



Edition KWV

Die „Edition KWV“ beinhaltet hochwertige Werke aus dem Bereich der Wirtschaftswissenschaften. Alle Werke in der Reihe erschienen ursprünglich im Kölner Wissenschaftsverlag, dessen Programm Springer Gabler 2018 übernommen hat.

Weitere Bände in der Reihe <http://www.springer.com/series/16033>

Florian Dotzler

Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen

Eine exemplarische Betrachtung von
Systemen auf der Grundlage des
biometrischen Merkmals Tippverhalten

Florian Dotzler
Wiesbaden, Deutschland

Bis 2018 erschien der Titel im Kölner Wissenschaftsverlag, Köln
Dissertation Universität Regensburg, 2009

Edition KWW
ISBN 978-3-658-24047-9 ISBN 978-3-658-24048-6 (eBook)
<https://doi.org/10.1007/978-3-658-24048-6>

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

Springer Gabler

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2010, Nachdruck 2019

Ursprünglich erschienen bei Kölner Wissenschaftsverlag, Köln, 2010

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

*Meinen Eltern
für ihr Vorbild und ihr Vertrauen*

Erstes Geleitwort

Eine wirksame und effiziente Authentifizierung ist notwendige Voraussetzung für den sicheren Zugang und den nachvollziehbaren Zugriff auf die wertvolle Ressource „Information“. Biometrische Verfahren werden für diese Aufgabenstellung seit einigen Jahren in der Praxis eingesetzt. Denn sie bieten zunehmende Effizienz und können, wenn sie entsprechend gestaltet werden, auch einen sehr hohen Zugangs- und Zugriffsschutz gewährleisten. Andererseits wirft der Personenbezug der Daten unmittelbar Fragen des Datenschutzes auf, ohne dass zu den aktuellen Entwicklungen angemessene gesetzliche Regelungen oder eine umfassende Rechtsprechung existieren. Dies hat zu erheblicher Verunsicherung im praktischen Einsatz geführt und erfordert immer wieder lange Diskussionsprozesse in den Unternehmen. In einigen Fällen mussten sogar bereits getätigte Investitionen abgeschrieben werden. Die vorliegende Publikation hat das Ziel, diese Lücke zu schließen, und geht die Aufgabe in drei Schritten an. Zunächst werden die IT-technischen wie auch die juristischen Grundlagen gelegt. Dieser Schritt vermittelt auch denjenigen das nötige Ausgangswissen, die sich nicht täglich mit der Materie befassen. Im zweiten Schritt arbeitet der Autor heraus, wie der Einsatz unterschiedlicher biometrischer Verfahren vor dem Hintergrund datenschutzrechtlicher Aspekte zu beurteilen ist. Er entwickelt dazu ein Bewertungsverfahren und setzt ein Zwei-Ebenen-Modell mit einem Kriterienkatalog ein, das sowohl wissenschaftlich abgesichert als auch für den praktischen Einsatz tauglich ist. Schließlich zeigt der Autor anhand des konkreten Beispiels „Tippverhalten“, wie biometrische Verfahren so ausgestaltet werden können, dass ihre Anwendung bestmöglich mit datenschutzrechtlichen Aspekten vereinbar ist. Ein breiter empirischer Test rundet die Untersuchung ab. Die Ergebnisse der Arbeit sind überzeugend. Dem Autor ist es gelungen, die juristische und die IT-technische Sicht voll integriert und in gleicher Tiefe zu betrachten. Die Ergebnisse halten nicht nur den Kriterien stand, die an wissenschaftliches Arbeiten gestellt werden. Die Arbeit ist auch so praxisnah gehalten und formuliert, dass sie einen hervorragenden Leitfaden für die Verantwortlichen im Unternehmen zur Verfügung stellt. Insofern wünsche ich mir, dass dieser Leitfaden zum Standard-Vorgehensmodell zur Lösung der geschilderten Problemstellung wird.

Regensburg, im Januar 2010

Prof. Dr. Hans-Gert Penzel
Generaldirektor
Europäische Zentralbank

Zweites Geleitwort

Die Schnittstelle zwischen Informationstechnologie und Datenschutz(recht) ist äußerst praxisrelevant und es zeichnet sich ab, dass sie in Zukunft noch weiter an Bedeutung gewinnen wird. Gerade die Frage der Datenvermeidung und Datensparsamkeit spielt in diesem Zusammenhang eine herausragende Rolle. Für dieses grundlegende datenschutzrechtliche Prinzip gilt in besonderer Weise die Problematik eines massiven Vollzugsdefizits, weil es weder trennscharfe Kriterien noch sinnvolle Möglichkeiten der Kontrolle und Vollstreckung gibt. In diesem Buch werden interdisziplinär Ideen zum Einsatz biometrischer Systeme in Unternehmen entwickelt, die nicht zuletzt speziell in dieser Hinsicht fruchtbar gemacht werden können.

Zunächst wird dem Leser eine instruktive Darstellung datenschutzrechtlicher Grundlagen geboten, wobei bereits erste Übertragungen auf biometrische Systeme vorgenommen werden. Sodann wird konkret der betriebliche Einsatz der Biometrie beleuchtet. Sowohl Risiken als auch geeignete Schutzmaßnahmen werden herausgearbeitet und evaluiert. Unter Berücksichtigung der besonderen Gefahren einer dauerhaften Merkmalskompromittierung werden entsprechende Beurteilungskriterien entwickelt und auf ausgewählte Systeme angewendet. Dabei werden die Ansätze nicht nur differenziert und strukturiert dargelegt, sondern auch umfassenden empirischen Tests unterzogen.

Die Arbeit ist im besten Sinne interdisziplinär und in beiden Bereichen gleichermaßen profund. Ihr ist eine nachhaltige Rezeption gerade auch in der Praxis zu wünschen.

Regensburg, im Januar 2010

Prof. Dr. Jürgen Kühling, LL.M.

Lehrstuhl für Öffentliches Recht und Immobilienrecht

Universität Regensburg

Vorwort

Die vorliegende Arbeit entstand während meiner Forschungs- und Projektstätigkeit am Lehrstuhl für Wirtschaftsinformatik II, insbesondere Bankinformatik an der Universität Regensburg. Sie wurde von der wirtschaftswissenschaftlichen Fakultät der Universität Regensburg als Dissertation unter dem Titel „Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen - Eine exemplarische Betrachtung von Systemen auf der Grundlage des biometrischen Merkmals Tippverhalten“ angenommen. Da sich die Arbeit auf den folgenden über 200 Seiten mit dem sehr interessanten, aber dadurch umfassend behandelten Thema der datenschutzrechtlichen Bewertung biometrischer Systeme befasst, möchte ich an dieser Stelle auf inhaltliche Aus- und Einführungen verzichten.

Vielmehr ist es mir ein großes Anliegen, mich bei denjenigen Menschen zu bedanken, die mich bei meiner Arbeit und somit auf dem Weg zu diesem Vorwort so gut und uneigennützig unterstützt haben. Für die Übernahme der Begutachtung sowie die wissenschaftliche Begleitung der Arbeit möchte ich mich bei Prof. Dr. Hans-Gert Penzel und Prof. Dr. Jürgen Kühling bedanken. Sie konnten in vielen Gesprächen durch ihre Erfahrung und ihre Fähigkeit, die richtigen Fragen zu stellen, entscheidende Hilfestellung und großen fachlichen Input geben. So verschafften sie mir eine solide und verlässliche Basis für meine Arbeit. Ferner gilt mein Dank zahlreichen Freunden und Kollegen für ihre Unterstützung während der Zeit der Erstellung meiner Dissertation: Dr. Thomas Wölfl, der meine Arbeit stets förderte und durch seine Expertise immer der richtige fachliche Ansprechpartner war, Prof. Dr. Dieter Bartmann, der mich in unzähligen Diskussionen mit neuen Ideen und seiner Begeisterung unterstützte sowie mir die Betrachtung des Praxisbeispiels bei der Psylock GmbH ermöglichte, Dr. Marco Nirschl, Karl Mühlbauer, Sebastian Däs und Christian Senk, die beim Lesen der Arbeit akribisch und ausdauernd jedem Satz und jedem Wort auf den Zahn fühlten.

Schließlich gilt mein größter Dank meinen Eltern, Anneliese und Georg Dotzler, auf die ich mich stets verlassen konnte. Sie haben meine Ausbildung bis zur Promotion immer uneingeschränkt unterstützt und mir zu jeder Zeit das größtmögliche Vertrauen geschenkt. Daneben haben Sie mir bedeutende Werte wie Fleiß, Zielstrebigkeit und Ausdauer vermittelt und vorgelebt und mir gezeigt, was es heißt, für andere einzustehen.

Meinen Eltern widme ich diese Arbeit.

Regensburg, im Januar 2010

Dr. Florian Dotzler

Inhaltsübersicht

Abbildungsverzeichnis	XXIII
Tabellenverzeichnis	XXV
Abkürzungsverzeichnis.....	XXVII
Management Summary	XXIX
1 Datenschutz und der betriebliche Einsatz der Biometrie	1
2 Grundlagen biometrischer Authentifizierungssysteme	3
3 Biometrische Systeme auf der Basis des Merkmals Tippverhalten	49
4 Datenschutzrechtlich relevante Vorschriften und Konzepte.....	65
5 Biometriespezifisches Gefährdungspotenzial und Schutzmaßnahmen ...	101
6 Bewertungskriterien für eine datenschutzrechtliche Evaluation.....	131
7 Evaluation ausgewählter Tippverhalten basierender Systeme	151
8 Legitimationsgrundlage für den Systemeinsatz im Unternehmen.....	207
9 Abschließende Wertung und Ausblick	217
Literaturverzeichnis	221

Inhaltsverzeichnis

Abbildungsverzeichnis	XXIII
Tabellenverzeichnis	XXV
Abkürzungsverzeichnis	XXVII
Management Summary	XXIX
1 Datenschutz und der betriebliche Einsatz der Biometrie	1
1.1 Notwendigkeit einer datenschutzrechtlichen Betrachtung des betrieblichen Einsatzes biometrischer Systeme	1
1.2 Aufbau der Arbeit	2
2 Grundlagen biometrischer Authentifizierungssysteme	3
2.1 Biometrie und biometrische Merkmale	3
2.2 Technische Grundlagen biometrischer Systeme	5
2.2.1 Prinzipien der Authentizitätsprüfung	5
2.2.2 Aufbau eines biometrischen Systems	9
2.2.3 Ablauf einer biometrischen Authentifizierung	12
2.2.4 Adaptive biometrische Verfahren	15
2.2.5 Betriebsarten biometrischer Systeme	16
2.2.5.1 Betrieb im Verifikationsmodus	16
2.2.5.2 Betrieb im Identifikationsmodus	18
2.3 Sicherheit biometrischer Systeme	20
2.3.1 Sicherheit durch biometrische Systeme	20
2.3.2 Erhöhte Sicherheitsnotwendigkeit beim Systemeinsatz	21
2.3.3 Fehlerraten als Gütemaße für die Erkennungsleistung biometrischer Verfahren und Systeme	22
2.3.3.1 Grundlegendes zur Ermittlung von Fehlerraten	23
2.3.3.2 False Accept Rate (FAR)	23
2.3.3.3 False Rejection Rate (FRR)	24
2.3.3.4 Equal Error Rate (EER)	25

2.3.3.5	Detection Error Trade-off (DET)- und Receiver Operating Characteristic (ROC)-Kurve.....	28
2.3.3.6	Failure to Enrol Rate (FTE).....	30
2.3.3.7	Failure to Acquire Rate (FTA)	31
2.3.3.8	False Match Rate (FMR) und False Non-Match Rate (FNMR) vs. FAR und FRR	32
2.3.4	Statistische Signifikanz der Fehlerraten.....	34
2.3.5	Versuchsdesign für die Ermittlung der Fehlerraten	44
3	Biometrische Systeme auf der Basis des Merkmals Tippverhalten.....	49
3.1	Tippverhalten als biometrisches Merkmal.....	49
3.2	Biometrische Verfahren zur Tippverhaltenserkennung.....	53
3.3	Biometrische Systeme auf der Grundlage des Tippverhaltens.....	57
3.3.1	Repräsentative Systemansätze.....	57
3.3.1.1	Textgebundene Authentifizierungssysteme	58
3.3.1.2	Textungebundenen Authentifizierungssysteme	61
3.3.2	Psylock-Kernsystem als Basisarchitektur für verschiedene Systemansätze.....	63
4	Datenschutzrechtlich relevante Vorschriften und Konzepte	65
4.1	Recht auf informationelle Selbstbestimmung.....	66
4.2	Personenbezug biometrischer Daten.....	68
4.3	Grundsätze und Vorschriften aus dem Bundesdatenschutzgesetz als Ausgangspunkte einer Bewertung	71
4.3.1	Notwendigkeit einer Rechtsvorschrift oder einer Einwilligung für die Einsatzlegitimation	71
4.3.2	Grundsatz der Zweckbindung	72
4.3.3	Grundsatz der Erforderlichkeit.....	72
4.3.4	Grundsatz der Datenvermeidung und der Datensparsamkeit.....	73
4.3.5	Schutz sensibler Daten	74
4.3.6	Transparenzgebot, offene Datenerhebung und Grundsatz der Direkterhebung	75

4.3.7	Technische und organisatorische Schutzmaßnahmen	76
4.4	Weitere relevante Vorschriften und Gegebenheiten	77
4.4.1	Grundgesetzlich motivierte Aspekte	77
4.4.1.1	Grundsatz der Gleichheit	77
4.4.1.2	Gefahr der Schaffung eines einheitlichen Personenkennzeichens	78
4.4.2	Legitimationsgrundlagen mit datenschutzrechtlicher Relevanz für den betrieblichen Systemeinsatz	80
4.4.2.1	Einwilligung oder Rechtsvorschrift als Ausgangsbasis einer Legitimation	80
4.4.2.2	Allgemeine Normierung des Persönlichkeitsschutzes in § 75 Abs. 2 Satz 1 BetrVG	82
4.4.2.3	Mitbestimmung des Betriebsrats gemäß § 87 Abs. 1 Satz 6 BetrVG	84
4.4.2.4	Legitimation des betrieblichen Einsatzes biometrischer Systeme auf der Grundlage des § 32 Abs. 1 Satz 1 BDSG	89
4.5	Position und Mitwirken des betrieblichen Datenschutzbeauftragten bei der Einführung biometrischer Systeme	93
4.5.1	Rolle des betrieblichen Datenschutzbeauftragten	94
4.5.2	Position und Verantwortlichkeit des Datenschutzbeauftragten bei der Einführung biometrischer Systeme im Unternehmen	96
4.5.3	Zusammenarbeit mit dem Betriebsrat	97
5	Biometricspezifisches Gefährdungspotenzial und Schutzmaßnahmen... 101	
5.1	Allgemeine Risiken für den Einsatz biometrischer Systeme	102
5.2	Spezielle Risiken für den Einsatz biometrischer Systeme	103
5.2.1	Unrechtmäßige Aneignung der Nutzeridentität	103
5.2.2	Missbräuchliche Verwendung von Zusatzinformationen	105
5.2.3	Gefahr der lebenslangen Merkmalskompromittierung	106
5.2.4	Überwachungseignung biometrischer Systeme	107
5.2.5	Bildung von Personenprofilen	108

5.2.6	Zwang zur Nutzung biometrischer Systeme	109
5.3	Schutzmaßnahmen gegen das bestehende Gefährdungspotenzial.....	110
5.3.1	Technische Schutzmaßnahmen	110
5.3.1.1	Schutzmaßnahmen gegen den Datendiebstahl	110
5.3.1.2	Absicherung der Funktionsfähigkeit des Systems.....	114
5.3.1.3	Absicherung gestohlener oder verlorener biometrischer Daten.....	117
5.3.2	Gesetzliche Schutzmaßnahmen.....	120
5.3.3	Vertragliche Schutzmaßnahmen.....	121
5.4	Vertrauensbildende Maßnahmen als datenschutzförderliches Instrumentarium.....	122
5.4.1	Transparenz gegenüber den Systemnutzern.....	122
5.4.2	Überprüfung und Zertifizierung durch unabhängige Dritte	124
5.4.3	Selbstbeschränkung des Systembetreibers	126
5.4.4	Freiwilligkeit der Systemnutzung	127
5.5	Biometrie und Privacy Enhancing Technology (PET).....	128
6	Bewertungskriterien für eine datenschutzrechtliche Evaluation	131
6.1	Prüfkriterien für eine Bewertung biometrischer Merkmale	133
6.1.1	Informationsgehalt des biometrischen Merkmals	133
6.1.2	Zeitliche Variabilität des biometrischen Merkmals	134
6.1.3	Ausspähbarkeit des biometrischen Merkmals.....	135
6.1.4	Willentliche Beeinflussbarkeit des biometrischen Merkmals....	136
6.2	Prüfkriterien für eine Bewertung biometrischer Systeme	137
6.2.1	Notwendigkeit des Systemeinsatzes.....	137
6.2.2	Berücksichtigung des vorab zu definierenden Verwendungszwecks im Systemdesign	138
6.2.3	Berücksichtigung der Erforderlichkeit im Systemdesign	139
6.2.4	Betriebsart des Systems: Identifikation versus Verifikation.....	140
6.2.5	Verzicht auf die Anlage einer zentralen Referenzdatenbank.....	141

6.2.6	Umsetzung eines datenschutzfreundlichen Speicherkonzepts ...	142
6.2.7	Reduktion des Personenbezugs bei den biometrischen Daten ...	142
6.2.8	Technische Sicherheit und Zuverlässigkeit des Systems	143
6.2.9	Umgang mit sensiblen Daten im biometrischen System.....	144
6.2.10	Transparenz des Systems und der Sicherheitsmechanismen	145
6.2.11	Gewährleistung hinreichender Mechanismen für die technische und die organisatorische Sicherheit.....	147
6.2.12	Angebot effektiver Alternativverfahren	149
7	Evaluation ausgewählter Tippverhalten basierender Systeme	151
7.1	Detaillierte Evaluation des Merkmals Tippverhalten	152
7.1.1	Informationsgehalt des Tippverhaltens	152
7.1.2	Zeitliche Variabilität des Tippverhaltens	153
7.1.3	Ausspähbarkeit des Tippverhaltens.....	153
7.1.4	Willentliche Beeinflussbarkeit des Tippverhaltens.....	154
7.1.5	Zusammenfassung der Evaluationsergebnisse des biometrischen Merkmals Tippverhalten.....	155
7.2	Vergleichende Gegenüberstellung mit weiteren Merkmalen	156
7.3	Evaluation textgebundener Authentifizierungssysteme	161
7.3.1	Notwendigkeit des Systemeinsatzes.....	161
7.3.2	Berücksichtigung des vorab zu definierenden Verwendungszwecks im Systemdesign.....	163
7.3.3	Berücksichtigung des Grundsatzes der Erforderlichkeit im Systemdesign	164
7.3.4	Betriebsart textgebundener Systemansätze	164
7.3.5	Verzicht auf eine zentrale Referenzdatenbank.....	165
7.3.6	Umsetzung eines datenschutzfreundlichen Speicherkonzepts ...	167
7.3.7	Reduktion des Personenbezugs bei den Tippverhaltensdaten....	169
7.3.8	Technische Sicherheit und Zuverlässigkeit textgebundener Authentifizierungssysteme	170

7.3.8.1	Aufbau des Testszenarios und Beschreibung der Testdatenbasis.....	171
7.3.8.2	Ergebnisse des Performancetests.....	173
7.3.8.3	Vergleich mit weiteren marktgängigen biometrischen Systemen.....	179
7.3.8.4	Bewertung der Sicherheit der Systemarchitektur	181
7.3.8.5	Abschließende Beurteilung des Sicherheitsniveaus	183
7.3.9	Umgang mit sensiblen Daten in textgebundenen Authentifizierungssystemen	183
7.3.10	Transparenz textgebundener Authentifizierungssysteme und deren Sicherheitsmechanismen	184
7.3.11	Gewährleistung hinreichender Mechanismen für die technische und die organisatorische Sicherheit.....	185
7.3.12	Angebot effektiver Alternativverfahren	186
7.3.13	Zusammenfassung der Evaluationsergebnisse textgebundener Systemansätze.....	186
7.4	Evaluation textungebundener Authentifizierungssysteme	188
7.4.1	Notwendigkeit des Systemeinsatzes.....	188
7.4.2	Berücksichtigung des vorab zu definierenden Verwendungszwecks im Systemdesign	190
7.4.3	Berücksichtigung des Grundsatzes der Erforderlichkeit im Systemdesign.....	192
7.4.4	Betriebsart textungebundener Systemansätze	193
7.4.5	Verzicht auf eine zentrale Referenzdatenbank.....	194
7.4.6	Umsetzung eines datenschutzfreundlichen Speicherkonzepts ...	196
7.4.7	Reduktion des Personenbezugs bei den Tippverhaltensdaten....	196
7.4.8	Technische Sicherheit und Zuverlässigkeit textungebundener Authentifizierungssysteme	198
7.4.9	Umgang mit sensiblen Daten in textungebundenen Authentifizierungssystemen	199
7.4.10	Transparenz textungebundener Authentifizierungssysteme und deren Sicherheitsmechanismen	200

7.4.11 Gewährleistung hinreichender Mechanismen für die technische und die organisatorische Sicherheit.....	201
7.4.12 Angebot effektiver Alternativverfahren	202
7.4.13 Zusammenfassung der Evaluationsergebnisse textungebundener Systemansätze	202
8 Legitimationsgrundlage für den Systemeinsatz im Unternehmen.....	207
8.1 Systeme zur Tippverhaltenserkennung und der Schutz der Persönlichkeitsrechte von Betriebsangehörigen	207
8.2 Mitbestimmung des Betriebsrats beim Einsatz von Systemen zur Tippverhaltenserkennung.....	210
8.3 Systeme zur Tippverhaltenserkennung und die im Bundesdatenschutzgesetz manifestierten Legitimationsgrundlagen	214
9 Abschließende Wertung und Ausblick	217
Literaturverzeichnis.....	221

Abbildungsverzeichnis

Abbildung 1: Grundprinzipien der Authentizitätsprüfung.....	7
Abbildung 2: Basisarchitektur eines biometrischen Systems	12
Abbildung 3: Grundsätzlicher Ablauf eines Enrolmentprozesses	14
Abbildung 4: Grundsätzlicher Ablauf eines Verifikationsprozesses	18
Abbildung 5: Grundsätzlicher Ablauf eines Identifikationsprozesses.....	20
Abbildung 6: Zusammenhang von FAR- und FRR-Kurve.....	26
Abbildung 7: Idealtypischer Verlauf von FAR- und FRR-Kurve	28
Abbildung 9: Haltedauern als Charakteristika des Tippverhaltens.....	50
Abbildung 10: Übergangsdauern als Charakteristika des Tippverhaltens.....	51
Abbildung 11: Überholungen als Charakteristika des Tippverhaltens	52
Abbildung 12: Grundsätzlicher Ablauf eines Mustererkennungsverfahrens.....	54
Abbildung 13: Systemarchitektur einer Password Reset Lösung	60
Abbildung 14: Psylock-Kernsystem zur Nutzerauthentifizierung.....	64
Abbildung 15: Ebenenmodell der datenschutzrechtlichen Bewertung	132
Abbildung 16: FAR- und FRR-Kurve des Psylock-Kernsystems	175
Abbildung 17: DET-Kurve des Psylock-Kernsystems	176
Abbildung 18: DET-Kurven weiterer ausgewählter biometrischer Systeme	181

Tabellenverzeichnis

Tabelle 1: „Rule of 3“ zur Abschätzung von Fehlerraten.....	35
Tabelle 2: Doddingtons „Rule of 30“.....	37
Tabelle 3: Best-Practice-Ansatz nach Mansfield und Wayman	38
Tabelle 4: Beta-binomial-Ansatz nach Schuckers	40
Tabelle 5: Logit-beta-binomial-Ansatz nach Schuckers.....	42
Tabelle 6: Datenschutzrechtlich motivierte Bewertung des Tippverhaltens	156
Tabelle 7: Intermerkmalsvergleich Teil I.....	159
Tabelle 8: Intermerkmalsvergleich Teil II	160
Tabelle 9: Arbeitspunkte für den Vergleich der Erkennungsleistung.....	177
Tabelle 10: Konfidenzintervallschätzungen.....	179
Tabelle 11: Bewertung textgebundener Authentifizierungssysteme	187
Tabelle 12: Bewertung textungebundener Authentifizierungssysteme Teil I	204
Tabelle 13: Bewertung textungebundener Authentifizierungssysteme Teil II	205

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interface
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BER	Binning Error Rate
BEM	Biometrics Evaluation Methodology
BetrVG	Betriebsverfassungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CC	Common Criteria
d. h.	das heißt
DET	Detection Error Trade-off
DNA	Desoxyribonukleinsäure
EAL	Evaluation Assurance Level
EG-DSRL	Europäische Gemeinschaft Datenschutzrichtlinie
et al.	et alii
etc.	et cetera
evtl.	eventuell
f.	folgende Seite
FAQ	Frequently Asked Questions
FAR	False Accept Rate
ff.	folgende Seiten
FIR	False Identification Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
FTA	Failure to Acquire
FTE	Failure to Enrol
GG	Grundgesetz

i. d. R.	in der Regel
i. V. m.	in Verbindung mit
IP	Internetprotokoll
ISO	International Organization of Standardization
IT	Informationstechnologie
LDAP	Lightweight Directory Access Protocol
LDSG	Landesdatenschutzgesetz
Mrd.	Milliarde(n)
NEA	Number of Genuine or Enrollee Attempts
NFA	Number of False Rejections
NIA	Number of Imposter Attempts
NNA	Number of Not Acquired Persons
NNE	Number of Not Enrolled Persons
NPU	Number of Potential Users
PC	Personal Computer
PET	Privacy Enhancing Technology
PIN	Persönliche Identifikationsnummer
PP	Protection Profile
PR	Penetration Rate
Rn.	Randnotiz
ROC	Receiver Operating Characteristics
sog.	sogenannt
u. Ä.	und Ähnliche(s)
u. U.	unter Umständen
USA	United States of America
z. B.	zum Beispiel

Management Summary

Die Rahmenbedingungen des betrieblichen Einsatzes biometrischer Systeme sind aus datenschutzrechtlicher Sicht in Deutschland derzeit nicht eindeutig geregelt. Es mangelt sowohl an der entsprechenden Gesetzgebung als auch an einer konkreten und eindeutigen Rechtsprechung in diesem Bereich. Die Beurteilung biometrischer Systeme und deren Betrieb erfolgt aktuell aus einer einseitig geprägten juristischen Sichtweise, welche die technischen Eigenheiten und Details der entsprechenden Anlagen oftmals sehr allgemein betrachtet und dementsprechend nur pauschal beurteilt. Das Bundesdatenschutzgesetz und das Betriebsverfassungsgesetz, die spärliche Rechtsprechung in diesem Bereich und eine Reihe datenschutzrechtlicher Konzepte können aber herangezogen werden, um dennoch Richtlinien und Vorgaben für ein datenschutzfreundliches Design und einen rechtskonformen betrieblichen Einsatz biometrischer Systeme abzuleiten.

Diese Arbeit beschäftigt sich sowohl mit den gesetzlich begründeten Anforderungen als auch mit den technischen Details biometrischer Lösungen am Beispiel von auf dem Tippverhalten basierenden Anlagen. Sie schließt also für diesen Anwendungsfall die Lücke zwischen der technischen Betrachtung und einer stark einseitig juristisch geprägten Beurteilung. Die vorliegende Abhandlung identifiziert Gefährdungen für den Datenschutz, die mit dem betrieblichen Einsatz von Biometrie einhergehen, und leitet Schutzmaßnahmen ab, welche dieses Risikopotenzial reduzieren können. Sie ermittelt weiterhin die datenschutzrechtlich relevanten Anforderungen und Rahmenbedingungen, die es beim Einsatz biometrischer Systeme in Unternehmen zu beachten gilt. Aus diesen Grundlagen werden allgemeine Richtlinien abgeleitet, welche für eine Bewertung unterschiedlicher Systeme, die mit verschiedenen biometrischen Merkmalen arbeiten, heranzuziehen sind.

Die praktische Untersuchung von Systemansätzen auf der Basis des vornehmlich verhaltensgeprägten biometrischen Merkmals Tippverhalten liefert eine Reihe von Erkenntnissen und unterstreicht die Praxistauglichkeit der identifizierten Wertungskriterien. Es wird dabei die allgemein vorherrschende Meinung entkräftet, dass derartige Systeme immer dazu geeignet sind, den Nutzer verdeckt zu überwachen. Diese Aussage ist als zu pauschal und zu wenig differenziert zu erachten. Das biometrische Merkmal Tippverhalten weist vielmehr eine Reihe von Eigenschaften auf, die aus Sicht des Datenschutzes sehr positiv zu beurteilen sind. Es enthält beispielsweise grundsätzlich keine sensiblen personenbezogenen Daten und es tritt nicht offen zutage. Ferner zeichnet sich das Merkmal durch seine verhältnismäßig hohe zeitliche Variabilität und seine gute willentliche Beeinflussbarkeit aus.

Systemansätze, die mit einem Erkennungsverfahren arbeiten, welches immer denselben Eingabetext verlangt, sind bezüglich der datenschutzrechtlichen Vorgaben als durchweg vorteilhaft zu sehen. Kritisch im Sinne des Datenschutzes ist hingegen nur das Design und der Einsatz spezieller Anlagen, die mit einem Erkennungsverfahren arbeiten, welches beliebige Eingabetexte verarbeiten kann, und die zur verdeckten Nutzerüberwachung geeignet sind. Aber auch im Falle eines derartigen Erkennungsverfahrens erweisen sich nicht alle möglichen Systemarchitekturen als problematisch. Ein Systemdesign, das von den im Rahmen dieser Arbeit abgeleiteten Wertungskriterien als gut empfunden wird, verbunden mit einem für den Nutzer transparenten Systembetrieb, ermöglicht auch hier eine datenschutzrechtlich unbedenkliche Verwendung biometrischer Anlagen zur Tippverhaltenserkennung im Unternehmen.

Weiterhin zeigt sich, dass die aktuell vorherrschende, rechtlich motivierte Bewertung biometrischer Lösungen häufig zu oberflächlich vorgenommen wird. Vielmehr gilt es bestehende Systeme auch aus juristischer Sicht in Zukunft differenzierter, anwendungsfallbezogener und aus einem mehr technisch geprägten Fokus zu betrachten und zu beurteilen. Diese Arbeit bietet einen Leitfaden für derartige Analysen.