Kapitel V. Thesen

1. Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung geht mit einem besonderen Gefährdungspotenzial einher, denn er betrifft viele Unbeteiligte (Streubreite), birgt ein spezifisches Fehlerrisiko (Fehleranfälligkeit), erfolgt ohne Wissen der Betroffenen (Heimlichkeit) und ermöglicht die einfache und schnelle Vernetzung verschiedener Informationen (Vernetzungsmöglichkeit), die einer Person persönlich und eindeutig zugeordnet werden können (Biometrie).[1117]
2. Die Verwendung automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger birgt eine spezifische Fehleranfälligkeit.[1118] Zwar besteht in Ermittlungsverfahren immer die Gefahr, dass Unschuldige betroffen sind, da sich die Maßnahmen gegen Verdächtige (und nicht gegen Verurteilte) richten. Gesichtserkennung erhöht jedoch die Wahrscheinlichkeit, dass gänzlich Unbeteiligte beschuldigt werden und dass der Fehler wegen großer optischer Ähnlichkeit von Täter und Beschuldigtem im Laufe des Ermittlungsverfahrens nicht frühzeitig erkannt wird.
3. Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger begründet Eingriffe in das Recht auf informationelle Selbstbestimmung. Eigenständige Eingriffe sind die Erstellung der Embeddings, der Abgleich des Suchbilds mit allen Lichtbildern einer Datenbank sowie das Auftauchen in der Kandidatenliste.[1119]
4. Dem Abgleich und dem Auftauchen in der Kandidatenliste kommt ein erhebliches Eingriffsgewicht zu.[1120] Grund dafür sind vor allem die Heimlichkeit, Streubreite und Anlasslosigkeit, Anknüpfung an höchstpersönliche körperliche Merkmale und die drohenden Folgeeingriffe. Nachrangig können auch Einschüchterungseffekte und die grundsätzliche leichte Verknüpfbarkeit von Informationen durch Gesichtserkennung herangezogen werden. Auch die spezifische Fehleranfälligkeit von Gesichtserkennung wirkt eingriffserhöhend.

1117 Kapitel I. D. I.
1118 Kapitel I. D. I. 2.
1119 Kapitel II. A. I. 2. a) aa), bb) und cc).
1120 Kapitel II. A. I. 2. b).

5. Die Maßstäbe für die Bewertung der Eingriffsintensität von verdeckten Maßnahmen sollten weiterentwickelt und um die Kategorie der spezifischen Fehleranfälligkeit einer Maßnahme erweitert werden.[1121] Diese sollte als eigenes Kriterium eingriffserhöhend berücksichtigt werden.
6. Die nachträgliche Auswertung von Aufzeichnungen einer Versammlung per Gesichtserkennung, um unbekannte Verdächtige zu identifizieren, ist geeignet, Bürgerinnen und Bürger von künftigen Versammlungen abzuhalten. Dies muss wegen des objektiv-rechtlichen Gehalts der Versammlungsfreiheit auch bei der Ausgestaltung oder Auslegung einer strafprozessualen Rechtsgrundlage für Gesichtserkennung berücksichtigt werden.[1122]
7. Es existiert derzeit keine strafprozessuale Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger.[1123]
8. Die in Praxis und Literatur herangezogene Vorschrift des § 98c StPO ist keine taugliche Ermächtigung.[1124] Sie ist materiell weitgehend und formell vollständig voraussetzungslos und wird auch mit Blick auf die Bestimmtheit und Normenklarheit nicht den Anforderungen gerecht, die eine Ermächtigung für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erfüllen muss. Der Zweck des maschinellen Datenabgleichs („zur Aufklärung einer Straftat") ist angesichts der Eingriffsintensität automatisierter Gesichtserkennung zu unbestimmt formuliert, die Art der Datenabfrage bzw. das technische Eingriffsinstrument (Gesichtserkennung) sind nicht ausreichend spezifiziert, die zum Abgleich zugelassenen Datenbanken sind nicht hinreichend begrenzt und die Verwendung höchstpersönlicher biometrischer Merkmale geht aus der Norm nicht hervor.
9. Automatisierte Gesichtserkennung birgt nicht nur das (nicht unkritisch zu sehende) Potenzial, dass in Zukunft mehr und mehr Delikte verfolgt und aufgeklärt werden können. Sie droht auch auf die ohnehin bestehende Selektivität der Strafverfolgung verstärkt einzuwirken.[1125] Die Technologie bewirkt eine Verschiebung der Strafverfolgungsressourcen hin zu Straftaten, die (insbesondere in der Öffentlichkeit) visuell wahrnehmbar und erfassbar sind. Zudem droht eine intensi-

1121 Kapitel II. A. I. 2. b) gg).
1122 Kapitel II. A. II. 1. b).
1123 Kapitel II. C.
1124 Kapitel II. C. I.
1125 Kapitel III. A.

vere Verfolgung von Bagatellkriminalität als bisher, insbesondere bei Wiederholungstätern. Eine solche Entwicklung sollte nicht unbemerkt voranschreiten, sondern kriminologisch untersucht und kritisch hinterfragt werden.

10. Beschränkungen der durchsuchbaren Datenbanken sind ambivalent zu sehen.[1126] Einerseits verringert eine Begrenzung die Streubreite der Gesichtserkennungsmaßnahme und die Anzahl der Personen, die potenziell als der unbekannte Verdächtige fehlidentifiziert werden könnten. Andererseits bewirkt die Beschränkung eine immer stärkere Verschiebung der Verfolgung hin zu Personen, die bereits in der Vergangenheit mit der Polizei interagiert haben oder die aus anderen Gründen in den durchsuchbaren Datenbanken gespeichert sind (z. B. Asylsuchende).
11. Der Einsatz automatisierter Gesichtserkennung kann Folgen – insbesondere Ermittlungsmaßnahmen – für gänzlich Unbeteiligte mit sich bringen. Die Ursache hierfür liegt in Fehlern der Technologie, aber auch in menschlichen Fehlern, die durch die Mensch-Maschine-Interaktion noch verstärkt werden.[1127] Die menschlichen Fähigkeiten zur Gesichtserkennung sind stärker begrenzt als häufig angenommen. Der Automation bias, also die menschliche Tendenz, sich zu sehr auf automatisierte Hilfsmittel zu verlassen, erhöht das Risiko, dass Fehler nicht erkannt werden. Dies muss bei einer Regulierung von Gesichtserkennung berücksichtigt werden, um Ermittlungen gegen Unbeteiligte so weit wie möglich zu verhindern.
12. Gesichtserkennung birgt die Gefahr, dass Fehlidentifizierungen im Rahmen von Wahllichtbildvorlagen und Gegenüberstellungen zunehmen.[1128] Die Technologie ist besonders gut darin, sehr ähnlich aussehende Personen zu finden. Wenn durch Gesichtserkennung eine dem Täter optisch stark ähnelnde Person identifiziert und verdächtigt wird, ist es für den Zeugen besonders schwierig zu erkennen, dass es sich nicht um den Täter handelt.
13. Die Fehler, die im Zusammenhang mit Gesichtserkennung zu den Festnahmen Unschuldiger in den USA geführt haben,[1129] können nicht nur auf Fehler der Technologie und schlechte Polizeiarbeit zurückgeführt werden. Menschliche Fehler waren entscheidend mitverantwort-

1126 Kapitel III. A. II. 1.
1127 Kapitel III. B. II.
1128 Kapitel III. B. II. 2. f) und 3.
1129 Kapitel III. B. I. 1.

lich,[1130] insbesondere wurden offensichtliche optische Unterschiede zwischen Täter und Verdächtigtem ignoriert.

14. In der medialen Debatte wird Gesichtserkennung als eine fehleranfällige und „rassistische" Technologie dargestellt.[1131] Fehler beim Einsatz automatisierter Gesichtserkennung werden vorrangig der Technologie, nicht den Menschen zugeschrieben. Die menschliche Verantwortung und ein möglicher Automation bias werden regelmäßig übersehen.
15. Das Phänomen, dass der Automation bias von Menschen in einem zweiten Schritt von den Medien übersehen wird, lässt sich unter dem Begriff *sekundärer* Automation bias zusammenfassen.[1132] Einer solchen verzerrten Wahrnehmung sollte der Gesetzgeber nicht unterliegen und daher Regelungen treffen, um auch menschliche Fehler bei der Interaktion mit Gesichtserkennungssystemen so weit wie möglich zu verhindern.

1130 Kapitel III. B. II. 2. und 3.
1131 Kapitel III. B. III. 3.
1132 Kapitel III. B. IV. 3.