
DuD-Fachbeiträge

Reihe herausgegeben von

G. Hornung, Kassel, Deutschland

H. Reimer, Erfurt, Deutschland

K. Rihaczek, Bad Homburg v.d. Höhe, Deutschland

A. Roßnagel, Kassel, Deutschland

Die Buchreihe ergänzt die Zeitschrift DuD – Datenschutz und Datensicherheit in einem aktuellen und zukunftssträchtigen Gebiet, das für Wirtschaft, öffentliche Verwaltung und Hochschulen gleichermaßen wichtig ist. Die Thematik verbindet Informatik, Rechts-, Kommunikations- und Wirtschaftswissenschaften.

Den Lesern werden nicht nur fachlich ausgewiesene Beiträge der eigenen Disziplin geboten, sondern sie erhalten auch immer wieder Gelegenheit, Blicke über den fachlichen Zaun zu werfen. So steht die Buchreihe im Dienst eines interdisziplinären Dialogs, der die Kompetenz hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit der Informationstechnik fördern möge.

Reihe herausgegeben von

Prof. Dr. Gerrit Hornung
Universität Kassel

Dr. Karl Rihaczek
Bad Homburg v.d. Höhe

Prof. Dr. Helmut Reimer
Erfurt

Prof. Dr. Alexander Roßnagel
Universität Kassel

Weitere Bände in der Reihe <http://www.springer.com/series/12486>

Bernd Uwe Desoi

Big Data und allgemein zugängliche Daten im Krisenmanagement

Exemplarische technische und
normative Gestaltung von Analysen
zur Entscheidungsunterstützung

Mit einem Geleitwort von Prof. Dr. Alexander Roßnagel

 Springer Vieweg

Bernd Uwe Desoi
Universität Kassel
Kassel, Deutschland

Dissertation Universität Kassel (Fachbereich Wirtschaftswissenschaften), 2017, u.d.T.: Rechtsgemäße Big Data-Analysen allgemein zugänglicher Daten zur Entscheidungsunterstützung. Technische und normative Gestaltung dargestellt anhand von Visual Analytics-Werkzeugen im Katastrophenmanagement.

Tag der mündlichen Prüfung: 30.05.2017

DuD-Fachbeiträge

ISBN 978-3-658-21291-9

ISBN 978-3-658-21292-6 (eBook)

<https://doi.org/10.1007/978-3-658-21292-6>

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

Springer Vieweg

© Springer Fachmedien Wiesbaden GmbH 2018

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.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg 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

Geleitwort des Herausgebers

Gegenstand der Arbeit ist eine sehr aktuelle und bedeutsame Herausforderung des Datenschutzrechts, nämlich der Einsatz von Big Data-Analysen – hier zur Entscheidungsunterstützung bei der Gewährleistung von Sicherheit und Katastrophenschutz von kritischen Infrastrukturen.

Durch die Nutzung von Telekommunikation, Internet und datenverarbeitenden Dingen entsteht täglich über jede Person – ob sie sich dessen bewusst ist oder nicht und ob sie dies will oder nicht – eine erhebliche Menge an Daten. Diese aus unterschiedlichen Quellen stammenden, in unterschiedlichen Formaten vorliegenden enormen Datenmassen in sehr kurzer Frist zu analysieren und zu nutzen, ist Zweck von Big Data-Analysen. Damit sollen bisher unbekannte Korrelationen zwischen relevanten Phänomenen entdeckt und Muster des Verhaltens von Einzelnen und Gruppen erkannt werden. Sie werden künftig die Grundlage vieler Entscheidungen für unterschiedlichste Zwecke sein.

Einer dieser Zwecke wird auch die Vermeidung und die Bewältigung von Katastrophen sein, die insbesondere durch den Ausfall von kritischen Infrastrukturen entstehen können. Zu diesem Zweck müssen die Verantwortlichen in kürzester Zeit sehr große Mengen vielfältigster Informationen verarbeiten und für ihre Entscheidungen berücksichtigen. Hierfür wäre es sehr hilfreich, wenn sie Big Data-Werkzeuge für die Daten-Analyse und Visual Analytics als Instrument zur Darstellung der Big Data-Muster verwenden könnten. Als eine wichtige Gruppe von Daten für die Big Data-Auswertung bieten sich für diesen Zweck die öffentlich zugänglichen Daten aus Online Social Networks an. Denn durch den Informationsaustausch über diese Netzwerke können die katastrophalen Entwicklungen an vielen Orten gleichzeitig sehr gut nachvollzogen und analysiert werden.

Sowohl der Zweck der Big Data-Analysen als auch der Einsatz von Big Data und Visual Analytics als Werkzeuge liegen im öffentlichen Interesse. Dennoch darf nicht übersehen werden, dass sie personenbezogene Daten erfassen und individuelles Verhalten analysieren, auch wenn sie sich – wie im Rahmen der Untersuchung – auf allgemein zugängliche Daten beschränken. Sie greifen damit massenhaft in das Grundrecht auf informationelle Selbstbestimmung und weitere Grundrechte ein. Daher stellt sich in diesem Fall für einen rechtsstaatlichen Einsatz von Big Data-Analysen die Frage, ob es gelingen kann, die Vorteile einer Entscheidungsunterstützung zu nutzen und zugleich ihre Nachteile für die Grundrechtsausübung zu vermeiden.

Die Arbeit von Herrn Desoi verfolgt daher das Ziel, die rechtlichen Möglichkeiten und Grenzen von Big Data-Analysen zur Auswertung allgemein zugänglicher Daten zu Zwecken der Entscheidungsunterstützung zu erforschen. Dieses erfolgt exemplarisch am Beispiel des Krisenmanagements, wie es im Fall von gebietsübergreifendem Katastrophenschutz notwendig wird. Die Arbeit konzentriert sich dabei zum einen auf die

Analyse der rechtlichen Gestaltungsmöglichkeiten von Big Data-Analysen und zum anderen auf die normativen Gestaltungsmöglichkeiten, die dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn sowohl den notwendigen Handlungsspielraum liefern als auch die betroffenen Grundrechte bestmöglich schützen.

Für diesen Zweck untersucht Herr Desoi zum einen, wie die Grundrechte, die von Big Data-Analysen betroffen sind, technikadäquat konkretisiert werden müssen. Zum anderen überprüft er die rechtlichen Grundlagen für die Erfassung und Auswertung personenbezogener Daten aus öffentlich zugänglichen Quellen durch Big Data-Analysen. Drittens erarbeitet er Empfehlungen zur rechtlichen Gestaltung fehlender Erlaubnistatbestände und zur organisatorischen und technischen Gestaltung von Entscheidungsunterstützungssystemen, die Grundrechtsrisiken vermeiden.

Indem er diese drei – methodisch wie fachlich – großen Herausforderungen bewältigt, füllt Herr Desoi wesentliche Lücken im Datenschutzrecht. Indem er die für Big Data-Analysen anwendbaren Grundrechte und einfachgesetzlichen Regelungen untersucht, bietet er sowohl wertvolle Hinweise für das notwendige Rechtsverständnis gegenüber modernster Technik und damit grundlegende Hilfestellungen für die Praxis. Indem er zeigt, wie grundrechtliche Risiken durch die rechtliche, technische und organisatorische Gestaltung von Big Data-Entscheidungsunterstützungssystemen vermieden werden können, trägt er zur Bewältigung schwieriger grundlegender Fragen der künftigen Rechtspraxis bei.

Die Arbeit entstand zu großen Teilen im Rahmen der Mitarbeit von Herrn Desoi im Forschungsprojekt „Visual Analytics for Security Applications (VASA)“. In diesem Forschungsprojekt hat die Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel, der Herr Desoi angehörte, die rechtswissenschaftlichen Fragen der rechtlichen Bewertung von Big Data-Analysen aus allgemein zugänglichen Daten zur Gewährleistung von Sicherheit und Katastrophenschutz von kritischen Infrastrukturen untersucht. Das Forschungsprojekt wurde vom Bundesministerium für Bildung und Forschung im Rahmen der „internationalen Kooperation in der zivilen Sicherheitsforschung zwischen Deutschland und den USA“ von 2011 bis 2014 unterstützt. In diesem Verbundprojekt arbeitete provet mit den Universitäten Konstanz und Stuttgart, mit dem Fraunhofer-Institut für graphische Datenverarbeitung (IGD) in Darmstadt und dem Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme (IAIS) in Birlinghofen, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn, der Siemens Corporate Technology (CT) in München und mit der EnBW Energie Baden-Württemberg AG in Karlsruhe zusammen. In diesem Kontext konnte Herr Desoi in enger interdisziplinärer Zusammenarbeit mit Informatikern, Ingenieuren und Praktikern des Katastrophenmanagements Fragen nachgehen, die in der zu begutachtenden Arbeit relevant sind. Er hat die Untersuchung seitdem vervollständigt und auf den heutigen Stand aktualisiert.

Für die künftige Entwicklung und Gestaltung von Big Data-Analysen sowie die rechtswissenschaftliche Diskussion über diese ist zu hoffen, dass die Entscheidungsträger in Politik, Wirtschaft, Justiz, Wissenschaft und Gesellschaft die Erkenntnisse und Hinweise dieser Arbeit zur Kenntnis nehmen und bei ihren Entscheidungen berücksichtigen.

Kassel, im September 2017

Alexander Roßnagel

Vorwort des Autors

Die Arbeit wurde unter dem Titel „Rechtsgemäße Big Data-Analysen allgemein zugänglicher Daten zur Entscheidungsunterstützung – Technische und normative Gestaltung dargestellt anhand von Visual Analytics-Werkzeugen im Katastrophenmanagement“ an der Universität Kassel im November 2016 zur Begutachtung eingereicht. Die Disputation erfolgte 30. Mai 2017. Änderungen der Sach- und Rechtslage wurden für die Druckfassung bis Juli 2017 berücksichtigt. Die Arbeit ist im Wesentlichen in der Zeit als wissenschaftlicher Mitarbeiter an der Universität Kassel zwischen 2011 und 2014 entstanden und wurde seither vervollständigt.

Danken möchte ich zunächst meinem Doktorvater Prof. Dr. Roßnagel für die geduldige Betreuung dieser Arbeit. Ebenfalls danke ich den Herren Prof. Dr. Rott, Prof. Dr. Kuhn und Prof. Thaenert für die Begleitung des Vorhabens durch Zweitbegutachtung beziehungsweise Prüfungsgespräch. Herrn Dr. Dennis Thom von der Universität Stuttgart danke ich für die Antworten auf zahlreiche technische Fragen. Den proveten danke ich für Hinweise, Kritik und Beistand während der Dissertation. Insbesondere Edith Weise danke ich für die administrative Unterstützung während der Zeit in Kassel.

Mein besonderer Dank gilt meiner Schwiegermutter Maria Desoi und meinem Vater Ernst Volland für die kritische Durchsicht und Korrektur des Manuskripts.

Schließlich danke ich ganz herzlich meinen Eltern für die Begleitung während und vor der Dissertation, die zu einem erheblichen Teil zum Gelingen – nicht nur dieser Arbeit – beigetragen hat. Meiner Mutter Gerlinde Volland danke ich für die zahlreichen aufmunternden Worte.

Meiner Frau Monika danke ich ganz besonders für die herausragende Toleranz, Motivation und fachliche Kritik, mit der sie mich in dieser gemeinsam durchlittenen und zeitgleich abgeschlossenen Phase immer begleitet hat.

Karlsruhe, im Oktober 2017

Bernd Desoi

Inhaltsverzeichnis

Abbildungsverzeichnis.....	XXIII
Abkürzungsverzeichnis	XXV
1 Einführung	1
1.1 Motivation der Arbeit.....	1
1.2 Herangehensweise und Methodik	4
1.3 Gang der Arbeit.....	5
2 Technische und soziale Grundlagen.....	9
2.1 Entwicklung der Datenanalyse und -verarbeitung	10
2.1.1 Entscheidungsunterstützung, Data Mining, Olap.....	11
2.1.2 Big Data	13
2.2 Netzgeschichte – vom Arpanet zum Internet der Dinge	15
2.2.1 Die Entwicklung des Internets.....	15
2.2.2 Ubiquitous Computing und „Smarte“ Umgebungen.....	17
2.3 Web 2.0 oder nutzergenerierte Datenquellen	18
2.3.1 Twitter	18
2.3.2 Youtube	19
2.3.3 Flickr.....	19
2.4 Visual Analytics als Big Data-Analysetechnik	20
2.5 ScatterBlogs.....	23
2.5.1 Technischer Aufbau und Datenfluss	23
2.5.2 Analysepotential des Systems	29
3 Risiken und Chancen.....	31
3.1 Risiken.....	31
3.1.1 Identifizierbarkeit von Personen.....	31
3.1.2 Identifizierbarkeit und öffentliche Kommunikation.....	32
3.1.3 Prognose und virtuelle Sippenhaft.....	33
3.1.4 Rechtsstaatlichkeit, Akzeptabilität und Akzeptanz von Entscheidungen.....	34
3.2 Chancen	35
3.2.1 Statistik „in Echtzeit“	35
3.2.2 Verbessertes Katastrophenmanagement als verbesserter Grundrechtsschutz.....	36

3.2.3	Verminderung von Ausfallrisiken kritischer Infrastrukturen, Effizienzsteigerung und Infrastrukturgewährleistung	37
3.3	Zwischenergebnis	38
4	Das Allgemeine Persönlichkeitsrecht und seine Ausprägungen.....	39
4.1	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	42
4.1.1	Erwartung von Integrität und Vertraulichkeit	42
4.1.2	Kernbereich privater Lebensgestaltung	44
4.1.3	Beeinträchtigung durch Analyseverfahren	44
4.1.4	Ausblick auf künftige Technik	45
4.1.5	Geltung unter Privaten	46
4.1.6	Schranken des IT-Grundrechts	46
4.1.7	Keine Übertragbarkeit bestehender Schranken	48
4.1.8	Schranken zum Einsatz von Analyse-Systemen in der Entscheidungsunterstützung	49
4.1.9	Zwischenergebnis	50
4.2	Informationelle Selbstbestimmung im internationalen Kontext	50
4.2.1	Internationale Übereinkünfte	51
4.2.1.1	OECD Guidelines	51
4.2.1.2	UN Guidelines	52
4.2.1.3	Europäische Menschenrechtskonvention	52
4.2.1.4	Zusammenfassung und Ausblick	53
4.2.2	Datenschutz als europäische Primärrechtsschutz	53
4.2.2.1	Vertrag über die Arbeitsweise der europäischen Union	53
4.2.2.2	Charta der Grundrechte der europäischen Union	54
4.2.2.3	Verhältnis des europäischen Datenschutzgrundrechts zum Recht auf informationelle Selbstbestimmung	55
4.2.3	Zwischenergebnis	57
4.3	Das Recht auf informationelle Selbstbestimmung	58
4.3.1	Zum Begriff des personenbezogenen Datums	61
4.3.2	Prinzipien des Datenschutzes als Anforderungsgrundlagen	62
4.3.2.1	Beschränkte Ermächtigungsgrundlage	63
4.3.2.2	Zweckfestlegung und Zweckbindungsgrundsatz	64
4.3.2.3	Grundsatz der Erforderlichkeit	66

4.3.2.4	Datensparsamkeit	67
4.3.2.5	Grundsatz der Verhältnismäßigkeit.....	69
4.3.2.6	Transparenzgebot	69
4.3.2.7	Datensicherheit.....	71
4.3.2.8	Datenschutzkontrolle.....	72
4.3.2.9	Zwischenergebnis.....	73
4.3.3	Geltung zwischen Privaten.....	73
4.3.4	Eingriff in das Recht auf informationelle Selbstbestimmung	74
4.3.4.1	Maßnahmen der Datenerhebung	76
4.3.4.1.1	Anlassunabhängige Untersuchungen einzelner Quellen und Datensätze	76
4.3.4.1.2	Einwilligung oder Annahme einer „öffentliche Sphäre“?	76
4.3.4.1.3	Genauere Betrachtung der Einwilligungslösung	80
4.3.4.1.4	Einwilligung als Ausübung.....	80
4.3.4.1.5	Keine Vertrauens- oder Sphärenabhängigkeit	81
4.3.4.1.6	Grenzen der Einwilligungslösung und Fallgruppen	82
4.3.4.1.7	Konsequenzen der gewählten Lösung.....	84
4.3.4.2	Datenerhebung und -verarbeitung für Entscheidungsunterstützungssysteme	85
4.3.4.2.1	Eingriffscharakter der Maßnahme	85
4.3.4.2.2	Zwischenergebnis.....	87
4.3.4.2.3	Eingriffsausschluss bei sofortiger Löschung oder Anonymisierung?.....	87
4.3.4.2.4	Ausschlussmöglichkeit von Eingriffen durch „Auslagerung“?.....	90
4.3.4.2.5	Auswirkungen auf die Eingriffsintensität	92
4.3.4.2.6	Indikatoren der Eingriffsintensität	93
4.3.4.2.6.1	Streubreite und Anlass der Maßnahme.....	93
4.3.4.2.6.2	Offenheit der Maßnahme.....	95
4.3.4.2.6.3	Analysetiefe, Sensitivität, Prognose und Entscheidung	96
4.3.4.2.6.4	Anpassungsdruck ohne Personenbezug im Kontext von Big Data-Analysen	98

4.3.4.3	Überwachungsgesamtrechnung.....	99
4.3.5	Zwischenergebnis	100
5	Gleichheitsrechte in der Informationsverarbeitung.....	103
5.1	Die Angst vor Diskriminierung und Hemmung von Verhalten	103
5.2	Schutzbereich: Gleichheitsgebot und Diskriminierungsverbote bei Visual Analytics.....	105
5.2.1	Der allgemeine Gleichheitssatz	105
5.2.2	Die speziellen Gleichheitssätze	107
5.2.3	Wirkung im Krisenmanagement und Katastrophenschutz.....	107
5.2.4	Geltung unter Privaten.....	110
5.2.4.1	Gleichheitsrechtliche Schutzpflichten über Umwege?	111
5.2.4.2	Gleichheitsrechtliche Schutzpflichten und Big Data-Analysen ...	112
5.3	Europäischer Gleichheitsschutz	113
5.4	Verbleib einer Schutzlücke?.....	114
6	Sonstige Grundrechte im Rahmen von Big Data-Analysen.....	117
6.1	Fernmeldegeheimnis	117
6.2	Unverletzlichkeit der Wohnung	120
6.3	Weitere Grundrechte und verfahrensbezogener Grundrechtsschutz.....	121
6.3.1	Grundrechte bei gezielter Massenbeobachtung.....	121
6.3.2	Verfahrensbezogener Grundrechtsschutz und Art. 20 GG	123
6.3.3	Bestehen einer Schutzlücke bei umfassender Betrachtung?	124
6.3.4	Zwischenergebnis	127
7	Information Privacy im US-amerikanischen Recht	129
7.1	Privacy im System des Rechts	129
7.2	Grundlagen der Privacy im geschriebenen Verfassungsrecht.....	130
7.3	Entwicklung des Begriffs Privacy.....	131
7.4	Von Privacy zu „Information Privacy“	132
7.5	Die „Reasonable Expectation of Privacy“	133
7.6	Die “Third Party Doctrine”	134
7.7	Personenbezogene Daten.....	135
7.8	Information Privacy und National Security	136
7.9	Zwischenergebnis.....	137
8	Informationsrechte verarbeitender Stellen	139
8.1	Öffentliche Stellen.....	139

8.1.1	Schutzpflichten	139
8.1.2	Infrastrukturgewährleistung	141
8.1.3	Informationsvorsorge, Steuerung und kurzfristige Reaktion	143
8.1.4	Forschungsfreiheit	144
8.2	Nicht-öffentliche Stellen	144
8.2.1	Informationsfreiheit	145
8.2.1.1	Trennung zwischen Erhebung und Verarbeitung als Kriterium ..	145
8.2.1.2	Fortgeltung der Trennung angesichts technischer Entwicklung ..	146
8.2.2	Weitere Grundrechte.....	148
8.3	Zwischenergebnis.....	148
9	Einfachgesetzliche Zulässigkeit der Datenerhebung und -verarbeitung in Visual Analytics-Systemen im Katastrophenschutz	149
9.1	Gesetzgebungskompetenzen	149
9.2	Europäisches Sekundärrecht	150
9.2.1	Datenschutzrichtlinie	151
9.2.2	Datenschutz-Grundverordnung	152
9.2.3	Richtlinie für Polizei und Justiz	158
9.3	Grundstruktur und Vorgehen im einfachen Datenschutzrecht.....	160
9.4	Das personenbezogene Datum	161
9.4.1	Definition des personenbezogenen Datums	161
9.4.2	Anonymisierung, Pseudonymisierung und Visual Analytics.....	163
9.4.3	Zukunftsbezogene Grauzone?	165
9.5	Einwilligung bei Aufruf zur Äußerung	166
9.6	Der Begriff der „allgemein zugänglichen Daten“	167
9.7	Rechtslage bei öffentlichen Stellen	168
9.7.1	Öffentliche Stellen des Bundes	169
9.7.2	Öffentliche Stellen der Länder	173
9.8	Erlaubnistatbestand für nicht-öffentliche Stellen.....	175
9.8.1	Eigene Geschäftszwecke	175
9.8.2	Berechtigtes Interesse und Abwägung	175
9.9	Kombination mit Energieinformationsdaten und weiteren Daten	177
9.10	Würdigung des geltenden Rechtsrahmens	178

10	Datenschutzrechtliche Zulässigkeit der Analyse allgemein zugänglicher Datenquellen zu Zwecken der Technikforschung.....	181
10.1	Mögliche Arten von Ermächtigungsgrundlagen	181
10.2	Der Begriff der wissenschaftlichen Forschung im Datenschutzrecht	182
10.3	Technikentwicklung als Gegenstand weiterer Grundrechte	184
10.4	Systematik und Bedeutung der forschungsbezogenen Normen	185
10.4.1	Modell des Bundes und der meisten Bundesländer.....	185
10.4.2	Alternative Modelle.....	187
10.4.3	Zwischenergebnis	189
10.5	Mängel der Forschungsprivilegien im Bereich der Technikentwicklung	189
10.6	Europarechtlicher Gestaltungsspielraum.....	191
10.6.1	Forschung in der Datenschutzrichtlinie.....	191
10.6.2	Forschung in der Datenschutz-Grundverordnung	194
10.7	Allgemeine Vorschläge zur Verbesserung des Forschungsdatenschutzes....	196
11	Normative Gestaltung.....	199
11.1	Grundlagen des Katastrophenschutzes und seiner Organisation	199
11.1.1	Katastrophenschutzrecht im Grundgesetz	200
11.1.2	Einfaches Katastrophenschutzrecht der Länder	200
11.1.3	Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	201
11.2	Überlegungen de lege ferenda.....	202
11.3	Rechtsgrundlagen für die Datenverarbeitung am gemeinsamen Melde- und Lagezentrum	203
11.4	Ausgangssituation	203
11.5	Notwendigkeit einer Erweiterung	204
11.6	Ergänzungen zur Datenerhebung und -verarbeitung.....	205
11.7	Ergänzung verarbeitungsspezifischer Vorgaben.....	206
11.8	Ergänzungen zur Transparenzsicherung	209
11.9	Ergänzungen zur Sicherung der Technikentwicklung	210
11.10	Fazit	211
12	Technische Gestaltung.....	213
12.1	Die Methode KORA.....	213
12.2	Verfassungsrechtliche Vorgaben.....	214

12.2.1	Vorgabe 1: Grundrechte, insbesondere allgemeines Persönlichkeitsrecht.....	214
12.2.2	Vorgabe 2: Sozialstaatsprinzip	216
12.2.3	Vorgabe 3: Rechtsstaatsprinzip	217
12.2.4	Vorgabe 4: Katastrophenschutz.....	217
12.3	Anforderungen.....	218
12.3.1	Anforderung 1: Informationelle Selbstbestimmung.....	218
12.3.2	Anforderung 2: Rechtsstaatliche Einzelentscheidung.....	218
12.3.3	Anforderung 3: Nachvollziehbarkeit der Entscheidungsfindung.....	219
12.3.4	Anforderung 4: Menschenwürdige Entscheidung.....	220
12.3.5	Anforderung 5: Sichere Infrastrukturgewährleistung und effektiver Katastrophenschutz.....	220
12.4	Kriterien.....	221
12.4.1	Kriterium 1: Menschliche Entscheidungshoheit	221
12.4.2	Kriterium 2: Sachorientierte Erwägungen.....	222
12.4.3	Kriterium 3: Nichtdiskriminierung.....	222
12.4.4	Kriterium 4: Systemtransparenz.....	223
12.4.5	Kriterium 5: Erforderlichkeit.....	223
12.4.6	Kriterium 6: Datenvermeidung und Datensparsamkeit.....	224
12.4.7	Kriterium 7: Datensicherheit	224
12.4.8	Kriterium 8: Beweistauglichkeit.....	225
12.4.9	Kriterium 9: Zweckbindung	225
12.4.10	Kriterium 10: Effektivität der Entscheidungsfindung.....	226
12.5	Technische Gestaltungsziele	226
12.5.1	Gestaltungsziel 1: Informationsüberblick.....	226
12.5.2	Gestaltungsziel 2: Folgenüberblick	227
12.5.3	Gestaltungsziel 3: Alternativenüberblick	227
12.5.4	Gestaltungsziel 4: Revisionsfähigkeit	228
12.5.5	Gestaltungsziel 5: Zurechenbarkeit	228
12.5.6	Gestaltungsziel 6: Datenvermeidung und frühestmögliche Löschung, Anonymisierung oder Pseudonymisierung.....	229
12.5.7	Gestaltungsziel 7: Vorrang flüchtiger Speicherung von Rohdaten... ..	229
12.5.8	Gestaltungsziel 8: Gestufter Datenzugriff und skalierbare Analyse	230

12.5.9	Gestaltungsziel 9: Neutrale Visualisierung	230
12.5.10	Gestaltungsziel 10: Diskriminierungserkennung	231
12.5.11	Gestaltungsziel 11: Verifizierbarkeit.....	231
12.6	Gestaltungsvorschläge.....	232
12.6.1	Gestaltungsvorschlag 1: Visualisierung mittels Ampelmatrix	232
12.6.2	Gestaltungsvorschlag 2: Stufungsnormierung und Protokollierung	232
12.6.3	Gestaltungsvorschlag 3: Vorrang nicht ID-bezogener Indexierung..	234
12.6.4	Gestaltungsvorschlag 4: Gebietsbezogene Datenerhebung.....	235
12.6.5	Gestaltungsvorschlag 5: Offene Schlagwort Whitelist	235
12.6.6	Gestaltungsvorschlag 6: ID-Hashing.....	236
12.6.7	Gestaltungsvorschlag 7: Zeitstempelung von Rohdaten	236
12.6.8	Gestaltungsvorschlag 8: Aggregatspeicherung	237
12.6.9	Gestaltungsvorschlag 9: Zugriffskontrolle und Zeitstempelung	237
12.6.10	Gestaltungsvorschlag 10: Nutzung aggregierter Energieinformationsdaten.....	238
12.6.11	Gestaltungsvorschlag 11: Homomorphe Verschlüsselung.....	239
12.6.12	Gestaltungsvorschlag 12: Maskierung mit Zufallswerten.....	239
12.6.13	Gestaltungsvorschlag 13: Einbindung von Energieinformationsdaten kritischer Nutzer.....	240
12.6.14	Gestaltungsvorschlag 14: Festlegung von Löschungs- und Anonymisierungsroutinen	240
12.6.15	Gestaltungsvorschlag 15: Informationstrennung bis zur Visualisierung.....	241
12.6.16	Gestaltungsvorschlag 16: Aggregation und Informationsverkürzung	241
12.6.17	Gestaltungsvorschlag 17: Gezielte Informationseinholung	242
12.6.18	Gestaltungsvorschlag 18: Alternative Kontaktmöglichkeit	243
12.6.19	Gestaltungsvorschlag 19: Dokumentation und teilautomatisierte Publikation.....	243
13	Schlussbetrachtung.....	245
	Thesen	249
	Anhänge	251
	Anhang 1) Datenflussmodell Scatterblogs.....	251
	Anhang 2) Scatterblogs-Komponenten	254

Anhang 3) Musterdatensatz im JSON Format	256
Anhang 4) Löschnotiz	260
Anhang 5) Exemplarische Gesetzgebung	261
Literaturverzeichnis	265

Abbildungsverzeichnis

Abbildung 1: Gang der Arbeit.....	8
Abbildung 2: Der Feedback Loop.....	21
Abbildung 3: Der Menschliche Kontext von Visual Analytics	22
Abbildung 4: Tag Map	25
Abbildung 5: Scatterblogs Benutzeroberfläche.....	26
Abbildung 6: Selektorenwerkzeug zur Eingrenzung spezifischer Tweets.	28
Abbildung 7: Selektive Visualisierungen, thematisch zweidimensional.....	28
Abbildung 8: Selektive Visualisierungen, thematisch, raumzeitlich dreidimensional. .	29
Abbildung 9: Systemarchitektur nach Gestaltungsvorschlägen.	251

Abkürzungsverzeichnis

A	rechtliche Anforderung
a.A.	andere Ansicht
a.F.	alte Fassung
ABl. C	Amtsblatt der Europäischen Union beziehungsweise der Europäischen Gemeinschaft, Communications et informations
ABl. L	Amtsblatt der Europäischen Union beziehungsweise der Europäischen Gemeinschaft, Législation
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
API	Application Programming Interface
Art.	Artikel
Aufl.	Auflage
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Bd.	Band / Bände
BDSG	Bundesdatenschutzgesetz
Begr.	Begründer
Beschl.	Beschluss
BGBI.	Bundesgesetzblatt, öffentliches Verkündungsblatt der Bundesrepublik Deutschland
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKR	Bank- und Kapitalmarktrecht
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Inneren
BT-Drs.	Deutscher Bundestag Drucksachen
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidungen
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
BvR	Aktenzeichen einer Verfassungsbeschwerde zum Bundesverfassungsgericht
bzw.	beziehungsweise
c't	Magazin für Computertechnik
Cath. U. L. Rev.	Catholic University Law Review
CR	Computer und Recht
d.h.	das heißt
DB	Datenbank
DIN	Deutsches Institut für Normung
Doc / Dok.	Document / Dokument
DÖV	Die Öffentliche Verwaltung
DSRL	Europäische Datenschutzrichtlinie
DuD	Datenschutz und Datensicherheit

DVBl.	Deutsches Verwaltungsblatt
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
Einf.	Einführung
EMRK	Europäische Menschenrechtskonvention
endg.	Endgültig
ENEL	Ente Nazionale per l'energia Elettrica
et al.	et alii / et aliae
etc.	et cetera
EU	Europäische Union / European Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische GRUNDRECHTE-Zeitschrift
EuR	Europarecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f.	folgende
FASMI	Fast Analysis of Shared Multidimensional Information
ff.	folgenden
Fn.	Fußnote
FS	Festschrift
gen.	genannt
GG	Grundgesetz der Bundesrepublik Deutschland
GMLZ	Gemeinsames Melde- und Lagezentrum
GPS	Global Positioning System
GRCh	Charta der Grundrechte der Europäischen Union
GVBl.	Gesetz- und Verordnungsblatt
h.M.	Herrschende Meinung
HBKG	Hessisches Brand- und Katastrophenschutzgesetz
HDSG	Hessisches Datenschutzgesetz
HGR	Handbuch der Grundrechte
Hrsg.	Herausgeber
HS.	Halbsatz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HStR	Handbuch des Staatsrechts
i.d.F.	in der Form
i.S.d.	im Sinne des
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
ID	Identifizier
IMP	Interface Message Processor
inkl.	Inklusive
IT	Informationstechnik
J.L. & Pol'y	Journal of Law and Policy
Jl	Justiz und Inneres

JSON	JavaScript Object Notation
JZ	Juristen Zeitung
K&R	Kommunikation & Recht
Kap.	Kapitel
KatSG	Katastrophenschutzgesetz
KDD	Knowledge Discovery in Data Bases
Kfz	Kraftfahrzeug
KOM	Europäische Kommission
KRITIS	Kritische Infrastrukturen
LfD	Der Landesbeauftragte für den Datenschutz
lit.	littera, Buchstabe
LSA	Land Sachsen-Anhalt
m.w.N.	mit weiteren Nachweisen
MMR	Multimedia und Recht
MsbG	Messstellenbetriebsgesetz
n.F.	neue Fassung
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
o.Ä.	oder Ähnlichem
OLAP	Online Analytical Processing ()
PIK	Praxis der Informationsverarbeitung und Kommunikation
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
RDV	Recht der Datenverarbeitung
Rn.	Randnummer
Rspr.	Rechtsprechung
S.	Seite
s.	Siehe
St. Rspr.	ständige Rechtsprechung
TCP/IP	Transmission Control Protocol/Internet Protocol
teilw.	Teilweise
TKG	Telekommunikation
u.	Und
u. a.	unter anderem
u.a.	und andere
UCLA J.L. & Tech.	University of California, Los Angeles, Journal of Law and Technology
Urt.	Urteil
USA	United States of America
usw.	und so weiter
V	rechtlicher Gestaltungsvorschlag
v.	Vom
v.	von
VASA	Visual Analytics for Security Applications

VerwArch	Verwaltungsarchiv
vgl.	vergleiche
Vo	rechtliche Vorgabe
Vorb.	Vorbemerkung
VwVfG	Verwaltungsverfahrensgesetz
WI	Wirtschaftsinformatik
Z	rechtliches Gestaltungsziel
z.B.	zum Beispiel
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZRP	Zeitschrift für Recht und Politik