universität wien

Exposé zum Dissertationsvorhaben

Titel der Dissertation:

„Die Risikobeurteilung nach der DSGVO und die datenschutzrechtlichen Implikationen beim Einsatz von Gesichtserkennungstechnologien“

verfasst von

Mag. iur. FLEISCH Jessica

Angestrebter akademischer Grad

Doktor der Rechtswissenschaften („Doctor iuris“)

Wien, Juli 2020

Studienkennzahl: UA 783 101
Dissertationsgebiet: Rechtsinformatik
Dissertantin: Mag. Fleisch Jessica
Matrikelnummer: 01215000
Betreuer: ao. Univ.-Prof. Mag. DDr Erich Schweighofer

Einleitung und Problemstellung:

Der Einsatzbereich von Künstlicher Intelligenz („*Artificial Intelligence*“) umfasst mittlerweile ein breites Spektrum an Anwendungsmöglichkeiten und wird sowohl vom privaten als auch vom öffentlichen Sektor genutzt. Auch auf dem Gebiet der biometrischen Erkennungsverfahren anhand von Gesichtsaufnahmen sind große Fortschritte zu verzeichnen. Der Marktwert lag 2019 noch bei knapp 3,2 Milliarden USD und soll bis 2024 auf geschätzte sieben Milliarden USD anwachsen.[1]

Im Öffentlichen Bereich werden Gesichtserkennungstechnologien vor allem für die strafrechtliche Verfolgung und Identifizierung von Straftätern eingesetzt, aber auch in anderen Öffentlichen Bereichen eröffnet sich ein vielfältiges und breit gefächertes Einsatzfeld. Vor allem auch auf Grund der aktuell grassierenden Covid-19-Pandemie ergeben sich neue kontroverse Einsatzzwecke.[2] Aber auch abseits der derzeitigen Pandemiebekämpfung sind Gesichtserkennungstechnologien ein umstrittenes Instrument der staatlichen Massenüberwachung. China setzt automatisierte Gesichtserkennung u.a. für die Irisüberwachung und somit zur Messung der Aufmerksamkeit ihrer Schüler ein und auch die Minderheit der Uiguren wird anhand von den individuell ausgeprägten Merkmalen des Gesichts getrackt, um deren Aufenthaltsort zu bestimmen und diese zu überwachen.[3] In Europa kommen biometrische Erkennungsverfahren anhand von Gesichtsaufnahmen auch vermehrt zum Einsatz. Beispielsweise möchte Frankreich als erstes Land innerhalb der EU eine digitale Identität einführen und das Österreichische BMI hat eine Software mit 10 Millionen Gesichtsbildern erworben, die am Flughafen Straftäter mittels eines Datenbankabgleich identifizieren soll.[4]

---

[1] *Markets and Markets*, Facial Recognition Market: https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html (15.06.2020); Zu den Gründen ausführlich: *Molavi* Ramak, Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung, JRP 2018/7, 7 ff.

[2] In Russland wird beispielsweise anhand von biometrischen Gesichtserkennungsanlagen überprüft, ob die verhängte Quarantäne vorschriftsgemäß eingehalten, sowie soziale Kontakte rasterartig im Infektionsfall rekonstruiert, um die Ausbreitung des Virus einzudämmen bzw. zu entschleunigen: dazu *Schmidt* Friedrich (FAZ), Moskau ergreift drastische Maßnahmen wegen Coronavirus: https://www.faz.net/aktuell/politik/ausland/moskau-ergreift-drastische-massnahmen-wegen-coronavirus-16667368.html (15.06.2020).

[3] *Standard*, China: Schule zwingt Schüler mit Gesichtserkennung zum Aufpassen: https://www.faz.net/aktuell/politik/ausland/moskau-ergreift-drastische-massnahmen-wegen-coronavirus-16667368.html (15.06.2020); *NYT*, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (15.06.2020); *Lu* Xiaoguang/*Chen* Hong/Jain Anil K., Multimodal Facial Gender and Ethnicity Identification, in *Zhang* D./*Jain* A.K. (Hrsg), Advances in Biometrics (Springer Berlin/Heidelberg 2005).

[4] Norwegen hat bereits eine; *Bloomberg*, France Set to Roll Out Nationwide Facial Recognition ID Program: https://www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan (15.06.2020); *Der Standard*, Innenministerium setzt seit Monaten Gesichtserkennungssoftware ein: https://www.derstandard.at/story/2000116445514/innenministerium-setzt-gesichtserkennungssoftware (15.06.2020); *Parlamentarische Anfrage*, Gesichtsbilderdatenbanken der österreichischen Sicherheitsbehörden: https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_00750/index.shtml (15.06.2020); *Parlamentarische*

Im privaten Sektor wird Gesichtserkennung u.a. als kontaktloses Zahlungssystem, aber auch für die Überprüfung von Zugangs- und Zutrittsberechtigungen eingesetzt. Die Anwendungsmöglichkeiten sind vielfältig und teils im Hinblick zum Verarbeitungszweck mE nicht verhältnismäßig und widersprechen dem allgemeinen Paradigma der DSGVO.[5]

Vor diesem Hintergrund mag es nicht verwunderlich erscheinen, dass innerhalb der Grenzen der EU über ein Verbot solcher Technologien nachgedacht wird. Der geleakte Whitepaper-Entwurf zur Regulierung Künstlicher Intelligenz der EU-Kommission sprach sich für ein vorübergehendes Gesichtserkennungstechnologienverbot im Öffentlichen Raum aus, bis Risiken durch deren Einsatz absehbar und Schutzvorkehrungen konzipiert und formuliert sind, die ein ausreichendes Datenschutzniveau für die Rechte der Betroffenen garantieren und die Zulässigkeit der Verarbeitung von Gesichtsaufnahmen an ein ausreichendes Pflichtniveau koppelt.[6] Im offiziellen Dokument wurde von diesem Passus allerdings abgesehen.

Bei Gesichtserkennungstechnologien handelt es sich generell um Risikotechnologien, deren Wesensgehalt sich dadurch kennzeichnet, dass die Wahrscheinlichkeit des materiellen oder immateriellen Schadenseintritts nur schwer feststellbar bzw. belegbar ist.[7] Der Regulierungsfokus sollte sich deshalb nicht nur am Anknüpfungspunkt des personenbezogenen Datums, sondern an dem am wahrscheinlichsten eintretenden Risiko orientieren.[8] Der Risikogehalt der Verarbeitungstätigkeit sollte somit bei der Zulässigkeitsprüfung von biometrischen Gesichtserkennungsverfahren in den Vordergrund rücken und deren rechtmäßiger Einsatz vom zu erwartendem Risiko abhängig gemacht werden. In der jetzigen datenschutzrechtlichen Ausgestaltung ist das Verarbeitungsrisiko für die Rechte der betroffenen Personen nicht an die Zulässigkeit des Einsatzes von Gesichtserkennungstechnologien gekoppelt, was dem besonderen

---

Anfrage, BMI-LR2220/0327-II/BK/6.3/2019: https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03406/imfname_757757.pdf (1.07.2020).

[5] Weitere Beispiele: Der Standard, Bezahlen per Gesichtserkennung: Kommt der Trend zu uns?: https://www.derstandard.at/story/2000103477818/gesichtserkennung-facial-recognition-payments-applepay-alipay (15.06.2020); *FAZ*, Taylor Swift hat ihr Publikum gescannt: https://www.faz.net/aktuell/feuilleton/pop/gesichtserkennung-taylor-swift-setzt-auf-biometrische-ueberwachung-15946630.html (15.06.2020); *Schmidt* Joana, Neue Technologie: Blutdruck messen durch Gesichtserkennung: https://link.springer.com/article/10.1007/s11298-019-7393-2#:~:text=Eine%20neue%20Studie%20zeigt%2C%20dass,kurzen%20Videos%20ihres%20Gesichtes%20messen (1.07.2020); *Der Standard*, Chinesischer Finanzkonzern scannt Gesichter seiner Kunden: https://www.derstandard.at/story/2000106469870/chinesischer-finanzkonzern-scannt-gesichter-seiner-kunden (01.07.2020); Auch interessant: *Kasper* Lioba/*Tretter* Hannes, Zutrittskontrolle mittels Handvenenerkennung bei Badegästen, ZiiR 2019/4, 394-401.

[6] *Redaktion MMR-Aktuell*, EU-Kommission: Verbot automatisierter Gesichtserkennung im öffentlichen Raum geplant, MMR-Aktuell 2020, 425975; *Martini*, Blackbox, 161.

[7] *Bieker* Felix/*Brennert* Benjamin/*Hansen* Marit, Die Risikobeurteilung nach der DSGVO, DuD 2018/8, 492 (493); ErwG 76 DSGVO; Zur Regulierung von Risikotechnologien; *Martini*, Blackbox, 115.

[8] Vgl. *Martini*, Blackbox 161; Zum Risikobegriff in der DSGVO: *Datenschutzkonferenz (DSK)*, Risiko für die Rechte und Freiheiten natürlicher Personen (Kurzpapier Nr. 18): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (01.07.2020).

Schutzbedürfnis des geometrischen Gesichtsmerkmals – wie in dieser Arbeit später noch aufgezeigt werden soll – nicht gerecht wird.[9] In der DSGVO ist stellenweise zwar ein risikobasierter Ansatz zu erkennen, die Effektivität dieser Schutzvorkehrungen weist jedoch für den Einsatz von Künstlicher Intelligenz für die Rechte der Betroffenen nachhaltige Lücken auf, die im Rahmen dieses Dissertationsvorhabens detailliert aufgezeigt und anschließend der Versuch angestellt wird Lösungsansätze zu eruieren, die diese zu schließen versuchen.

Es stellt sich deshalb im ersten Schritt die Frage, welche Risiken vom Einsatz von biometrischen Erkennungsverfahren mittels Gesichtsaufnahmen zu erwarten sind. Grundsätzlich kann man zwischen allgemeinen und speziellen Risiken unterscheiden. Allgemeine Risiken betreffen den Einsatz jeder biometrischen Anlage *per se*. Spezielle Risiken betreffen die spezifischen Bedrohungen für die Betroffenen, wie z.B. die Gefahr der lebenslangen Merkmalskompromittierung und Identitätsdiebstahl, aber auch Deep-Fake-Technologien sind in diesem Zusammenhang interessant und müssen berücksichtigt werden.[10] Das zentrale Problem, das sich bei der Verarbeitung von biometrischen Merkmalen ergibt, ist, dass wenn die Merkmale einmal missbraucht oder gefälscht worden sind, sie nicht wie künstlich geschaffene Authentifizierungskomponenten auf der Basis von Wissen oder Besitz ohne Weiteres ausgetauscht werden können. Die Tatsache, dass die zur Verfügung stehenden biometrischen Merkmale einer Person naturgemäß begrenzt sind, kommt erschwerend hinzu und verstärkt deren besondere Schutzbedürftigkeit.[11]

Im zweiten Schritt muss geklärt werden, wie eine Risikoreduktion erreicht werden kann. Um den Gefahren und den Risiken von Gesichtserkennungstechnologien zu begegnen, stehen dem Gesetzgeber mehrere Möglichkeiten zur Verfügung. Es können präventiv, begleitend und nachträglich Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen ergriffen werden. Auch das Instrument der begleitenden Selbstregulierung, wie z.B. eine Etablierung eines Zertifizierungsverfahrens oder auch die Einführung eines Datenschutzsiegel ist eine Regulierungsmethode, von der der Gesetzgeber Gebrauch machen kann.[12]

Um entscheiden zu können wie effektiv die aktuellen Schutzvorkehrungen sind, muss erarbeitet werden, was überhaupt im Zusammenhang mit dem geometrischen Gesichtsmerkmal beschützt

[9] Vgl dazu auch: *Roßnagel* Alexander, Gesetzgebung im Rahmen der Datenschutz-Grundverodrnung: Aufgaben und Spielräume des deutschen Gesetzgebers?, DuD 2017/5, 277 ff; vgl *Schwichtenberg*, Datenschutz, 149.
[10] Aufzählung nicht taxativ; vgl. *Feiler* Lukas, Selig, die sehen und doch nicht glauben, Die Presse 2018/44/02.
[11] *Dotzler* Florian, Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen, 21 f; nicht nur ein personenbezogenes Datum, sondern auch personengebunden.
[12] *Martini*, Blackbox 141 und 168.

werden soll und welche Risiken mit dem Einsatz einher gehen.[13] Deshalb wird im ersten Teil meiner Arbeit das Schutzbedürfnis des geometrischen Gesichtsmerkmals analysiert, dessen Besonderheiten herausgearbeitet und auch eine vergleichende Gegenüberstellung mit anderen biometrischen Merkmalen angestellt, um deren datenschutzrechtlichen Unterschiede systematisch zu veranschaulichen.

Das geometrische Gesichtsmerkmal weist nämlich einige Besonderheiten auf. Es besitzt eine leichte Aufspürbarkeit und anders als beispielsweise bei einer DNA-Probe eröffnet sich die Möglichkeit einer kontaktlosen Identifizierung. Beim menschlichen Gesicht handelt es sich folglich um ein offenes biometrisches Merkmal, das sich dadurch besonders für eine ungefragte und unbewusste Authentifizierung eignet, da es sehr einfach ohne das Wissen und Mitwirken des Merkmalsträgers zu erfassen ist.[14] Auch hat man oftmals keine Möglichkeit die Verarbeitung zu verhindern insbesondere beim Einsatz zur Überwachung des Öffentlichen Raums oder wie die Vorgangsweise der Datensatzbeschaffung von *Clearview AI* aufzeigt auch in der virtuellen Sphäre des Internets.[15] Das US-Start-up Unternehmen hat mittels öffentlich zugänglicher Gesichtsaufnahmen und in Kombination mit weiteren frei verfügbaren Informationen von den Betroffenen aus den sozialen Netzwerken eine umfassende Referenzdatenbank erstellt und eine dazugehörige Software entwickelt, die unter die Klassifikation einer Personensuchmaschine zu subsumieren ist und es den Nutzern ermöglicht anhand einer Gesichtsaufnahme Personen zu identifizieren.[16]

Weitere rechtliche Probleme ergeben sich aus dem Umfang des Informationsgehaltes des menschlichen Gesichts, da unweigerlich weitere Zusatzinformationen offengelegt werden. Aus den Informationen des geometrischen Gesichtsmerkmals kann nicht nur ein Rückschluss auf die Identität gezogen werden, sondern u.a. auch auf die Rasse, Religionszugehörigkeit, Alter und Gesundheitszustand.[17] Der Verarbeitungsinhalt geht also meistens über den Verarbeitungszweck hinaus, was dem Wesen der allgemeinen Verarbeitungsgrundsätze des Art 5 DSGVO widerspricht. Zudem lässt sich durch die Kombination mit anderen Informationen leicht ein

[13] Siehe auch ErwG 75 DSGVO.
[14] *Dotzler,* Aspekte 108.
[15] Keine Möglichkeit zur Einwilligung.
[16] *NYT*, The Secretive Company That Might End Privacy as We Know It: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (15.06.2020); ZD-Aktuell 2020: Interpol entwickelt Gesichtserkennung, beck-online 07033; *AI News*, Clearview AI lawyer: 'Common law has never recognised a right to privacy for your face': https://artificialintelligence-news.com/2020/03/06/clearview-ai-lawyer-common-law-has-never-recognised-a-right-to-privacy-for-your-face/ (05.07.2020).
[17] *Dotzler*, Aspekte 152 f.

umfassendes persönliches Nutzerprofil oder auch Bewegungsprofil erstellen, das die Überwachung der einzelnen Individuen ermöglicht.

Die zeitliche Variabilität des Gesichts ist aus datenschutzrechtlicher Sicht als Vorteil zu werten, da eine starke Permanenz des Merkmals den Personenbezug zwischen Merkmalsträger und biometrischen Merkmal unweigerlich verstärkt.[18] Angesichts der Tatsache, dass das menschliche Gesicht eine dynamische Struktur aufweist, ergeben sich auch jugendschutzrechtliche Fragestellungen, da das geometrische Gesichtsmerkmals bereits im Alter zwischen zwölf und vierzehn als stabil einzuordnen ist.[19]

Als weitere Charakteristika des menschlichen Gesichts ist die willentliche Beeinflussbarkeit anzuführen, die es dem Merkmalsträger ermöglicht z.B. durch das Tragen einer Brille oder eines Bartes sein Gesicht zu verändern. Auch die plastische Chirurgie leistet dazu einen nicht unbeachtlichen Beitrag, da durch kosmetische Eingriffe das Gesichtsbild eines Menschen nachhaltig verändert werden kann. So wurde beispielsweise schon 2005 in Frankreich eine komplette Gesichtstransplantation durchgeführt.[20] Je nach Erkennungsleistung der biometrischen Anlage unterscheiden sich nun die Möglichkeiten der Manipulationen durch die Beeinflussung des Merkmalsträgers. Beispielsweise ist aufgrund des zunehmenden Aufkommens des Covid-19-Virus das verpflichtende Tragen eines Mund-Nasen-Schutzes gängiger *usus* geworden, weshalb bereits bei einigen biometrischen Systemen festgestellt worden ist, dass dies eine Verringerung der Erkennungsleistung zur Folge hat, was eine willentliche Beeinflussung des biometrischen Merkmals darstellt.[21] Das bedeutet allerdings nicht, dass eine Identifizierung nicht möglich ist, da durch die leichte Kombinierbarkeit mit anderen Informationen des Betroffenen u.U. sich immer noch eine Rekonstruktion der Identität bewerkstelligen lässt.

Mit biometrischen Systemen können grundsätzlich zwei verschiedene Erkennungsziele verfolgt werden. Die Verifizierung und die Identifizierung. Beide Betriebsarten („*modi*“) unterscheiden sich grundsätzlich in ihrer Ausgestaltung und ihrem Ablauf, weshalb sich auch die Risiken erheblich voneinander abgrenzen. Verifikationssysteme werden vor allem für die Kontrolle der Zugriffs- bzw. Zutrittsberechtigung der betroffenen Person benützt. Die biometrische Anlage prüft hier: „Ist das die Person?“, wohingegen ein biometrisches Erkennungsverfahren zur

[18] *Dotzler*, Aspekte 157.
[19] *Fritz* Carmen, Internationaler Datenschutz und Rechtsschutz beim Austausch biometrischer Daten – eine Würdigung des ePasses und des Prümer Ratsbeschlusses, 25; vgl. *Seiss* Constanze und *Raabe-Stuppnig* Katharina, Kinder und ihre Persönlichkeitsrechte, ZIR 2014/2, 100 – 105; siehe auch ErwG 38 DSGVO.
[20] *Fritz*, Datenschutz 28.
[21] *Der Standard*, Maskiert und trotzdem erkannt: Gesichtserkennung schreitet voran: https://www.derstandard.at/story/2000117655752/maskiert-und-trotzdem-erkannt-gesichtserkennung-schreitet-voran (21.06.2020).

Personenidentifikation ausfindig macht „Wer ist diese Person?“, was datenschutzrechtlich mehrere Probleme aufwirft.[22] Die Anlage einer zentralen Referenzdatenbank ist unumgänglich und auch deren Sicherung vor unberechtigten Zugriffen sollte einheitlichen Standards unterliegen. Weiteres sollten auch organisatorische Maßnahmen hinsichtlich der Einschränkung der Anzahl von Zugriffsberechtigten ergriffen werden, um die sensiblen Daten vor Dritteinwirkungen zu schützen. Je nach Betriebsmodus der biometrischen Anlage sind also auch unterschiedliche Maßnahmen notwendig, worauf momentan weder das Gesetz noch die Literatur konkrete Handlungsanweisungen für die Anbieter von Gesichtserkennungstechnologien liefern.

Einen Teil meiner Arbeit soll sich der Vollständigkeit halber auch mit der Unterscheidung zwischen konventioneller und intelligenter Überwachung beschäftigten. Bereits die herkömmliche Videoüberwachung stellt nämlich ein umstrittenes Instrument dar. Insbesondere bei automatischer Gesichtserkennung verschärfen sich jedoch die Beeinträchtigungen der verfassungsrechtlich gewährleisteten Grundrechte, die diese Arbeit zu evaluieren versucht.

Aktuelle Gesetzeslage und Judikatur:

Laut dem 51. Erwägungsgrund der DSGVO gelten Lichtbilder nur dann als biometrische Daten, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Je nachdem richtet sich die Zulässigkeit der Verarbeitung nach Art 6 oder 9 DSGVO.[23] Für die Verarbeitung der besonderen Kategorien von personenbezogenen Daten sieht Art 9 DSGVO ein grundsätzliches Verarbeitungsverbot von biometrischen Daten vor, wohingegen in Abs 2 einige Erlaubnistatbestände formuliert sind, die jedoch nicht den Schwerpunkt dieser Arbeit bilden sollen. Weiteres sind bei der Verarbeitung von biometrischen Daten – wie bei jeder anderen Verarbeitung von personenbezogenen Daten auch – die allgemeinen Verarbeitungsgrundsätze des Art 5 DSGVO zu berücksichtigen und speziell in Österreich ist die querschnittsmaterielle Regelung des §78 UrhG und in Deutschland die §§ 22 und 23 KUG, die einen Bildnisschutz normieren, zu beachten.[24] Auch die „household-exemption“ (Art 2 Abs 2 lit c DSGVO), die für die Verarbeitung von Gesichtsaufnahmen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten eine Ausnahme vom Anwendungsbereich vorsieht, ist allenfalls zu berücksichtigen.[25]

[22] *Dotzler*, Aspekte 164 ff.
[23] ErwGr 34 und 51; Art. 4 Z 13 und 14; *Matejek* Michael/*Mäusezahl* Steffen, Gewöhnliche vs. Sensible personenbezogene Daten, ZD 2019, 551 ff.
[24] *Solmecke* Christian/*Kocatepe* Sibel, Google Glass – Der Gläserne Mensch 2.0, ZD 2014, 22 ff.
[25] *Ehmann* Eugen, Personenaufnahmen nach der DS-GVO, ZD 2020, 65 ff.

Auf Grund der Gefahr, dass es beim Einsatz von Gesichtserkennungstechnologien zu nicht unerheblichen Diskriminierungen kommen kann, ist es weiters überlegenswert über eine Regulierung, die über die Ansätze der Art 9 Abs 1 und 22 Abs 4 DSGVO hinausgeht, nachzudenken.[26]

Der Gleichbehandlungsgrundsatz schützt vor Diskriminierungen, sodass der Voreingenommenheit von KI-Anwendungen durch den Datenschutz entgegengewirkt werden muss.[27] Im Anwendungsfall von Gesichtserkennungstechnologien haben mehrere Studien ergeben, dass sie vor allem Probleme dabei haben schwarze Frauen korrekt zu erkennen.[28] Dies ist auf der einen Seite auf die der KI zur Verfügung gestellten Lerndaten und den KI-Lernprozess *per se* zurückzuführen, aber andererseits auch auf den implementierten Quellcode.[29] Die automatisierte Gesichtserkennung von *Google Fotos* beispielsweise ging so weit, dass Schwarze als Gorillas kategorisiert wurden, da der dahinter agierende Algorithmus nicht ausreichend zwischen Menschen und Tier unterscheiden konnte. Auch *Flickr* hatte ähnliche Probleme mit der Gesichtserkennung und Schwarze wurden als „Animal" oder „Ape" kategorisiert.[30] Eine KI ist mithin nicht werteneutral, sie lernt anhand der Daten, die man ihr zu Verfügung stellt und entscheidet auf Grundlage der Regeln, die man implementiert. Bei der Entwicklung künstlicher Intelligenz muss deshalb gesetzlich sichergestellt werden, dass die Systeme nicht gegen das europäische Antidiskriminierungsrecht verstoßen. Vereinzelt finden sich in der DSGVO zwar schon antidiskriminierende Ansätze, jedoch mangelt es an der Gewährleistung von gruppenbezogenen Schutzmechanismen.

Es stellt sich daher die Frage, inwieweit der Antidiskriminierungsschutz in der DSGVO ausgestaltet ist, was auch eine Aufklärung des Verhältnisses zu bereits geltenden Antidiskriminierungsgesetzen impliziert. Derzeit besitzen Aufsichtsbehörden und auch (potenziell) Betroffene aufgrund der aktuellen rechtlichen Rahmenbedingungen kein Einsichtsrecht in den Quellcode, was die Nachvollziehbarkeit von Entscheidungen bzw. auch Diskriminierungen erheblich erschwert.[31] Auch eine Begründungspflicht für die Entscheidungen, die auf biometrischen

[26] *Steege* Hans, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz, MMR 2019, 715 (721).
[27] *Molavi*, JRP 2018/1, 7 (10).
[28] *NYT*, Many Facial-Recognition Systems Are Biased, Says U.S. Study: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html (22.06.2020).
[29] Vgl. *Conrad* Sebastian Conrad, Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017/12, 743.
[30] *FAZ*, Meine Freundin ist kein Gorilla: https://www.faz.net/aktuell/feuilleton/medien/gesichtserkennung-google-markiert-schwarzes-paar-als-gorillas-13681262.html (15.06.2020); *Die Presse*, Gesichtserkennung in Google Photos macht Schwarze zu Gorillas: https://www.diepresse.com/4766453/gesichtserkennung-in-google-photos-macht-schwarze-zu-gorillas (15.06.2020).
31 Vgl. Eigene Regulierungsbehörde für KI: *Molavi*, JRP 2018/1, 7 (11 f); *Tutt* Andrew, An FDA for Algorithms: https://pdfs.semanticscholar.org/492e/603fd095ed76a15e44f27e0f541a54313290.pdf (01.07.2020).

Erkennungsverfahren beruhen ist nachzudenken, um Diskriminierungen gezielt entgegensteuern zu können und sie breitflächig präventiv zu unterbinden.

Der bereits angesprochene risikobasierte Ansatz der DSGVO ergibt sich aus dem Wortlaut der Art 24, 25, 32 und 35 DSGVO. Die soeben aufgezählten Gesetzesbestimmungen machen die Verarbeitung ausdrücklich von der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken abhängig. Dabei bildet Art 35 DSGVO die zentrale rechtliche Grundlage für die Risikobewertung und -ermittlung eines Verarbeitungsvorganges in der DSGVO.

Eine Datenschutzfolgeabschätzung (DSFA) ist jedoch anders als es vermuten lässt, nicht bei jedem Verarbeitungsprozess von biometrischen Daten zu erstellen, vielmehr stellt Art 35 DSGVO auf die Eigenverantwortung der Unternehmer ab und verlangt die DSFA nur, wenn das Risiko der Verarbeitung zu hoch für die Rechte natürlicher Personen ist.[32] Es handelt sich dabei dementsprechend immer um eine Schwellenwertanalyse, die dem Verarbeitungsprozess voranzugehen hat, da jeglicher Verarbeitungsvorgang von personenbezogenen Daten – Technik immanent – irgendwelche Risiken für die Rechte der Betroffenen mit sich bringt.[33] Art 35 (3) DSGVO zählt allerdings deklarativ zu riskante Verarbeitungsvorgänge auf, bei denen eine DSFA zwingend zu erstellen ist. Die DSFA wird vom Gesetz bei der Verarbeitung von biometrischen Daten ausdrücklich verlangt, wenn einerseits große Mengen verarbeitet werden oder die Verarbeitung zur umfassenden und systematischen Bewertung von persönlichen Aspekten natürlicher Personen genutzt wird und anderseits, wenn die Verarbeitungstätigkeit systematisch erfolgt. Ergänzend dazu hat die Art 29 Datenschutzgruppe Leitlinien erlassen und ein Prüfschema mit neun Kriterien konzipiert, um zu klären, wann eine DSFA zu erstellen bzw. wann das Risiko als zu hoch zu qualifizieren ist.[34]

Unabhängig davon, wann eine DSFA zu erstellen ist, verlangt der Wortlaut des Art 35 DSGVO grundsätzlich keine Überprüfung der DSFA durch die Beiziehung von Experten bzw. unabhängigen Stellen. Das birgt insbesondere das Problem, dass den Unternehmen aufgrund fehlender Expertise gewisse Risiken nicht bewusst sind oder absichtlich Risiken verheimlicht werden, um

[32] Das Gesetz spricht hier nicht von den Betroffenen vgl. dazu: *Schwichtenberg* Simon, Datenschutz in drei Stufen. Ein Auslegungsmodell am Beispiel des vernetzten Automobils, 148.

[33] *Datenschutzkonferenz (DSK)*, Datenschutzfolgeabschätzung nach Art 35 DSGVO (Kurzpapier Nr. 5): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (01.07.2020). Berücksichtigt muss jedenfalls auch die von den mitgliedsstaatlichen Aufsichtsbehörden erstellten Blacklists werden (Art 35 (4) DSGVO); ErwG 91 DSGVO.

[34] Ausführend dazu: *Datenschutzgruppe nach Art 29*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01.

das vollständige Wertschöpfungspotential des geplanten Technologieneinsatzes ausnützen zu können.[35] Es stellt sich deshalb die Frage, ob aufgrund des Risikogelages von Gesichtserkennungstechnologien die DSFA erst nach der Einholung bzw. Beiziehung von Expertenmeinungen durchgeführt werden soll und sich nicht nur auf die Risikoeinschätzung durch die Unternehmen selbst stützen sollte, dessen eigenes Verarbeitungsinteresse primär im Vordergrund steht.[36] Weiters ist die DSFA in ihrer jetzigen Ausgestaltung kein Genehmigungsverfahren und daher nicht an die Zulässigkeit von Gesichtserkennungstechnologien gekoppelt.[37] Die Aufsichtsbehörde muss laut den Bestimmungen der DSGVO nur konsultiert werden, wenn das zu erwartenden Risiko (sog. Restrisiko) trotz getroffener Vorkehrungen zu hoch ist. Dem allenfalls bestellten Datenschutzbeauftragten kommt nach geltender Rechtslage dabei lediglich die Stellung eines Beraters zu, weshalb auch hier eine stärkere konstitutive Einbindung überlegenswert ist.[38] Auch für die inhaltlichen Vorgaben spricht sich die Art 29 Datenschutzgruppe für die Erarbeitung von branchenspezifischen DSFA-Rahmenbedingungen, die die Komponenten des Art 35 Abs 7 berücksichtigen sollten, aus. Aufgrund dessen, dass die DSFA in ihrer jetzigen Form nicht als umfassende Risikoanalyse konzipiert ist, berücksichtigt sie nur die datenschutzrechtlichen „klassischen", aber nicht andere Schutzgüter wie Eigentum, Meinungsfreiheit oder körperliche Integrität, weshalb sich dadurch weitere rechtliche Problemstellungen ergeben.[39]

Daraus ergibt sich auch die Frage, ob Dritte insbesondere Betroffene ein Recht haben sollten die DSFA einsehen zu dürfen bzw. ob eine generelle Veröffentlichungspflicht – auch vor allem für die kritische Öffentlichkeit wie z.B. Verbraucherverbände – zweckentsprechend ist.[40] Der Umfang der Veröffentlichungspflicht wird sich hierbei am legitimen Schutz der Geschäftsgeheimnisse orientieren müssen und sollte sich deshalb, wenn überhaupt auf die abschätzbaren Risiken beschränken und in gekürzter und klarer Form erfolgen.[41] Im privaten Rechtsverkehr ist allerdings grundsätzlich niemand verpflichtet Dritten offenzulegen welche Intention sich hinter einer Handlung verbirgt bzw. auf welchen Leitmaßstäben und Kriterien eine Entscheidung getroffen wird.[42] Weiteres ist bei der Erstellung einer DSFA für Verarbeitungsvorgänge, die Technik immanent einen erheblichen Grundrechtseingriff fordern, eine stärkere Einbindung

[35] *Martini*, Blackbox 209.
[36] Vgl. *Schwichtenberg*, Datenschutz, 148.
[37] *Feiler/Forgó*, DSGVO, 24; *Martini*, Blackbox 125 f.
[38] *Feiler/Forgó*, DSGVO, 24.
[39] *Martini*, Blackbox 209; Ausführlich zur Schutzgutdebatte der DSGVO: *Veil* Winfried, Die Schutzgutmisere des Datenschutzrechts: https://www.cr-online.de/blog/2019/03/18/die-schutzgutmisere-des-datenschutzrechts-teil-ii/ (01.07.2020).
[40] *Martini*, Blackbox 210 f.
[41] *Martini*, Blackbox 211.
[42] *Martini*, Blackbox 72.

der Aufsichtsbehörden wünschenswert. Überlegenswert wäre bei Gesichtserkennungstechnologien auch eine allgemeine Meldepflicht einzuführen.[43] Aus Sicht der Risikoregulierung und auch dem Schutz vor Diskriminierung wären dies erste Ansätze Gesichtserkennungstechnologien rechtlich transparenter zu gestalten.

Die DSGVO sieht als weitere präventive Regulierungsmöglichkeit den Datenschutz durch Technikgestaltung vor, jedoch findet man keine konkreten rechtlichen Vorgaben wie weit die Gesichtserkennungssoftware fortgeschritten, d.h. die prozentuale Erkennungsleistung der biometrischen Anlage ausgereift sein muss, was auch auf die in der DSGVO vorherrschenden Grundsatz der Technikneutralität zurückzuführen ist, da sie in ihrem Wesenskern als GrundVO konzipiert ist, die datenschutzrechtlichen Besonderheiten von Risikotechnologien nicht explizit berücksichtigt.[44]

Eine dieser Besonderheiten kennzeichnet sich dadurch, dass ein biometrisches Erkennungsverfahren lediglich auf Grundlage eines Ähnlichkeitsvergleichs seine Entscheidungsaussage trifft. Für die Ermittlung der Erkennungsleistung spielen deshalb die Fehlerraten eine zentrale Rolle. Die Fehlerquoten sind der Qualitätsmaßstab für die Erkennungsleistung biometrischer Entscheidungssysteme und maßgebend für die Manipulationsanfälligkeit des biometrischen Systems.[45] Anders als bei klassischen Authentifizierungsverfahren, die auf Basis von Wissen und Besitz beruhen – wie bei der PIN-Eingabe –, ist eine eindeutige Entscheidungsaussage bei einem biometrischen Identifizierungsverfahren nicht möglich, da das biometrische Entscheidungsverfahren auf einem Ähnlichkeitsvergleich von Merkmalsproben basiert und keine eindeutige Entscheidungsaussagen getroffen werden können.[46] Die Gewährleistung der Objektivität bei der Fehlerratenermittlung ist allerdings sehr schwer zu bewerkstelligen, da die Ermittlung der Fehlerquote größtenteils von der Auswahl der Testpersonen und von den Versuchsrahmenbedingungen ihrer Ermittlung abhängt. Zudem handelt es sich dabei immer nur um schätzbare Komponenten. Um deshalb zu einem realistischen Ergebnis zu gelangen, muss die Testdatenbank auf repräsentativen Datensätzen und auch quantitativ eine dementsprechende Größe aufweisen, weshalb auch hier rechtlich abgesicherte einheitliche Standards bzw. Rahmenbedingungen wünschenswert sind, um ein standardisiertes Datenschutzniveau zu erreichen.[47] Es gibt momentan nämlich keine konkreten gesetzlichen Anforderungen an die

[43] ErwG 89 DSGVO: Entfall der generellen Meldepflicht.
[44] *Martini*, Blackbox 157.
[45] Vgl. Art 5 DSGVO (Grundsatz der Richtigkeit); *Dotzler*, Aspekte, 3.
[46] *Anil* K. Jain, Biometric Recognition: How Do I Know Who You Are?, in *Zhang* D./*Jain* A.K. (Hrsg), Advances in Biometrics (Springer Berlin/Heidelberg 2005); *Dotzler*, Aspekte, 22.
[47] *Dotzler*, Aspekte, 23.

Erkennungsleistung von Gesichtserkennungstechnologien und auch keine sonstigen einheitlichen Verfahren für die Fehlerquotenermittlung, was weitere Rechtsunsicherheiten erzeugt und der Zulässigkeitsdebatte von Gesichtserkennungstechnologien negativ entgegensteht.[48]

Weiterführend muss auch geklärt werden, inwiefern nationale Regelungen im Bereich von biometrischen Erkennungsverfahren anhand von Gesichtsaufnahmen getroffen werden dürfen. Für mitgliedstaatliche Regelungen gilt grundsätzlich, dass der nationale Gesetzgeber aufgrund der Sperrwirkung nicht ohne Weiteres Bestimmungen erlassen kann.[49] Dies fußt auf dem Vorhaben das Datenschutzrecht unionsrechtweit zu harmonisieren, um ein einheitliches Datenschutzniveau zu erreichen.[50] Die DSGVO sieht für mitgliedsstaatliche Regelung allerdings Öffnungsklauseln vor, die eine Co-Regulierung des Datenschutzes durch Union und Mitgliedstaaten ermöglichen, weshalb das Datenschutzrecht, um es vollzugsfähig zu machen auf die ergänzende Regulierung der nationalen Gesetzgeber angewiesen ist.[51] Jedoch ist der Umfang dieser Co-Regulierung nicht abschließend geklärt. Um die Modernisierung des Datenschutzrecht voranzutreiben sollten die Mitgliedstaaten von ihren Regelungsspielräumen allerdings Gebrauch machen und durch risikospezifische Regulierung Grundrechte und -freiheiten stärken und der VO somit mehr Rechtssicherheit verleihen. [52]

Deshalb stellt sich die Frage, inwiefern die Öffnungsklauseln, die in der DSGVO vorgesehen sind, sich auf die Regulierungskompetenz von Gesichtserkennungstechnologien auswirken. Und inwiefern von den Mitgliedsstaaten außerhalb des Bereichs der Öffnungsklausel gesetzliche Maßnahmen gesetzt werden dürfen, um den Risiken ausgehend vom Einsatz von Risikotechnologien insbesondere Gesichtserkennungsalgorithmen entgegenzuwirken. Daraus ergibt sich auch implizit die Fragestellung, da die DSGVO als technikneutrale GrundVo konzipiert ist, ob eine Fragmentierung des Datenschutzrechts hinsichtlich der Regulierung von Risikotechnologien vorteilhaft ist und deshalb in Betracht gezogen oder ob die Abstraktheitsfunktion der Technikneutralität beibehalten werden sollte.[53]

[48] Vgl dazu: *Höhne* Thomas, „Neue" Persönlichkeitsrechte in „neuen Medien", in Berka/Grabenwarter/Holoubek (Hrsg), Persönlichkeitsschutz in elektronischen Massenmedien, Bd 9 der Schriftreihe Recht der elektronischen Massenmedien REM (Manz Wien 2012) 35 ff wörtlich: Google verfügt mittlerweile über Patente, die bspw darin bestehen, dass ein einziges Bild von mindestens fünf Megapixeln genügt, um eine Person nur anhand der Augen und Hautcharakteristika zu identifizieren.
[49] *Martini,* Blackbox 212.
[50] *Roßnagel,* DuD 2017/5, 277 ff; ErwG 10 DSVO; *Martini,* Blackbox 212.
[51] *Roßnagel,* DuD 2017/5, 277 (278).
[52] *Roßnagel,* DuD 2017/5, 277 (278).
[53] Vgl. ErwG 15 DSGVO.

Ziel der Arbeit:

In meiner Arbeit möchte ich deshalb evaluieren, ob die Gefährdungspotentiale ausgehend vom biometrischen Gesichtserkennungsverfahren von der DSGVO vollumfänglich erfasst sind und wie die Risikobeurteilung nach der DSGVO im Detail geregelt ist und welche offenen Rechtsfragen sich daraus im Speziellen ergeben, weshalb ich methodisch die einzelnen Bestimmungen, die ausdrücklich auf eine Risikobeurteilung abstellen untersuchen werde. Voraussichtlich wird sich der Schwerpunkt meiner Arbeit ausschließlich auf die präventive Risikoregulierung richten.

In summa summarum wird sich mein Dissertationsvorhaben mit der Risikoregulierung von Gesichtserkennungstechnologien beschäftigten und im ersten Schritt die derzeit geltenden Ansätze der DSGVO (vor allem Art 25, 35 und den Antidiskriminierungsschutz) untersuchen und im zweiten Schritt sollen Lösungsvorschläge formuliert und präsentiert werden, die die Zulässigkeit von Gesichtserkennungstechnologien an das damit einhergehende Risiko zu koppeln versuchen.

Abschließend ergeben sich für die inhaltliche Grundlage meines Dissertationsvorhabens aus dem soeben skizzierten Problemaufriss folgende Forschungsfragen:

Wie ist die Risikoregulierung in der DSGVO ausgestaltet? Wie sehen die rechtlichen Vorgaben zur Risikoermittlung im Detail aus? Wie sollte die Risikoermittlung beim Einsatz von biometrischen Erkennungsverfahren rechtlich gestaltet sein, um die Rechte der Betroffenen bestmöglich zu schützen? Welche Rechtsgüter werden durch die DSGVO bzw. sollten zusätzlich beim Einsatz von Gesichtserkennungssoftware verstärkt geschützt werden? Welche datenschutzrechtlichen Besonderheiten weist das geometrische Gesichtsmerkmal auf? Sollte die Zulässigkeit von dem damit einhergehenden Risiko abhängig gemacht werden? Wie könnte dies rechtlich bewerkstelligt werden? Wie kann man Gesichtserkennungstechnologien transparenter gestalten, um technikbasierte Diskriminierungen zu erkennen und präventiv zu vermeiden? Wie sehen die rechtlichen Gestaltungsmöglichkeiten für die Mitgliedstaaten aus?

Vorläufiger Zeitplan:

Ist-Stand: Absolvierung eines Seminars aus Rechtsphilosophie und aus dem Öffentlichen Recht; Erfolgreiche Teilnahme an der VO Juristische Methodenlehre, Recherche und Annäherung an das Dissertationsthema, Verfassen eines Exposés

SS 2020: Vorstellung des Dissertationsvorhabens und Abschließung der Dissertationsvereinbarung; weitere vertiefende Problembefassung und Beginn mit der Ausarbeitung

WS2020/21 – SS 2022: Einschlägige Lehrveranstaltungen aus dem Bereich „Technologierecht" und „Computer und Recht", Verfassen der Dissertation, Finalisieren der Arbeit, Abgabe der Dissertation

WS 2022/23: Vornahme von Korrekturen, Abgabe der Endfassung, Öffentliche Defensio

Auszug aus dem Literaturverzeichnis

Albrecht Astrid, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz (Nomos Frankfurt 2003)

Amtsblatt der Europäischen Union, Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu „Die digitale Revolution und die Bedürfnisse und Rechte der Bürgerinnen und Bürger", C 190/7 am 05.06.2019

Bächle Thomas Chistian, „Hochinvasive Überwachung" und der Verlust der Autonomie (die es nie gab?), in *Thimm* Caja/*Bächle* Thomas Christian (Hrsg), Die Maschine: Freund oder Feind? (Springer Wiesbaden 2019)

Bieker Felix/*Brennert* Benjamin/*Hansen* Marit, Die Risikobeurteilung nach der DSGVO, DuD 2018/8, 492 ff

Bisges Marcel, Personendaten, Wertzuordnung und Ökonomie, MMR 2017, 301 ff

BSI, Biometrie und Gesichtserkennung: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile&v=1 (25.02.2020)

Conrad Sebastian Conrad, Kann die Künstliche Intelligenz den Menschen entschlüsseln? – Neue Forderungen zum Datenschutz, DuD 2018/9, 541-546

Conrad Sebastian Conrad, Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017/12, 740-744

Datenschutzkonferenz (DSK), Positionspapier zur biometrischen Analyse, 3. und 4. April 2019 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden

Datenschutzkonferenz (DSK), Datenschutzfolgeabschätzung nach Art 35 DSGVO (Kurzpapier Nr. 5): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (01.07.2020)

Datenschutzkonferenz (DSK), Risiko für die Rechte und Freiheiten natürlicher Personen (Kurzpapier Nr. 18): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (01.07.2020)

Datenschutzgruppe nach Art 29, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01

EDPB, Guidelines 3/2019 on processing of personal data through video devices (Version 2.0): https://www.dsb.gv.at/documents/22758/1101467/guidelines_3_2019_video_devices.pdf/febd7ed7-7e94-46fa-9698-74d911ad8ba2 (14.06.2020)

EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Version 3.0): https://www.dsb.gv.at/documents/22758/1101467/guidelines_1_2018_on_certification_and_identifying_certification_criteria_in_accordance_with_articles_42_and_43_of_the_regulation.pdf/2c1dc0e2-38f6-4a62-910f-80f9e9f7fd02 (14.06.2020)

Datenschutzgruppe nach Art. 29, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01

Dotzler Florian, Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen (Springer Wiesbaden 2010)

Ehmann Eugen, Personenaufnahmen nach der DS-GVO, ZD 2020, 65 ff

Eifert Martin, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521 ff

Eisenberger Iris, Digitalisierung und Selbstbestimmung, ALJ 2017/2, 140-149

Ennöckl Daniel, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung (Verlag Österreich Wien 2014)

Ennöckl, Daniel, Aktuelle Herausforderungen im Datenschutzrecht, JRP 2015/23, 158-168

Europäische Kommission, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final am 19.02.2020

Feiler Lukas/ *Horn* Bernhard, Umsetzung der DSGVO in der Praxis (Verlag Österreich Wien 2018)

Feiler Lukas/*Forgó* Nikolaus, EU-DSGVO (Verlag Österreich 2017)

Fuhlrott Michael, Data Incident Management: Rechtlicher Umgang mit „Datenpannen", NZA 2019, 649 ff

Heißl Gregor, Grundrechtskollisionen am Beispiel von Persönlichkeitseingriffen sowie Überwachungen und Ermittlungen im Internet (Verlag Österreich Wien 2017)

Heißl Gregor, Persönlichkeitseingriffe im Internet (Verlag Österreich Wien 2017)

Heldt Amélie P., Gesichtserkennung: Schlüssel oder Spitzel?, MMR 2019, 285 ff

HmbbBfDI, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg: https://datenschutz-hamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf (25.02.2020)

Höhne Thomas, „Neue" Persönlichkeitsrechte in „neuen Medien", in *Berka/Grabenwarter/Holoubek* (Hrsg), Persönlichkeitsschutz in elektronischen Massenmedien, Bd 9 der Schriftreihe Recht der elektronischen Massenmedien REM (Manz Wien 2012) 1 ff

Höhne Thomas, DSGVO und Digitalfotografie, ZIIR 2018, 244 ff

Hornung Gerrit/ *Schindler* Stephan, Das biometrische Auge der Polizei, ZD 2017, 203 ff

Jandt Silke, Biometrische Videoüberwachung – was wäre wenn …, ZRP 2018, 16 ff

Klaushofer Reinhard, Die menschenrechtliche Dimension Künstlicher Intelligenz, ZÖR 2019/74, 399-425

Knorre Susanne/*Müller-Peters* Horst/*Wagner* Fred, Die Big-Data Debatte. Chancen und Risiken der digital vernetzten Gesellschaft (Springer Wiesbaden 2020)

Lioba Kasper/*Trettner* Hannes, Zutrittskontrolle mittels Handvenenerkennung bei Badegästen, ZIIR 2019, 394 ff

Martini Mario, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz (Springer Berlin 2019)

Matejek Michael/*Mäusezahl* Steffen, Gewöhnliche vs. Sensible personenbezogene Daten, ZD 2019, 551 ff

Mülleder Lisa, Datenschutz und Privatsphäre in Social Networks am Beispiel von Facebook, SPRW 2014, 471 ff

Opel Alexander/ *Körffer* Barbara/ *Nouak* Alexander, Datenschutz bei der Erhebung biometrischer Testdaten, DuD 2013/6, 347-351

Reuter Wiebke, Umgang mit sensiblen Daten bei allgemeiner Videoüberwachung, ZD 2018, 564 ff

Schindler Stephan, Biometrische Gesichtserkennung in den USA, ZD-Aktuell 2019, 06595

Schindler Stephan, China: Biometrische Gesichtserkennung in der Volksrepublik China, ZD-Aktuell 2019, 06494

Schindler Stephan, Super-Recognizer: Die menschliche Alternative zur biometrischen Gesichtserkennung?, ZD-Aktuell 2019. 06730

Schneider Jana/*Schindler* Stephan, Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, ZD 2018, 463 ff

Schrems Maxmilian, Private Videoüberwachung. Ein Leitfaden. (Jan Sramek Verlag Wien 2011)

Schwaiger Christina Maria, Biometrische Gesichtserkennung, in *Jahnel* Dietmar (Hrsg), Jahrbuch Datenschutzrecht 2016 (NWV 2016) 193 ff

Schweitzer Heike, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569 ff

Schwenke Thomas, Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach DS-GVO, NJW 2018, 823 ff

Seiss Constanze und *Raabe-Stuppnig* Katharina, Kinder und ihre Persönlichkeitsrechte, ZIR 2014/2, 100 – 105

Solmecke Christian/*Kocatepe* Sibel, Google Glass – Der Gläserne Mensch 2.0, ZD 2014, 22 ff

Steege Hans, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz, MMR 2019, 715 ff

Thiel Markus, Die Vermessung der Welt? – Zur Nutzung biometrischer Identifikationssysteme durch die Sicherheitsbehörden, ZRP 2016, 218 ff

Thiele Clemens, Persönlichkeitsschutz in Neue Medien – Facebook, Google & Co., Österreichisches Anwaltsblatt 2013/1, 11-18

Tinnefeld Marie-Theres, …fertig ist das Gesicht – eine Betrachtung im Spiegel digitaler Gesichtserkennungssysteme, MMR 2018, 777 ff

Vultejus Ulrich, Informationelle Selbstbestimmung auch bei Genen, ZRP 2002, 70 ff

Weichert Thilo, Big Data und Datenschutz, ZD 2013, 251 ff

Weichert Thilo, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463 ff

Weichert Thilo, Drohnen und Datenschutz, Bedrohungspotenzial und Gesetzgebungsbedarf bei der Beobachtung von oben, ZD 2012, 501 ff

Weichert Thilo, Informationstechnische Arbeitsstellung und datenschutzrechliche Verantwortung, ZD 2014, 605 ff

Winter Christian/*Battis* Verena/ *Halvani* Oren, Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489 ff

Däs Sebastian, Compliance-konforme Einbindung biometrischer Authentifizierungssysteme in das betriebliche IT-Sicherheitsmanagement (Springer Köln 2018)

Desoi Bernd Uwe, Big Data und allgemein zugängliche Daten im Krisenmanagement (Springer Wiesbaden 2018)

Taeger Jürgen, Chancen und Risiken von Smart Cams im öffentlichen Raum (Nomos Baden-Baden 2017)

Bretthauer Sebastian, Intelligente Videoüberwachung (Nomos Baden-Baden 2017)

Bieker Felix/*Bremert* Benjamin/*Hansen* Marit, Die Risikobeurteilung nach der DSGVO, DuD 2018/8, 492 ff

Rottmeier Christian*/Eckerl* Philipp, Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren, NStZ 2020, 193 ff

Feiler Lukas, Selig, die sehen und doch nicht glauben, Die Presse 2018/44/02

Drahansky Martin/*Goldmann* Tomaš/*Spurny* Martin, Gesichtsdedektion und -erkennung aus Videos aus öffentlichen Kamerasystemen ‚DuD 2017/7, 415 ff