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

Springer Gabler

Florian Dotzler
Wiesbaden, Deutschland

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

Edition KWV
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

Ursprünglich erschienen bei Kölner Wissenschaftsverlag, Köln, 2010

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 Projekttätigkeit 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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

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 Enrolee Attempts
NFA	Number of False Rejections
NIA	Number of Imposter Attempts
NNA	Number of Not Acquired Persons
NNE	Number of Not Enroled 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.