EGMR: Konventionswidriger Einsatz von Gesichtserkennungstechnologie bei Demonstrationsüberwachungen

» jusIT 2023/119

§ EMRK: Art 6, 8, 10
ABGB: §§ 16, 20
UrhG: § 78

EGMR 4. 7. 2023, 11519/20 (Glukhin/Russland)

1. Lassen sich aus personenbezogenen Daten auch Informationen über die Teilnahme an einer öffentlichen Demonstration ableiten, so können Rückschlüsse auf die politische Meinung gezogen werden. Dabei handelt es sich um besonders schutzwürdige („*sensible*“) Daten, denen nach Art 8 EMRK ein erhöhtes Schutzniveau gegenüber staatlichen Eingriffen zukommt.
2. Setzen die Sicherheitsbehörden Verfahren zur Identifizierung oder Bestätigung der Identität einer Person anhand ihres Gesichts (sog „*Gesichtserkennungstechnologie*“) ein, um an (friedlichen) Protestaktionen teilnehmende Personen zu überprüfen, so liegt ein Eingriff in die Privatsphäre der Betroffenen vor, an dessen Rechtfertigung in einer demokratischen Gesellschaft besonderes hohe Anforderungen zu stellen sind.
3. Dem Einsatz von (Live-)Gesichtserkennungstechnologie kommt eine abschreckende Wirkung („*chilling effect*“) betreffend die Ausübung des Rechts auf freie Meinungsäußerung und Versammlungsfreiheit zu, denn das Bewusstsein, „*verfolgt*“ zu werden, könnte davon abhalten, die eigene Meinung im öffentlichen Raum frei zu äußern.

Anmerkung des Bearbeiters:

Im aus Russland stammenden Beschwerdefall wurde der spätere Kläger von der Polizei in einem Zug der Moskauer Metro festgenommen. Die Polizei teilte ihm mit, dass sein Name auf der Fahndungsliste stehe und er von den in der Metro installierten Kameras zur Gesichtserkennung identifiziert worden sei. Anschließend wurde er wegen Verstoßes gegen die Vorschriften für öffentliche Veranstaltungen verurteilt, weil er im August 2019 in der Moskauer Metro eine lebensgroße menschliche Pappfigur des politischen Aktivisten *Konstantin Kotov* mit der englischsprachigen Aufschrift „*You must be f***king kidding me*“ zur Schau gestellt hatte. Die von der Polizei gegen ihn vorgelegten Beweise umfassten Screenshots eines auf einem öffentlichen Telegram-Kanal veröffentlichten Videos und Screenshots von Aufnahmen der Überwachungskameras der Metro. Die inländischen Gerichte befanden, dass der Antragsteller eine Solo-Demonstration mit einem „*schnell (de)montierten Objekt*“ abgehalten hatte und daher eine vorherige Anmeldung bei den örtlichen Behörden hätte einreichen müssen. Er wurde zu einer Geldstrafe iHv umgerechnet ca € 283 verurteilt. Der Kläger rügte im innerstaatlichen Rechtsschutzverfahren insb, dass die zur Identifizierung seiner Person durchgeführten operativen Fahndungsmaßnahmen rechtswidrig waren, insb seine geschützte Privatsphäre und seine Meinungsäußerungsfreiheit verletzt hätten. Die erlangten Beweismittel wären daher unverwertbar. Die russischen Gerichte bestätigten die Geldstrafe, da die Solo-Demonstration nicht gehörig angemeldet worden war.

Im daraufhin angestrengten Verfahren vor dem EGMR machte der Beschwerdeführer (Bf) die Verletzung von Art 6 EMRK, seines Rechts auf Privatleben nach Art 8 EMRK sowie der Freiheit der Meinungsäußerung gem Art 10 EMRK geltend.

Die Dritte Kammer gab der Beschwerde Folge und hielt einstimmig fest, dass der russische Staat sowohl die Meinungsfreiheit als auch die Privatsphäre des Bf verletzt hatte. Über die „*Qualität*“ des Verwaltungsstrafverfahrens sprach der EGMR angesichts der beiden gravierenden Konventionsverstöße nicht mehr ab, sondern anerkannte zugunsten des Bf einen Betrag iHv € 9.800 an immateriellem Schadenersatz und € 6.400 für Kosten und Auslagen.

Das vorliegende Urteil macht ganz deutlich, dass durch den Einsatz von Gesichtserkennungstechnologie zur Identifizierung und späteren Verhaftung in das Recht auf Achtung des Privatlebens des Betroffenen eingegriffen wird. Der Eingriff ist schon deshalb besonders schwerwiegend gewesen, weil es sich um eine friedliche Protestaktion – ohne Anzeichen oder Vorkommnisse von Gewalt – gehandelt hat. Nach den Feststellungen müsse die russische Polizei den Einsatz von Gesichtserkennung nicht dokumentieren und Betroffene würden nicht darüber informiert (Rz 60 ff des Urteils). Deshalb sei es für den Kläger schwierig gewesen, den Einsatz in seinem Fall zu beweisen. Nach Ansicht der Straßburger Richter:innen gibt es jedoch keine andere Erklärung dafür, dass die Polizei ihn so schnell nach seinem Protest identifizieren konnte; außerdem hätten die Regierungsvertreter den Einsatz auch nicht bestritten. Zudem gebe es zahlreiche weitere Fälle, in denen Demonstranten in Russland mit Gesichtserkennung identifiziert wurden (Rz 69 ff des Urteils).

Der Gerichtshof stellt fest, dass der Kläger wegen einer geringfügigen Straftat verfolgt wurde, die darin bestand, dass er ohne vorherige Anmeldung eine Einzeldemonstration abhielt. Anknüpfungspunkt für die Verhältnismäßigkeitsprüfung bildet also eine bloße Ordnungswidrigkeit bzw Verwaltungsübertretung und nicht eine Kriminalstraftat. Dem Bf wurde nie vorgeworfen, während seiner Demonstration verwerfliche Handlungen wie Verkehrsbehinderung, Sachbeschädigung oder Gewalttaten begangen zu haben. Es wurde nie behauptet, dass seine Aktionen eine Gefahr für die öffentliche Ordnung oder die Verkehrssicherheit darstellten. Damit war der Einsatz von Gesichtserkennungstechnologie überschießend und nicht erforderlich gewesen und wirkte abschreckend (Rz 88 des Urteils). Unter diesen Umständen entsprach der Einsatz der Gesichtserkennungstechnologie zur Identifizierung des Bf anhand der auf Telegram veröffentlichten Fotos und des Videos – und erst recht der Einsatz der Live-Gesichtserkennungstechnologie zur Lokalisierung

und Verhaftung des Beschwerdeführers, während er in der Moskauer U-Bahn unterwegs war – nicht einem „*dringenden gesellschaftlichen Bedürfnis*“ iSv Art 8 EMRK (Rz 89 des Urteils).

Ausblick: Die Entscheidung aus Straßburg dürfte weit über den bloßen Anlassfall hinauswirken, handelt es sich bei der Gesichtserkennung doch nur um eine Kategorie der biometrischen Sicherheit, maW der Vermessung biometrischer Merkmale zum automatischen Abgleich, um Zutritt zu gewähren oder Anwendungen freizuschalten. Weitere Arten biometrischer Software sind bspw die Spracherkennung, die Fingerabdruckerkennung sowie die Netzhaut- oder Iriserkennung. Die Technik wird größtenteils zu Sicherheitszwecken und zur Strafverfolgung eingesetzt, wenngleich sie auch in anderen Einsatzbereichen längst Teil der (digitalen) Realität ist. Denn Biometrie-Scanner werden immer ausgeklügelter. Die Technik zur Gesichtserkennung auf dem *iPhone X* von *Apple* bspw projizierte 30.000 Infrarotpunkte auf das Gesicht des Benutzers, um diesen anhand eines Musterabgleichs zu authentifizieren. Die Wahrscheinlichkeit eines Fehlers bei diesem Abgleich liegt bei eins zu einer Million. Seit dem Modell *iPhone 12* erkennt *Face ID* auch Personen unter einer Corona-Maske. Die aktuelle TrueDepth-Kamera zur Gesichtserkennung ist mit einem selbstlernenden KI-Algorithmus ausgestattet. Art 6 Abs 2 iVm Anhang III des Kommissions-Entwurfes zu einem Gesetz über Künstliche Intelligenz stuft die Gesichtserkennung als Hoch-Risiko-KI-System ein (vgl dazu jüngst *Burtscher/Fellner/Raabe-Stuppnig*, Klassifizierung und Risikobewertung von KI-Systemen nach dem Entwurf für ein EU Gesetz über Künstliche Intelligenz, ZIIR 2023, 382 [392 ff]).

Zusammenfassend hat der EGMR den Einsatz von Gesichtserkennungstechnologie durch die Sicherheitsbehörden zur präventiven Identifikation von Demonstrant:innen bei friedlichen und ohne Störung verlaufenden Protestaktionen aufgrund der abschreckenden Wirkung als eine Verletzung der Meinungs- und Versammlungsfreiheit qualifiziert.

Bearbeiter: Clemens Thiele

EGMR: Anlasslose Massenüberwachung der Internetkommunikation ist dem überwachenden Staat zuzurechnen, auch wenn sich die Grundrechtsträger im Ausland aufhalten

» jusIT 2023/120

§ EMRK: Art 8

EGMR 12. 9. 2023, 64371/16 und 64407/16 (Wieder und Guarnieri/Vereinigtes Königreich)

1. Ein innerstaatliches Rechtsmittel muss vor der Beschwerde an den EGMR nur ergriffen werden, wenn sein Bestehen hinreichend klar ist. Eine erst später erfolgte positive Klärung durch ein innerstaatliches Höchstgericht führt nicht zur Unzulässigkeit der bereits anhängigen Beschwerde.
2. Ein Grundrechtseingriff durch Abfangen, Durchsuchen, Auswerten und Verwerten einer Kommunikation findet am Ort dieser Vorgänge statt, unabhängig davon, ob sich der Grundrechtsträger im Gebiet des handelnden Staates aufhält.
3. Das „*Bulk-interception*“-Regime durch das *United Kingdom Government Communications Headquarters* („*GCHQ*“) ist, wie in der Rsp des EGMR schon festgestellt, nach wie vor konventionswidrig.

Anmerkung des Bearbeiters:

Die Beschwerdeführer waren *Joshua Wieder*, ein amerikanischer Staatsangehöriger, der in Florida lebt, und *Claudio Guarnieri*, ein italienischer Staatsangehöriger, der in Berlin lebt. In den zur Verhandlung verbundenen Beschwerden ging es vorrangig um die Frage, ob sich die für eine Passivlegitimation vor dem EGMR maßgebliche „*jurisdiction*“ des Konventionsstaats auch auf Fälle erstreckt, in denen sich die Grundrechtsträger nicht im betreffenden Staat aufhalten.

Die Anknüpfung muss diesfalls anhand des Durchgangs der Kommunikation durch den Konventionsstaat erfolgen, da das Abfangen, Durchsuchen, Auswerten und Verwerten einer Kommunikation im betreffenden Staat erfolgt. Dies hat der EGMR zutreffend bejaht und ua mit einer Analogie zum Schutz der Wohnung begründet: Es könne nicht ernsthaft behauptet werden, dass die Durchsuchung einer Wohnung dann nicht dem Staat zuzurechnen wäre, wenn die Person, zu deren Privatsphäre diese Wohnung gehört, im Ausland weilt (Rz 93 des Urteils). Diese Überlegung lässt sich ebenso zB auf Briefe, Datenträger und andere von der Person gelöste Aspekte der Privatsphäre ausdehnen. Solche Eingriffe muss sich der jeweilige Konventionsstaat zurechnen lassen.

Zur materiellen Grundrechtsprüfung bringt das Urteil wenig Neues, da der EGMR schon zuvor die „*bulk interception*“ des GCHQ als zu weitgehend und zu wenig überprüfbar verurteilt hatte (EGMR 25. 5. 2021, 58170/13 ua [Big Brother Watch ua/Vereinigtes Königreich], jusIT 2021/68, 188 [*Thiele*]): Das Fehlen einer unabhängigen Anordnung, das Fehlen spezifischer Angaben im Antrag auf eine Anordnung und das Fehlen einer eigenen Prüfung der Verbindung zur Einzelperson (Rz 104 des Urteils). Der Umstand, inwieweit sich die durch den Supreme Court erweiterte nationale Rechtsschutzmöglichkeit auswirkt, musste offenbleiben, da diese als im Beschwerdezeitpunkt nicht hinreichend klar bestehend qualifiziert worden ist.

Die Beschwerden wurden, soweit sie sich auf das „*intelligence sharing*“ mit anderen Nachrichtendiensten bezogen hatten, zurückgezogen und nicht behandelt, da der EGMR im Urteil 25. 5. 2021, 58170/13 ua (Big Brother Watch ua/Vereinigtes Königreich) die diesbezüglichen Regelungen als konventionskonform erkannt hatte.