van biometrische persoonsgegevens toestaat "in connection with the administration of justice", een erg ruime formulering. Bovendien is de verwerking van biometrische persoonsgegevens - zoals met behulp van gezichtsherkenningstechnologie - toegestaan in verband met elke gerechtelijke procedure. Het Hof geeft echter geen eindconclusie op dit punt, noch over de vraag of een legitiem belang werd gediend met de inbreuk; het EHRM merkt slechts op dat het zal uitgaan van de veronderstelling dat met de betwiste maatregelen het legitieme doel van misdaadpreventie werd nagestreefd.

5. Wat betreft de proportionaliteit van de inmenging benadrukt het Hof dat misdaadbestrijding uiteraard een belangrijke taak van de overheid is en dat nieuwe technologieën, waaronder gezichtsherkenning, onmisbaar kunnen zijn in die strijd. Maar live gezichtsherkenning is bijzonder ingrijpend in termen van privacy. Bovendien betroffen de persoonsgegevens onder meer de deelname aan een vreedzaam protest en onthulden dus zijn politieke mening, een bijzonder gevoelig persoonsgegeven, waarvoor een hoger beschermingsniveau geldt. Niet alleen is het gebruik van gezichtsherkenning in dit geval op zich onevenredig (art. 8 EVRM), het Hof is ook van oordeel dat het gebruik van zeer indringende gezichtsherkenningstechnologie voor het identificeren en arresteren van deelnemers aan vreedzame protestacties een *chilling effect* kan hebben met betrekking tot het recht op vrijheid van meningsuiting en vergadering.

6. Met zijn redelijk strenge aanpak op het vlak van gezichtsherkenning kiest het EHRM voor een benadering die gelijk is aan die van de EU. In de Algemene Verordening Gegevensbescherming[1] wordt het verwerken van biometrische gegevens sterk aan banden gelegd. Daarin zijn biometrische gegevens gedefinieerd als ‘persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens’.[2] Alhoewel er uitzonderingen mogelijk zijn is de verwerking van deze gegevens in principe verboden: ‘Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.’[3] De voorgestelde AI Act[4] definieert biometrische gegevens als: “biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens’.[5] Het verbiedt onder meer ‘het gebruik van biometrische systemen voor de identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving, tenzij en voor zover een dergelijk gebruik strikt noodzakelijk is voor’ het tegengaan van zware misdaad.[6] Andere AI systemen worden aangemerkt als hoog risico systemen,[7] waardoor tal van verplichtingen moeten worden nageleefd.[8] Ook Daarmee komt deze uitspraak de juridische consistentie tussen de Raad van Europa en de Europese Unie ten goede.

7. Wat echter opvalt is dat het EHRM niet uitlegt waarom deze techniek nu zo ingrijpend is. In die zin staat deze uitspraak in lijn met een keuze die het EHRM heeft gemaakt in het kader van juridische efficiëntie. Steeds vaker wijst het zaken waarin het niet uit de doeken doet wat de omstandigheden van het geval waren, maar simpelweg stelt dat het bijvoorbeeld om adoptie zonder toestemming ging,[9] waarin het de verschillende klagers in een zaak toelicht in een annex,[10] waarin ook hun claims staan, waarin het voor de inhoudelijke beoordeling van de zaak verwijst naar eerdere jurisprudentie, die het Hof ook op de zaak die dan bij hem voorligt van toepassing vindt,[11] en waarin voor de beoordeling van de eventueel toe te wijzen vergoedingen simpelweg verwijst naar de annex en stelt dat het de daarin gevraagde bedragen zal toekennen.[12] Vanuit het oogpunt van werkdruk is deze nieuwe houding begrijpelijk, maar de juridische begrijpelijkheid en rechtsvorming komt het niet ten goede. Eigenlijk zegt het Hof in deze zaken niet veel meer dan dat er een schending is van het EHRM,

zonder verder uit te leggen waarom dat zo is.

Bart van der Sloot

[1] 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).

[2] Artikel 4 lid 14 AVG.

[3] Artikel 9 lid 1 AVG.

[4] Voorstel Voor Een Verordening Van Het Europees Parlement En De Raad Tot Vaststelling Van Geharmoniseerde Regels Betreffende Artificiële Intelligentie (Wet Op De Artificiële Intelligentie) En Tot Wijziging Van Bepaalde Wetgevingshandelingen Van De Unie {Sec(2021) 167 Final} - {Swd(2021) 84 Final} - {Swd(2021) 85 Final}.

[5] Artikel 3 lid 33 AI Act.

[6] Artikel 4 AI Act.

[7] Bijlage 3 artikel 1 (a) AI Act.

[8] Titel III hoofdstuk 2 AI Ac.

[9] Zie bv meest recent: ECLI:CE:ECHR:2023:0912JUD003976917 en ECLI:CE:ECHR:2023:0912JUD006330717 en ECLI:CE:ECHR:2023:0912JUD000353715.

[10] Zie bv meest recent: ECLI:CE:ECHR:2023:0907JUD007523117

[11] Zie bv meest recent: ECLI:CE:ECHR:2023:0914JUD004176120.

[12] Zie bv meest recent: ECLI:CE:ECHR:2023:0914JUD002728417 en ECLI:CE:ECHR:2023:0914JUD003038919.