EU-Datenschutzgrundverordnung: Analyse, Auswirkungen und Handlungsempfehlungen

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Petersen Vorname: Jan

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Langenhagen, den 10.08.2018

Inhaltsverzeichnis

1. Einleitung

Der Begriff *Digitalisierung* ist in Mode. Mertens et al. (2017: XI) sprechen schon von einer „inflationären Verwendung des Wortes ‚digital'". Es finden derzeit Prozesse tiefgreifenden Wandels in Wirtschaft und Gesellschaft statt. Smartphones sind als digitale Alltagshelfer kaum noch wegzudenken, Smart Health digitalisiert unsere Gesundheit, die Verlagerung von Speicherplatz, Rechenleistung und Anwendungen in die Cloud wird immer beliebter (Forbes, 2017) und Unternehmen entdecken neue Wertschöpfungspotenziale durch digitale Geschäftsmodelle. Diese „digitale Liste" lässt sich beliebig fortführen und obwohl die öffentliche Diskussion um Digitalisierung von derartigen Trends bestimmt wird, ist die treibende Kraft der Digitalisierung viel grundlegender und historischer: *Daten*. Ohne Daten ist Digitalisierung nicht möglich. Die International Data Corporation (IDC) schätzt, dass bis zum Jahr 2025 163 Zettabyte an Daten produziert werden (Reinsel et al., 2017: 5). Das entspricht einer Billion Gigabyte und einer Verzehnfachung der im Jahr 2016 produzierten Daten. Die Entwicklung dieser nahezu ungreifbaren Zahl ist auf den Punkt gebracht jedoch einfach zu erklären. Mobile Endgeräte und mobiles Internet machen Daten ubiquitär verfügbar. Werden zusätzlich noch Gegenstände wie Kühlschrank, Armbanduhr oder Auto im *Internet der Dinge* vernetzt, vervielfacht sich die Menge der Datenquellen und produzierten Daten. Nach Angaben von Gartner Inc. (van der Meulen, 2017) sind bis zum Jahr 2020 annähernd 20,4 Milliarden vernetzte Geräte in Gebrauch.

Die Entwicklung der Datenmengen ist insbesondere dann kritisch zu betrachten, wenn *personenbezogene Daten* durch den Umgang mit Informationstechnik entstehen, erhoben, verarbeitet, übertragen und genutzt werden. An dieser Stelle rückt der Datenschutz und die Frage nach seiner Wirksamkeit in einer zunehmend digitalisierten Welt in den Fokus der Betrachtung. Der Datenschutz soll den Schutz personenbezogener Daten des Einzelnen gewährleisten und gilt in der Europäischen Union (EU) als Grundrechtsschutz. Mit der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, die am 25.05.2018 die Datenschutzrichtlinie (DSRL) aus dem Jahr 1995 ersetze, soll das europäische Datenschutzrecht unionsweit harmonisiert und in Hinblick auf die Herausforderungen der Digitalisierung umfassend modernisiert werden, um Grundrechte und Grundfreiheiten des Einzelnen zu schützen und den freien Datenverkehr im Binnenraum zu fördern.

Digitalisierung ist begrifflich jedoch sehr weit gefasst und wird in der Praxis häufig nicht einheitlich verwendet. Der Begriff impliziert keine spezifische Technologie, anhand derer die Herausforderungen belegt und untersucht werden könnten. Martini (2016: 25) führt hierzu aus, dass „es sich bei der Digitalisierung um keinen konsistenten und in sich abgeschlossenen Forschungsgegenstand [handelt], der sich mit einer detailscharfen Forschungsfrage umreißen ließe – vielmehr setzt sie nahezu alle Lebensbereiche einem umfassenden Umbruchsprozess aus, der

Ausstrahlungen in nahezu alle Wissenschaftsdisziplinen zeitigt“. Die oben bereits beschriebene Datengetriebenheit der Digitalisierung soll hier im Mittelpunkt der Untersuchung stehen. Wenn Daten, insbesondere personenbezogene Daten, als Funktionsbedingung der Digitalisierung verstanden werden, dann ist Big Data eine Schlüsseltechnologie und ein geeigneter Forschungsgegenstand, der den Begriff Digitalisierung exemplarisch und angemessen eingrenzt.

Die automatisierte und auf Algorithmen basierte Auswertung von stetig wachsenden Datenmengen mit Big Data Analyseverfahren bietet zahlreiche Chancen, stellt den Datenschutz jedoch auch vor gleichsam wachsenden Herausforderungen. Die Vielfältigkeit der Datenquellen und die Zusammenführung heterogener Daten zu ganzen Persönlichkeitsprofilen oder Verhaltensprognosen gefährdet das Grundrecht auf Schutz personenbezogener Daten nach Artikel 8 der Grundrechtecharta (GRCh). Big Data Analysen erlauben in Verbindung mit großen und ubiquitären Datenmengen „erhebliche Rückschlüsse auf das Leben des Einzelnen, seine finanziellen Verhältnisse, sein Konsumverhalten sowie seine Vorlieben und Interessen“ (Katko und Babaei-Beigi, 2014: 361). Derartige Rückschlüsse eröffnen zudem neue Wege der Verhaltensteuerung von Individuen. Kaufimpulse können gezielt gesetzt und Meinungsbildung im Wahlkampf beeinflusst werden (Richter, 2016: 581). Die Nutzer digitaler Technologien sind selbst auch ein treibender Faktor dieser Entwicklung. Sie geben quid pro quo freiwillig ihre Daten Preis, um bestimmte digitale Dienste scheinbar kostenfrei in Anspruch zu nehmen (Bottis und Bouchagiar, 2018: 193; Kugelmann, 2016: 566; Roßnagel, 2016: 562). Damit wird das personenbezogene Datum zum Zahlungsmittel und der „kostenfreie“ Dienst die Gegenleistung. Das Bedrohungspotential von Big Data steigt dabei mit der Menge der erzeugten Daten im Zeitablauf. Die steigende Verfügbarkeit der Datenmengen erleichtert die De-Anonymisierung von anonymen Daten, sodass potenziell jedes Datum personenbezogen sein kann.

Mit den Herausforderungen von Big Data steigen auch die Anforderungen an das Datenschutzrecht. Es stellt sich also die Frage, inwiefern die Datenschutz-Grundverordnung den Anforderungen gerecht wird. Folgende Forschungsfragen sollen die Arbeit leiten, um Änderungen und Auswirkungen der DSGVO hinsichtlich Big Data Technologien zu untersuchen:

A) *Inwiefern ändert sich mit der Datenschutz-Grundverordnung die Anwendung der Datenschutzgrundsätze auf Big Data Technologien?*

B) *Welche allgemeinen Regelungen der DSGVO lassen sich auf Big Data Technologien anwenden?*

C) *Werden die Herausforderungen von Big Data Technologien mit der Datenschutz-Grundverordnung insgesamt sinnvoll adressiert?*

Die Datenschutzgrundsätze sind in der DSGVO auch weiterhin das konzeptionelle Fundament des europäischen Datenschutzrechts. Aus diesem Grund soll untersucht werden, ob und inwiefern sich einzelne Grundsätze inhaltlich ändern und welche Auswirkungen sich daraus für Big Data Technologien ergeben. Daran anknüpfend werden ausgewählte Vorschriften der DSGVO untersucht, die sich auf Big Data Technologien anwenden lassen. Zur Beantwortung der Forschungsfragen wird eine ausführliche Literaturanalyse durchgeführt. Kapitel 2 stellt entsprechend einen wichtigen Bestandteil dieser Arbeit dar. Hier werden zunächst die zur Literaturanalyse verwendeten Konzepte, die inhaltliche Erschließung des Forschungsthemas und die Literatursuche detailliert beschrieben. Abschließend wird die Literaturauswertung anhand einer entwickelten Konzeptmatrix erläutert. Die Konzeptmatrix fasst die Ergebnisse der Literaturanalyse übersichtlich zusammen und ist Ausgangspunkt für die Diskussion in Kapitel 4.

Diese Arbeit schafft einen wissenschaftlichen Mehrwert, indem die thematisch verteilten Forschungen in der Literatur zu einer abschließenden Bewertung von Auswirkungen und Wirksamkeit der Datenschutz-Grundverordnung im Kontext von Big Data Technologien integriert und darauf aufbauend Forschungslücken in Kapitel 5 aufgezeigt werden. Ein Großteil der relevanten Publikationen identifiziert und kritisiert spezifische Probleme der DSGVO ohne inhaltlich konkrete Lösungsansätze zu formulieren. Aus diesem Grund werden Vorschläge zur datenschutzrechtlichen Bewältigung von Big Data Technologien in Kapitel 6 gemacht.

7. Fazit

Mit der Datenschutz-Grundverordnung soll der europäische Datenschutz eine gestärkte Position in Zeiten der Digitalisierung einnehmen, indem unter anderem datenschutzrechtliche Vorschriften umfassend harmonisiert und modernisiert werden. Eine besondere Gefahr geht von Big Data Anwendungen aus. Big Data Anwendungen gelten als wenig vereinbar mit den Datenschutzgrundsätzen des europäischen Datenschutzrechts. Die datenschutzrechtliche Technikneutralität gibt dem europäischen Gesetzgeber nur begrenzen Handlungsraum, um risikoadäquate Regelungen zu erlassen. Zwei schwerwiegende Herausforderungen von Big Data sind zum einen die technischen Möglichkeiten der De-Anonymisierung und Re-Identifikation anonymer Daten und zum anderen die Generierung personenbeziehbaren Wissens aus anonymen Datenbeständen bzw. Statistiken. Es stellt sich die Frage, ob Probleme und Herausforderungen von Big Data insgesamt sinnvoll mit der Verordnung adressiert werden.

Der europäische Gesetzgeber hält auch mit der Datenschutz-Grundverordnung konzeptionell an den etablierten Datenschutzgrundsätzen fest. Das ist angesichts der Herausforderungen von Digitalisierung im Allgemeinen und Big Data im Speziellen auch erforderlich. Insofern gilt für Big Data Anwendungen weiterhin ein grundsätzliches Vereinbarkeitsproblem mit den Grundsätzen des Datenschutzes. Der hybride Charakter der Verordnung führt derzeit noch zu offenen Fragen. Auslegungsentscheidungen zu abstrakten Regelungen liegen häufig im Verantwortungsbereich von verantwortlichen Stellen, deren Zulässigkeit die Rechtsprechung im Nachgang klären muss. Damit hängen Wirksamkeit und Erfolg der Verordnung auch wesentlich von mitgliedsstaatlichen Regelungsbefugnissen, Auslegungsentscheidungen der Verantwortlichen und Rechtsprechung ab. Unter dem unberührten Prinzip der Technikneutralität werden viele Regelungen aus der Datenschutzrichtlinie übernommen unter teils und neuem Namen inhaltlich ausgearbeitet. Die rechtliche Integration des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Technikeinstellungen sowie der Datenschutz-Folgenabschätzung machen den Datenschutz zu einer Aufgabe *ex ante* im Sinne eines risikobasierten Ansatzes, der die Datenverarbeiter in die Verantwortung zieht und Big Data Anwendungen risikoorientiert reguliert. Die drastisch erhöhten Geldbußen für Verstöße gegen die Vorschriften tragen zu einer allgemeinen Sensibilisierung der Verantwortlichen im Umgang mit personenbezogenen Daten, insbesondere mit Big Data Analysenverfahren, bei.

Insgesamt macht der europäische Gesetzgeber mit der DSGVO deutliche Fortschritte. Einzelne Regelungen tragen zu einer Stärkung des Schutzes personenbezogener Daten und damit zu einer Modernisierung des Datenschutzrechts bei. Die anreizbasierte Pseudonymisierung stellt einen Ansatz dar, der Unternehmen dazu bewegen könnte, personenbezogene Daten konsequenter zu De-Identifizieren. Hier sollten zeitnah konkrete Maßnahmen zur praktikablen Umsetzung

und Integration entwickelt werden, um den Ansatz für Unternehmen attraktiv zu halten. Die Generierung von personenbeziehbarem Wissen aus anonymen Statistiken bleibt vom Gesetzgeber jedoch kategorisch unbeachtet und stellt weiterhin eine große Herausforderung dar. Auch die Fachliteratur stellt bislang keine ausreichend konkreten Lösungen vor.

Basierend auf eigenen Erkenntnissen wurde eine Strategie vorgestellt, mit der anonyme Datenbestände indirekt über eine Datenschutz-Folgenabschätzung vom sachlichen Anwendungsbereich erfasst werden können. Darüber hinaus wurden mit der simultanen Informationspflicht für Verantwortliche und der Komplexitätsreduktion des Transparenzgrundsatzes allgemeine Vorschläge zur Gestaltung des Datenschutzrechts gemacht. Abschließend richtete sich ein Appell an die Nutzer digitaler Technologien. Die datenschutzrechtliche Selbstkontrolle ist in Zeiten von Digitalisierung und Big Data Analysen wichtiger denn je. Nicht nur zum Schutz der eigenen Rechte und Freiheiten, sondern auch zu Vermeidung externe Effekte, die das Risiko für den Einzelnen kollektivieren.