

Johanna Hahn

Automatisierte Gesichtserkennung in der Strafverfolgung



Nomos

DIKE 

Studien zum Strafrecht

Band 134

Herausgegeben von

Prof. Dr. Martin Böse, Universität Bonn

Prof. Dr. Beatrice Brühöber, Goethe-Universität Frankfurt

Prof. Dr. Gunnar Duttge, Universität Göttingen

Prof. Dr. Karsten Gaede, Bucerius Law School, Hamburg

Prof. Dr. Katrin Höffler, Humboldt Universität zu Berlin

Prof. Dr. Johannes Kaspar, Universität Augsburg

Prof. Dr. Dr. h.c. mult. Urs Kindhäuser, Universität Bonn

Prof. Dr. Hans Kudlich, Universität Erlangen-Nürnberg

Prof. Dr. Dr. Milan Kuhli, Universität Hamburg

Prof. Dr. Henning Radtke, Universität Hannover

Prof. Dr. Frank Saliger, Universität München

Prof. Dr. Helmut Satzger, Universität München

Prof. Dr. Brigitte Tag, Universität Zürich

Prof. Dr. Till Zimmermann, Heinrich-Heine-Universität Düsseldorf

Johanna Hahn

Automatisierte Gesichtserkennung in der Strafverfolgung



Nomos

DIKE

Gedruckt mit freundlicher Unterstützung
des Bundesministeriums des Innern und für Heimat.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische
Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Leipzig, Univ., Diss., 2024

u.d.T.: Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung

1. Auflage 2025

© Johanna Hahn

Publiziert von

Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:

Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-2294-6 (Print)

ISBN 978-3-7489-4945-9 (ePDF)

ISBN 978-3-03891-814-1 (Dike Verlag Zürich/St. Gallen)

DOI: <https://doi.org/10.5771/9783748949459>



Onlineversion
Nomos eLibrary



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung
4.0 International Lizenz.

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2023/24 von der Juristefakultät der Universität Leipzig als Dissertation angenommen. Literatur und Rechtsprechung sind grundsätzlich auf dem Stand vom 31.1.2024. Die Vorgaben der im Juli 2024 veröffentlichten KI-Verordnung der Europäischen Union und einige Beiträge hierzu konnten noch für die Veröffentlichung berücksichtigt werden.

Besonderer Dank gilt an erster Stelle meiner Doktormutter Professorin Elisa Hoven. Sie hat von Anfang an Vertrauen in mich gesetzt, mir große wissenschaftliche Freiheit gelassen und mich immer bei all meinen Vorhaben ganz außergewöhnlich unterstützt. Professor Eric Hilgendorf bin ich zutiefst dankbar für die zügige Erstellung des Zweitgutachtens, seinen fachlichen Rat und für seine Unterstützung meines wissenschaftlichen Wegs.

Die Idee für diese Arbeit stammt aus meiner Station am Bundesministerium der Justiz im Referat RB3 Strafverfahren (Ermittlungsverfahren, Zwangsmaßnahmen) Anfang 2021 unter der Leitung von OStAin BGH Dr. Monika Becker. Als ich mich dort erstmals vertieft mit biometrischer Fernidentifizierung befasste, hat mich dieses Thema gepackt und nicht mehr losgelassen. Professor Eric Hilgendorf und Professor Martin Asholt danke ich dafür, dass sie mit ihren Gutachten für die Studienstiftung des deutschen Volkes bereits zu Beginn Vertrauen in dieses Vorhaben gesetzt haben. Professor Christian Rückert bin ich von Herzen dankbar für den kontinuierlichen Austausch und seine richtungsweisenden Ratschläge an mehreren Stellen des Schreibprozesses. Juniorprofessorin Lucia Sommerer hat mich während der gesamten Promotionszeit durch ihren Rat unterstützt und dadurch maßgeblich zum Gelingen dieser Arbeit beitragen. Professor Hans Kudlich danke ich dafür, dass er mich so herzlich als Habilitandin an seinem Lehrstuhl und im DFG-Graduiertenkolleg „Cyberkriminalität und Forensische Informatik“ aufgenommen hat und mir ermöglicht, meine Forschung zu Strafrecht und neuen Technologien nun auszubauen. Ganz besonders bin ich Professor Jens Bülte dankbar, der mich seit unserem ersten Gespräch zum Tierschutzstrafrecht immer in allen Lebenslagen unterstützt.

Viele der Gedanken in dieser Arbeit stammen aus meiner Zeit an der Harvard Law School. Besonders bereichert haben mich dort die Gespräche

Vorwort

über meine Doktorarbeit mit Professor Christopher Bavitz, Professor James Waldo, Professor Alex Whiting, Professor Jonathan Zittrain und Shira Gur-Arieh. Das Feedback in der Law & Tech Policy Writing Group hat mich ebenso weitergebracht wie der Austausch im Harvard Student Leaders in AI Program am Berkman Klein Center for Internet & Society.

Zutiefst dankbar bin ich auch für die vielen Gespräche über technische Fragen der automatisierten Gesichtserkennung mit Dr. Oren Amsalem (Harvard Medical School), Mathias Ibsen (TU Darmstadt) und vor allem Dr. Martin Knoche (TU München). Unvergleichlich wertvolle Einblicke in die Praxis der Strafverfolgung mit automatisierter Gesichtserkennung ermöglicht haben mir Kay-Uwe Brandt und sein Team (Bundespolizei, Referat 33 – Gesichtserkennung). Die interessanten und kontroversen Diskussionen mit Patrick Rolfes (BKA, Referat ZI 21 – Strategie und Innovation Biometrie) haben mich ebenfalls sehr bereichert. Dr. Lena Leffer danke ich für den fachlichen und persönlichen Austausch über die gesamte Promotionszeit hinweg. Die ideelle und finanzielle Unterstützung der Studienstiftung des deutschen Volkes und der Fulbright Kommission haben dieses Vorhaben enorm erleichtert und mir die nötige Freiheit gegeben. Dem Bundesministerium des Innern und für Heimat danke ich für den gewährten Druckkostenzuschuss. Dr. Maximilian Gerhold, Dr. Nicolai Hahn, Bruno Kaufmann und Dr. Annika Obert haben die Arbeit vollständig oder in großen Teil gelesen. Für ihre Zeit und ihr Feedback bin ich sehr dankbar.

Besonderer Dank gilt darüber hinaus meinen Eltern Bruno und Irmtraud Kaufmann und meinem Bruder Sebastian für ihre Unterstützung bei diesem und all meinen Vorhaben. Meinem Mann Nicolai ist diese Arbeit gewidmet.

Inhaltsverzeichnis

Abbildungsverzeichnis	17
Kapitel I. Grundlagen	19
A. Einführung	19
B. Ziel und Gang der Untersuchung	21
C. Gesichtserkennung in der Strafverfolgung: Abgrenzung und Einsatzszenarien	23
I. Abgrenzung	23
1. Andere Methoden der biometrischen Erkennung	23
2. Andere Formen der Gesichtsanalyse	24
3. Andere Einsatzbereiche	25
II. Einsatzszenarien in der Strafverfolgung	25
1. Identitätsermittlung	26
2. Auswertung von umfangreichem Datenmaterial	27
3. Digitale Beobachtung	28
4. Echtzeit-Fahndung	29
D. Forschungszuschnitt dieser Arbeit	30
I. Besonderes Gefährdungspotenzial der Gesichtserkennung	30
1. Streubreite	31
2. Fehleranfälligkeit	32
3. Heimlichkeit	33
4. Vernetzungsmöglichkeit	34
5. Biometrie	34
6. Fazit	35
II. Relevantestes Einsatzszenario: Identitätsermittlung	36
III. Stand der Forschung und Forschungslücke	36
IV. Notwendigkeit einer Regulierung	38
E. Technologie	39
I. Verifizierung vs. Identifizierung	39
II. Entwicklung der automatisierten Gesichtserkennung	41
1. Anfänge der Forschung	41

Inhaltsverzeichnis

2. Nutzbarmachung für die Strafverfolgung	45
3. Durchbruch durch große Datenbestände und maschinelles Lernen	46
4. Neue Akteure	48
III. Ablauf einer Erkennung	49
IV. Fehlerraten	51
1. Arten von Fehlern	51
a) Falsche Nichttreffer (False negatives)	52
b) Falsche Treffer (False positives)	52
c) Messung	53
2. Ursachen von Fehlern	54
a) Unterschiedliche Leistungsfähigkeit verschiedener Systeme	54
b) Unkooperatives Setting	54
c) Qualität der abzugleichenden Bilder	55
d) Alterung und Gesichtsabnutzung	55
e) Größe der Datenbank	56
f) Gewählter Schwellenwert	56
3. „Erwünschte“ Fehler	57
4. Stand der Technik	58
a) Ergebnisse der Face Recognition Vendor Tests des NIST	58
b) Einordnung	60
5. Höhere Fehlerraten bei einigen Bevölkerungsgruppen	60
6. Fazit	63
F. Einsatz in Deutschland	63
I. Gesichtserkennungssystem GES beim BKA	64
1. Durchsuchbare Datenbank: INPOL-Z	64
2. Ablauf	66
a) Bild eines Tatverdächtigen	66
b) Generierung einer Kandidatenliste	67
c) Überprüfung durch Experten	68
d) Weitere Ermittlungsmaßnahmen	69
e) Case Study einer Recherche im GES	70
3. Keine näheren Informationen über Trainingsprozess des GES	72
4. Keine Evaluierung der grundsätzlichen Leistungsfähigkeit des GES	72

5. Keine Evaluierung der auf GES-Recherchen basierenden Ermittlungsverfahren	73
II. Landeskriminalämter und Landespolizeibehörden	73
1. Schnittstellen zum GES bei den Landeskriminalämtern	73
2. Eigene Systeme beim LKA Bayern und anderen Landespolizeibehörden	74
III. Einordnung	75
G. Chancen und Risiken des Einsatzes	76
I. Potenzial für die Strafverfolgung	76
1. Effizienz	77
2. Einfache Erfassung und Verfügbarkeit von Gesichtsbildern	77
3. Gesichtserkennung als einziger Spurenansatz	79
4. Überprüfbarkeit durch Menschen	80
II. Risiken	81
1. Erfahrung aus anderen Staaten	81
a) USA	81
b) China	84
c) Russland	85
2. Zentrale Probleme	86
a) Fehlidentifizierung und Ermittlungsmaßnahmen gegen Unbeteiligte	87
b) Privatheit der Betroffenen	87
c) Auswirkungen auf die gesamte Gesellschaft	88
3. Relevanz für Deutschland	88
H. Fazit zu Kapitel I. Grundlagen	91
Kapitel II. Rechtlicher Rahmen	93
A. Verfassungsrecht: Anforderungen an die Rechtsgrundlage	93
I. Recht auf informationelle Selbstbestimmung	94
1. Schutzbereich	94
2. Eingriffe und Intensität	97
a) Eingriff	97
aa) Eingriff durch Erstellung der Embeddings	99
bb) Eingriff durch Abgleich	101
cc) Eingriff durch Treffer	104
dd) Fazit	107

b)	Erhebliches Eingriffsgewicht	107
aa)	Heimlichkeit	109
bb)	Streubreite und Anlasslosigkeit	110
cc)	Einschüchterungseffekte	115
dd)	Anknüpfen an höchstpersönliche Merkmale	117
ee)	Möglichkeit der Verknüpfung von Informationen	118
ff)	Drohende Nachteile	119
gg)	Eigener Ansatz zur Fortschreibung der Maßstäbe: Spezifische Fehleranfälligkeit der Maßnahme	121
hh)	Eingriffsgewicht mindernde Umstände	124
c)	Fazit	127
3.	Rechtfertigung	129
a)	Verhältnismäßigkeit	130
aa)	Verfolgbare Straftaten	131
bb)	Geeignetheit	131
cc)	Erforderlichkeit	131
b)	Bestimmtheit und Normenklarheit	132
c)	Verfahren und Organisation	135
aa)	Richtervorbehalt	136
bb)	Benachrichtigungspflicht	136
cc)	Kontrolle	138
dd)	Berichts- und Evaluationspflichten	140
4.	Fazit	142
II.	Sonstige Grundrechte	142
1.	Versammlungsfreiheit	142
a)	Erhöhtes Eingriffsgewicht der Aufzeichnung der Versammlung	144
b)	Berücksichtigung der Versammlungsfreiheit bei späterer Gesichtserkennung	146
2.	Diskriminierungsverbot	149
3.	Menschenwürde	153
III.	Fazit zu den verfassungsrechtlichen Anforderungen an eine Rechtsgrundlage	157
B.	Europäisches Recht	158
I.	Unionsrecht	158
1.	KI-Verordnung	158
a)	Nachträgliche Gesichtserkennung als Hochrisiko-KI	159
aa)	Gesichtserkennung als Fernidentifizierung	160

bb) Einsatz zur Identifizierung unbekannter Verdächtiger	163
b) Vorgaben für Hochrisiko-KI-Systeme	165
aa) Konformitätsbewertungsverfahren	166
bb) Risikomanagementsystem	168
cc) Datenqualität	168
dd) Technische Dokumentation	170
ee) Aufzeichnungspflichten	170
ff) Transparenz und Bereitstellung von Informationen für die Betreiber	171
gg) Menschliche Aufsicht	172
hh) Genauigkeit, Robustheit und Cybersicherheit	175
ii) Registrierung	176
jj) Marktüberwachung	177
kk) Pflichten der Betreiber	178
c) Keine Benachrichtigungspflicht und kaum subjektive Rechte	180
d) Spezifische Vorgaben für die Identitätsermittlung per nachträglicher biometrischer Fernidentifizierung?	181
aa) Kein Genehmigungsvorbehalt	181
bb) Keine echten materiellen Vorgaben	182
cc) Keine Entscheidung mit nachteiliger Rechtsfolge ausschließlich auf Grundlage eines Treffers	184
e) Fazit	189
2. JI-Richtlinie	190
a) Art. 8 Abs. 2 JI-RL	192
b) Art. 10 JI-RL	193
c) Art. 11 JI-RL	196
aa) Verhältnis zu Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO	196
bb) Weitergehende Vorgaben	198
d) Fazit	202
3. Grundrechte-Charta	202
II. EMRK	204
1. Glukhin v. Russland	205
2. Schlussfolgerungen	210
III. Fazit	211

Inhaltsverzeichnis

C. Strafprozessrecht: Bestehen einer Rechtsgrundlage	212
I. § 98c StPO	213
1. Materielle und formelle Voraussetzungen	215
a) Materielle Voraussetzung: Anfangsverdacht für (irgend-)eine Straftat	216
b) Keine Verfahrensregeln oder Kontrollmechanismen	217
c) Fazit	218
2. Bestimmtheit und Normenklarheit	219
a) Weit formulierter Zweck („zur Aufklärung einer Straftat“)	220
b) Keine nähere Bezeichnung des technischen Eingriffsinstruments	222
c) Keine ausreichende Begrenzung der Datenbanken	225
d) Keine ausdrückliche Nennung biometrischer Merkmale	227
e) Fazit	228
II. Sonstige Rechtsgrundlagen	230
1. § 98a, b StPO	230
2. § 81b Abs. 1 Alt. 1 StPO	231
3. § 100h Abs. 1 S. 1 Nr. 1 StPO	232
4. § 163b Abs. 1 S. 1 StPO	232
5. §§ 161, 163 StPO	232
6. § 48 BDSG	233
III. Fazit: Keine Rechtsgrundlage	234
 Kapitel III. Folgen und mediale Darstellung des Einsatzes automatisierter Gesichtserkennung – kriminologische Betrachtung	237
A. Folgen für den strafrechtlichen Selektionsprozess	238
I. Bekanntwerden von strafbarem Verhalten	239
1. Verstärkte Anzeigebereitschaft durch Aufzeichnung von Taten und Verdächtigen	239
2. Polizeiliche Videoaufzeichnungen	243
II. Weitere Ermittlungen	245
1. Auffindbarkeit in Datenbanken	246
2. Anreiz zur Erfassung in Datenbanken	247
III. Fazit	248

B. Folgen für Unbeteiligte	249
I. Festnahme Unbeteiligter in den USA nach falschem Gesichtserkennungstreffer	250
1. Bekannt gewordene Fälle	250
a) Michael Oliver	250
b) Nijeer Parks	251
c) Robert Williams	252
d) Alonzo Sawyer	253
e) Randal Reid	254
f) Porcha Woodruff	254
2. Einordnung: Waren diese Festnahmen falsch (wrongful) oder rechtswidrig?	255
3. Gründe für mögliche weitere (unbekannte) Fälle	256
a) Verwendung von Gesichtserkennung wird nicht offengelegt	257
b) Keine Aufdeckung des Fehlers wegen Annahme eines Plea bargain	258
c) Keine offensichtlichen Unterschiede zwischen Täter und Verdächtigtem	260
d) Keine öffentliche Bekanntmachung des Falls	261
e) Fazit	261
II. Ursachen der Festnahmen	262
1. Fehler der Technologie	263
2. Fehler von Menschen	264
a) Menschliche Fähigkeiten zur Überprüfung von Gesichtserkennungstreffern	264
b) Überprüfung des Treffers am Computer	266
c) Überprüfung des Treffers vor Ort	267
d) Verwendung problematischen Inputs („Garbage in, Garbage out“)	267
e) Problematische weitere Polizeiarbeit	269
f) Wahllichtbildvorlagen	271
g) Fazit zu Fehlern von Menschen	272
3. Fehler in der Mensch-Maschine-Interaktion: Automation bias	273
III. Fazit	275
C. Mediale Darstellung des Einsatzes von Gesichtserkennung	277
I. Ausgangspunkt und Forschungsfragen	277

II. Methodik: Qualitative Inhaltsanalyse von Medienbeiträgen	279
1. Wahl der Methodik	280
2. Auswahl der Beiträge	281
3. Vorgehen bei der Analyse	282
III. Ergebnisse	283
1. Unterscheidung von Einsatzszenarien	283
2. Darstellung des Einsatzes in Deutschland	285
a) Differenzierung zwischen Einsatzszenarien	285
b) Einsatz zur Identifizierung unbekannter Verdächtiger	287
aa) Seltene Erwähnung	287
bb) Zum Abgleich herangezogene Datenbanken	288
cc) Bedenken mit Blick auf informationelle Selbstbestimmung	289
dd) Überprüfung der Treffer durch Menschen	290
3. Darstellung der Fehleranfälligkeit der Technologie	291
a) Hohe Fehlerquoten	291
b) Verweis auf öffentlichkeitswirksamen „Test“ durch die ACLU	292
c) Gesichtserkennung als rassistische Technologie	293
4. Berichte über Festnahmen Unschuldiger in den USA	294
IV. Diskussion und Schlussfolgerungen	296
1. Unklarheit über Einsatz in Deutschland	296
2. Bedenken	297
3. Sekundärer Automation bias in den Medien	298
D. Fazit zu Kapitel III. Folgen und mediale Darstellung des Einsatzes automatisierter Gesichtserkennung – kriminologische Betrachtung	299
 Kapitel IV. Empfehlungen für eine Regulierung	301
A. Technische Anforderungen an die verwendeten Gesichtserkennungssysteme	301
I. Genauigkeit und Freiheit von demografischen Verzerrungen	301
II. Einrichtung einer zentralen Zertifizierungsstelle	302
B. Rechtsgrundlage	304
I. Vorgaben des Grundsatzes der Bestimmtheit und Normenklarheit	304
1. Formulierung des Zwecks	304

2. Begrenzung der Datenbanken	304
3. Benennung des technischen Eingriffsinstruments	305
4. Ausdrückliche Nennung der Art biometrischer Merkmale (Gesichtsmerkmale)	306
II. Verfahrensregelungen	306
1. Benachrichtigungs-, Kennzeichnungs- und Löschpflichten	306
2. Richtervorbehalt	307
3. Subsidiaritätsklausel	308
4. Verfahren der Identifizierung	309
III. Besonderer Schutz der Versammlungsfreiheit	311
IV. Umsetzung in einer Rechtsgrundlage	312
1. Regelungstechnik	312
a) Orientierung an der Regelungstechnik der KI- Verordnung nicht empfehlenswert	312
b) Keine Ergänzung von § 98c StPO, sondern eigene Regelung	313
2. Vorschlag für eine Formulierung	314
C. Weitere Empfehlungen	315
I. Schulungen und Überarbeitung der RiStBV	315
II. Kontrolle und Evaluation	316
III. Bericht für die Öffentlichkeit	317
IV. Beobachtung technologischer und gesellschaftlicher Entwicklungen	317
D. Schlusswort	319
Kapitel V. Thesen	321
Literaturverzeichnis	325

Abbildungsverzeichnis

Abbildung 1: Verifizierung vs. Identifizierung	40
Abbildung 2: True positives, False positives, True negatives, False negatives	52
Abbildung 3: Fiktives Beispiel einer Recherche im GES	71
Abbildung 4: Eingriffsgewicht bestimmende Faktoren beim Abgleich mit Gesichtserkennung	129

