Smart Data

Smart Data – Smart Solutions

Fachgruppe Rechtsrahmen

Impressum

Herausgeber
Smart-Data-Begleitforschung
FZI Forschungszentrum Informatik
Außenstelle Berlin
Friedrichstr. 60, 10117 Berlin
www.smart-data-programm.de

Redaktion und Konzeption
Fachgruppe Rechtsrahmen der Smart-Data-Begleitforschung

Schlussredaktion und Gestaltung
LoeschHundLiepold Kommunikation GmbH

Stand
Mai 2018

Druck
WIRmachenDRUCK, Backnang

Bildnachweis
pickup – Fotolia.com (Titel)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Vorwort

Im Technologieprogramm „Smart Data – Innovationen aus Daten“ fördert das Bundesministerium für Wirtschaft und Energie 16 Leuchtturmprojekte, deren Erkenntnisse in diese Ergebnisbroschüre eingeflossen sind. Neben den relevanten Rechtsfragen aus den Einzelprojekten finden Sie im vorliegenden Bericht übergeordnete Themen, die im Laufe des Programms eine zentrale Rolle eingenommen haben.

Der dem Technologieprogramm zugrunde liegende Begriff „Smart Data“ lässt sich als Weiterentwicklung und Präzisierung von Big Data verstehen.[1] Während bei Big Data die Phänomene Volume, Variety und Velocity im Vordergrund stehen, konzentriert sich Smart Data auf die intelligente Analyse. Nicht unbedingt die Masse (Big), sondern die Gewinnung wertvoller Inhalte (Smart) steht hierbei im Vordergrund.[2] Ein provokativer Slogan wäre “Big Data is the problem and Smart Data is the solution.”[3] In einem Big Data Memorandum brachten es Wissenschaftler auf die griffige Formel: “Smart Data = Big Data + Nutzen + Semantik + Datenqualität + Sicherheit + Datenschutz“.[4] Dies ist insoweit interessant, als auch rechtliche Aspekte in diese Begriffsdefinition einbezogen wurden. Somit würde Smart Data nicht zur bloßen Wortneuschöpfung, sondern eine tatsächliche Neuausrichtung bedeuten. „Smart“ ist eine effektive Auswertung von Datenbeständen und führt zur Generierung neuer „wertvoller Inhalte“. Diese Inhalte können aber nur dann auch aus gesellschaftlicher Perspektive „wertvoll“ sein, wenn ihre Erhebung, Zusammenstellung, Auswertung und Nutzung mit rechtlichen Regularien im Einklang steht, wozu insbesondere das Datenschutzrecht zählt.[5] Ein wichtiger Schritt auf dem Weg von Big zu Smart Data liegt somit darin, Lösungsansätze zu finden, die die rechtlichen Herausforderungen von Big Data adressieren.

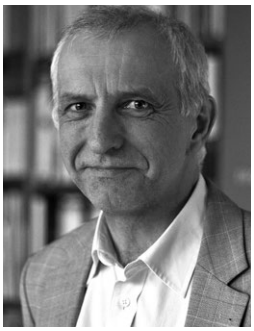
Aufgrund der neuen Datenschutz-Grundverordnung sowie der notwendigen Anpassungen des deutschen Rechtsrahmens auf Bundes- und Landesebene befindet sich das Datenschutzrecht derzeit noch in einer Umbruchsphase. Intensive interdisziplinäre Forschung kann dennoch die Ziele der Datenauswertung und des Datenschutzes durch eine datenschutzfreundliche Technikgestaltung in Einklang bringen.[6] Diese Erkenntnis kann nach den Ergebnissen der Begleitforschung nun als gesichert gelten.

Dies zeigt nicht zuletzt der Gastbeitrag von Dr. Thilo Weichert, der über die Laufzeit der Projekte eine konstruktiv-kritische Begleitung geleistet hat. Anschließend zeigen konkretisierend die Projekte SD-KAMA und SMARTREGIO wie sie sich erfolgreich den Herausforderungen gestellt und innovative Lösungen gefunden haben. Im Anschluss geben wir einen Überblick über typische Rechtsfragen exemplarischer Smart-Data-Fallkonstellationen mit Projekt-Kurzportraits von „Smart Solutions“. Diese Beispiele können zukünftig jungen Unternehmungen als Referenz dienen, wie sich die vermeintlichen Widersprüche von Datenschutz und Smart Data rechtskonform lösen lassen.

PD Dr. Oliver Raabe und Manuela Wagner
Begleitforschung des Technologieprogramms
„Smart Data – Innovation aus Daten“

Smart Data und der Datenschutz

Dr. Thilo Weichert, Netzwerk Datenschutzexpertise



Meine Forschungs- und Publikationsarbeiten innerhalb des Smart-Data-Projekt-Kontextes – wie auch darüber hinausgehend – beschäftigen sich mit der Frage, welcher Regulierung konkrete Big-Data-Anwendungen bedürfen. Waren die ersten Jahre der rechtlichen Diskussion von Grundsatzfragen bestimmt, etwa die Rolle von Datensparsamkeit, Anonymisierung, Zweckbindung und Betroffeneneinwilligung bei Smart Data, so steht nun die Frage im Vordergrund, wie trotz des strukturellen Konfliktes zwischen Big Data und dem Grundrecht auf Datenschutz in konkreten Anwendungsfeldern Analytics umfassend genutzt werden kann, ohne dass dabei der digitale Grundrechtsschutz aufgegeben wird.

Konkrete Fragestellungen, mit denen ich mich befasse, sind Smart Data im Medizinbereich generell wie speziell in der medizinischen Forschung, in den Bereichen des Konsumverhaltens und von Beschäftigungsverhältnissen, bei der Umsetzung des automatisierten und autonomen Fahrens im Straßenverkehr oder zur Bewältigung der Herausforderungen bei der IT-Sicherheit.

Die grundlegende Herausforderung besteht darin, die allgemeinen Regeln der Europäischen Datenschutz-Grundverordnung (DS-GVO), insbesondere deren Regelung zum Profiling und zu automatisierten Entscheidungen in Art. 22 auf konkrete Anwendungen herunterzubrechen. Dabei geht es nicht nur um sog. Use Cases und für diese nötigen rechtlichen Rahmenbedingungen, z. B. die Formulierung von Einwilligungstexten und die Gestaltung von Transparenz- und Optionsverfahren, die Wahl des besten Verarbeitungskonzeptes und der richtigen Pseudonymisierungs- und Auswertungsstrategien. Es geht auch um die Erarbeitung von spezifischen und zugleich abstrakten rechtlichen, prozeduralen sowie technisch-organisatorischen Rahmenbedingungen, die sich zwischen den Vorgaben der DS-GVO und den Use Cases bewegen.

Dabei stellen sich teilweise Fragen, auf welche die bisherige Rechtsordnung noch keine Antworten gefunden hat, etwa die Frage nach der Bewertung von Sensorik, die in den Kernbereich privater Lebensgestaltung eingreift, indem sie Gedanken, Gefühle und Stimmungen erfasst, speichert und auswertet, oder die des Einsatzes von sog. künstlicher Intelligenz. Für die Schnittstellen zwischen Computer und Mensch, die mit Biotechnologie und Robotik immer wieder neue Ausgestaltungen erfahren, müssen anwendungsspezifische Anforderungen definiert, umgesetzt, erprobt und normiert werden. Dabei muss beachtet werden, dass in jedem Bereich, ja oft bei jeder Anwendung eine sich unterscheidende Antwort gefunden werden kann und evtl. muss. Es gilt bei Smart Data kein „One fits all“. Gerade dies macht das Thema so spannend, voraussetzungsvoll und interdisziplinär.

Lösungen sind in jedem Fall ein – unterschiedlicher – Mix von materiell-rechtlichen, prozeduralen sowie technisch-organisatorischen Vorkehrungen, die ihrer-

seits einer normativen Grundlage bedürfen. Wichtige prozedurale Maßnahmen sind Zertifizierungen sowie regelmäßige Evaluationen bzw. unabhängige Audits. Bei der Festlegung dieses Mixes gibt es wiederum keine allgemeingültigen Antworten, außer vielleicht der, dass der klassische Gesetzgeber mit der Bewältigung der Aufgabe der Normierung praktisch durchgängig überfordert ist. Diese Erkenntnis darf aber nicht dazu führen, dass hinsichtlich der demokratischen Legitimation der Lösungen Abstriche gemacht werden. Dies lässt sich durch eine maximale Transparenz sowie die Einbindung von mehr oder weniger demokratisch legitimierten Fachgremien, etwa Aufsichtsbehörden, Beiräten, Ethikkommissionen oder Fachbeauftragten, einlösen. Das normative Instrument ist die regulierte Selbstregulierung, wobei in jedem Fall darauf geachtet werden muss, dass sämtliche Rollen bzw. Stakeholder angemessen berücksichtigt werden.

Voraussetzung jeder regulierten Selbstregulierung ist die demokratisch legitimierte Regulierung, also die normative Vorgabe durch den Gesetzgeber. Anstelle der bisher angestrebten Vollregulierung muss er sich aber beschränken auf die Vorgabe von Zwecken und Zielen sowie die Festlegung verbindlicher Verfahren zur Aushandlung der materiellen oder auch technischen Vorgaben. Ein Beispiel hierfür ist unser Vorschlag eines Bund-Länder-Staatsvertrags für die Medizinforschung, über den primäre Behandlungsdaten für sekundäre Forschungszwecke zur Verfügung gestellt werden, nachdem hierüber fachnahe und öffentlich bzw. transparent agierende unabhängige Use-and-Access-Committees (UACs) entschieden haben.[7]

Generell gilt, dass Geheimhaltungsregelungen zurückgefahren und Open-Data-Anforderungen – auch im Bereich der privaten Wirtschaft – gesetzlich normiert werden müssen. Der Grund hierfür ist so trivial wie einleuchtend: Entwickelt Smart Data eine gesellschaftliche Relevanz, so muss die Anwendung von Smart Data – egal ob von privaten oder öffentlichen Stellen exekutiert – gesellschaftlich mitbestimmt und kontrolliert werden können. Dem stehen immaterielle Ausschließlichkeitsrechte, wie sie aktuell immer wieder im Interesse einer Ökonomisierung der Digitalisierung erörtert werden, entgegen. Letztlich profitiert die Gesamtwirtschaft vom adäquaten Teilen und von zumindest teilweise staatlich zu finanzierenden Regulierungsstrukturen. Anreize zur Monopolisierung durch Deregulierung, wie sie in den USA und in Ostasien bestehen, zerstören ein plurales Marktgeschehen, behindern Kreativität und verhindern Gemeinsinn.

Die wichtigste Lektion ist die, dass es keine Patentlösungen und keine letzten Antworten gibt. Smart Data ist ein technischer, gesellschaftlicher und damit letztlich auch ein demokratischer und rechtlicher Prozess, der sich nicht nur immer weiterentwickelt, sondern der auch immer wieder vor Wegkreuzungen führt, an denen neue öffentlich diskutierte demokratische Entscheidungen getroffen werden müssen. Es ist nicht übertrieben zu behaupten, dass wir vor der grundsätzlichen Frage stehen, ob wir unsere globale Informationsgesellschaft demokratisch und freiheitlich gestalten oder ob wir deren Abgleiten ins Totalitäre weiter hinnehmen wollen.

Smart Solutions für Smart Data: Rechtliche Herausforderungen typischer Fallkonstellationen und Vorbilder erfolgreicher interdisziplinärer Forschung

Wissenschaftliche Arbeiten zu Big Data konzentrieren sich meist auf die Phänomene Volume, Variety und Velocity.[8] Aus rechtlicher Sicht besonders relevant sind jedoch auch Datenquellen und Datenqualität sowie Verwendungszwecke und -kontexte. Somit können sich typisierbare Herausforderungen in verschiedenen Bereichen unter verschiedensten rechtlichen Aspekten stellen. Einige möchten wir exemplarisch herausgreifen und für den zukünftigen Smart-Data-Anwender verständlich aufbereiten.

Weitere Bereiche mit typisierbaren Fallkonstellationen werden im Anschluss präsentiert. Hierzu gehören u. a. unter dem Stichwort „Smart Industry“ die unternehmensübergreifende Verwendung von industriellen Daten aus Maschinensensoren wie es im Kontext von Industrie 4.0 häufig anzutreffen ist. Innovationen einiger Smart Data Projekte, wie beispielsweise iTesa, basieren auf der Verwendung von Daten aus öffentlich zugänglichen Quellen (Fallgruppe „Smart Public Data“). Rechtliche Besonderheiten sind zudem im Mobilitätssektor (Fallgruppe „Smart Mobility“), bei Videoaufnahmen im öffentlichen Verkehrsraum (Fallgruppe „Smart Video Analysis“), im Bereich der medizinischen Forschung (Fallgruppe „Smart Health“) oder bei der Energieoptimierung (Fallgruppe „Smart Energy“) anzutreffen. Das folgende Schaubild soll zeigen welche Smart-Data-Projekte welchen sich teils überschneidenden Fallgruppen zugeordnet werden können. In den folgenden Abschnitten werden für diese Fallkonstellationen interessante Rechtsfragen aus unterschiedlichen Rechtsgebieten wie dem Datenschutz-, Urheber-, Straf- und Wettbewerbsrecht vorgestellt. Diese sind natürlich weder abschließend noch zwingend und können ebenso in anderen Konstellationen auftreten. Es soll dem Leser ein erfassbarer Überblick über die Komplexität der Rechtslage anhand typischer Fallkonstellationen gegeben werden.

Im Anschluss sollen kleine Kurzportraits einen Eindruck geben, wie sich einzelne Forschungsprojekte rechtlichen Herausforderungen gestellt haben.

Fallgruppen und Smart Data Projekte

Smart Health

InnOPlan: Innovative, datengetriebene Effizienz OP-übergreifender Prozesslandschaften

KDI: Klinische Datenintelligenz

SAHRA: Smart Analysis – Health Research

FAST Genomics – Fast Analysis of Single Cell Transcriptomics

Smart Industry

SAKE: Semantische Analyse komplexer Ereignisse

PRO-OPT: Big-Data-Produktionsoptimierung in Smart Ecosystems

SIDAP: Skalierbares Intergrationskonzept zur Datenaggregation, -analyse, -aufbereitung von großen Datenmengen in der Prozessindustrie

Smart Mobility

ExCELL: Echtzeitanalyse und Crowdsourcing für eine selbstorganisierte City-Logistik

Smart Video Analysis

VIRTUOSE-DE: Service-Plattform für echtzeitfähige Big-Data-Videoanalyse und -verarbeitung in der Cloud

Smart Public Data

Smart Data Web: Datenwertschöpfungsketten für industrielle Anwendungen

iTesa: intelligent Traveller Early Situation Awarness

SD4M: Smart Data for Mobility

Smart Energy

Smart Energy Hub: Datendrehscheibe für intelligente Energienutzung

Smart City

SmartRegio: Trend-Analysen auf der Basis heterogener Massendaten

sd-kama: Smart-Data-Katastrophenmanagement

Smartes Datenmanagement

EDV: Einfaches Digitales Vergessen

1 Smart City

Nicht nur für Unternehmen und Forschungseinrichtungen, sondern auch für Behörden steigt die Bedeutung von Smart Data für die Durchführung ihrer öffentlichen Aufgaben. Das Projekt sd-kama ist ein sehr gutes Beispiel, wie Behörden Katastrophen dank aussagekräftiger Echtzeitinformationen effektiv managen können und gleichzeitig den rechtlichen Compliance-Anforderungen umfassend Rechnung getragen werden kann. Im Projekt SmartRegio sollen dagegen Trends für die Stadtentwicklung genutzt werden, um die regionale Planung und Entwicklung zu fördern.

Das Projekt sd-kama: Smart-Data-Katastrophenmanagement

Ziel

Bei Naturkatastrophen wie Überschwemmungen oder Hochwasser gibt es zumeist nur wenige oder unsichere Informationen über die aktuelle Lage vor Ort. Dabei sind verlässliche Daten zum Ausmaß und zur Intensität der Katastrophe, etwa zur Anzahl der bedrohten Personen, zum Zustand von Gebäuden oder Infrastrukturen essenziell, damit Krisenmanager und Rettungskräfte schnell und gezielt reagieren können.

Das Projekt sd-kama entwickelt daher ein echtzeitfähiges System, das die relevanten Informationen aus unterschiedlichen Datenströmen sammelt und analysiert. Dafür werden bereits vorliegende Daten zusammengeführt und durch Echtzeitinformationen ergänzt, wie beispielsweise Informationen aus Satellitenbildern oder Bild- und Videoaufnahmen, die von freiwilligen Helfern oder Einsatzkräften mittels einer im Rahmen des Projektes entwickelten App übermittelt werden.

Zudem werden mithilfe von Wearables und der App körperliche Messwerte von Einsatzkräften und Helfern übermittelt, sodass Überlastungen rechtzeitig erkannt und Unterstützung bzw. eine Ablösung schneller organisiert werden können. Hinzu kommen Pegelstände und Wetterinformationen aus Diensten von Behörden. Moderne Plattformen für Echtzeitverkehrsdaten, zum Beispiel Navigationsprogramme wie HERE Maps, liefern darüber hinaus Informationen und Dienste für die Erreichbarkeit von Einsatzorten.

Durch die Verfügbarkeit dieser Fülle an Informationen entsteht ein umfassendes Bild von der Lage, wodurch die Einsatzzentren Ressourcen und Einsatzkräfte effizienter koordinieren, Gefahren besser einschätzen und fundierte Entscheidungen treffen können. sd-kama ermöglicht damit ein zielgerichtetes, effektives Katastrophenmanagement mit bedarfsgerechtem Ressourceneinsatz.

Herausforderungen

Eine große Herausforderung bestand darin, die Dienste durch eine rechtssichere Gestaltung attraktiv für Nutzer und Institutionen zu machen, die großen Wert auf Datenschutz legen.

Insbesondere die im Projekt entwickelten Applikationen zur Datengewinnung (physiologische Daten zur Überlastungsdetektion sowie Fotos und Videoclips) bedurften einer eingehenden datenschutzrechtlichen Betrachtung, während die meisten anderen Datenquellen (Verkehr, Wetter, Pegelstände) öffentlich zugänglich waren und keinen Personenbezug aufwiesen.

Bei den Löschfristen bedurfte es einer sorgfältigen Abwägung zwischen den schutzwürdigen Interessen Betroffener, die einer Speicherung über den Zeitraum zur Erreichung des eigentlichen Zwecks hinaus entgegenstehen, und der notwendigen Vorhaltung über einen längeren Zeitraum aufgrund einer Beweissicherungspflicht der Behörde mit Blick auf mögliche Schadensersatzansprüche von Geschädigten.

Lösung

Es wurde eine Datenschutzkonzeption erstellt, die sicherstellt, dass die Erarbeitungen im Rahmen des Projekts sd-kama einerseits dem Recht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und dem Datenschutzgrundrecht des Art. 8 EU-Grundrechte-Charta genügen und sich andererseits in der Praxis nutzer- und bedienfreundlich sowie dem Stand der Technik entsprechend und unter Berücksichtigung der Implementierungskosten ein- und umsetzen lassen.

In der Datenschutzkonzeption wurde zunächst der Schutzbedarf der in sd-kama verwendeten Daten ermittelt. Im Folgenden konnten wir uns dann ausschließlich auf die Betrachtung der schutzbedürftigen Daten fokussieren, wobei zunächst detailliert die Datenverarbeitung, von der Datenerhebung über die Datenweitergabe, -auswertung und -speicherung bis zur Datenlöschung betrachtet wurde. Daran schloss sich die rechtliche Prüfung der Zulässigkeit der Datenverarbeitung und die Beschreibung daraus resultierender technischer und organisatorischer Maßnahmen an. Ein Anhang mit Umsetzungs-Checklisten rundet das Dokument ab.

Berücksichtigung fand hierbei auch die im Mai 2018 gültig werdende europäische Datenschutz-Grundverordnung, die zu einem Datenschutz durch Technikgestaltung (Privacy-by-Design) verpflichtet. So werden ausschließlich Daten verarbeitet, die für den ausgewiesenen Zweck erforderlich sind. Sobald Daten nach Abschluss eines Verarbeitungsschrittes nicht mehr erforderlich sind, werden diese gelöscht. Beispiel: Zur Überlastungsdetektion werden verschiedene physiologische Daten der Einsatzkräfte erfasst, die mittels eines Algorithmus ausge wertet werden. Das Ergebnis dieser Auswertung (Überlastungswert plus Zeitpunkt und Ortskoordinaten) wird im Falle einer Grenzwertüberschreitung (= Überlastung wurde erkannt) gespeichert, die Rohdaten werden sofort nach der Auswertung vernichtet.

Bei der für den Upload von Fotos und Videoclips entwickelten App geschieht die Nutzung per Default anonym. Vor dem ersten Upload wird dem Anwender in leicht verständlicher Form geschildert, welche Daten zu welchem Zweck erhoben und verarbeitet werden. Der Nutzer erhält über Zusatzoptionen Anreize, sich zu registrieren, was auch mit Pseudonym möglich ist. Bei den die App nutzenden Einsatzkräften wird eine Registrierung vorausgesetzt.

Die App zur Erfassung physiologischer Daten zur Überlastungsdetektion kommt ausschließlich bei Einsatzkräften auf freiwilliger Basis nach vorheriger ausdrücklicher Einwilligung zum Einsatz.

Das sd-kama EUS (Entscheidungs- und Unterstützungssystem) ist nur einem begrenzten, autorisierten Personenkreis nach Anmeldung zugänglich, namentlich den Mitgliedern der Einsatzleitstelle/des Katastrophenstabes. Ein Rollenkonzept stellt sicher, dass jeder Nutzer nur die für ihn relevanten Daten einsehen kann.

Grundlage der technischen Maßnahmen sind die IT-Grundschutzkataloge des BSI, deren relevante Bausteine im Anhang der erstellten Datenschutzkonzeption aufgeführt sind. Jeder über öffentliche Kommunikationswege (Internet, WLAN, …) führende Datentransfer erfolgt transportverschlüsselt, öffentlich zugängliche Schnittstellen sind zugangsgeschützt. Die Server werden hinter einer Firewall betrieben, nur tatsächlich benötigte Protokolle und Ports sind freigeschaltet. Bei der Auswahl des externen Serverproviders wurde darauf geachtet, dass er seinen Firmensitz in Deutschland hat und an deutsches beziehungsweise europäisches Datenschutzrecht gebunden ist. Hochgeladene Fotos werden einer automatisierten Gesichtserkennung und -verpixelung unterworfen.

Empfehlungen

Im Bereich des Datenschutzes bleibt auch nach der Einführung der Datenschutzgrundverordnung eine entscheidende Frage, wem die Entscheidung über die Verwertung, d. h. die wirtschaftliche Nutzung von Daten, zufallen soll: Kann der Einzelne im Sinne des Rechts auf informationelle Selbstbestimmung aktiv über die Nutzung seiner Daten bestimmen oder muss er im Sinne eines überwiegenden Schutzrechts vor dem Eingriff Dritter geschützt werden? Die Hoheit über den persönlichen Gehalt der Daten erfordert wie beim Urheberrecht das Verbleiben eines höchstpersönlichen, unveräußerlichen Kerngehaltes beim Dateninhaber. Dieser Kerngehalt beinhaltet die Umkehrbarkeit bestimmter Entscheidungen zur Nutzung der Daten (Reversibilität) wie das Recht auf Vergessen, die Widerruflichkeit der Überlassung der Daten an Dritte, den Anspruch auf Information über die gespeicherten Daten und den Anspruch auf Löschung. Beide Bereiche, die Hoheit über den persönlichen Gehalt der Daten und die Hoheit über deren wirtschaftliche Verwertbarkeit, erfordern eine selbstbestimmte und ausdrückliche Einwilligung in die Nutzung der Daten und eine realistische Entscheidungsalternative zur Angabe der Daten. Soweit für den Bereich der wirtschaftlichen Verwertung die Daten als Entgeltsubstitut eingesetzt werden, begibt sich der Dateninhaber in ein Austauschverhältnis, auf das die allgemeinen Regeln für Schuldverhältnisse anzuwenden sind. Der Widerruf der Einwilligung zur Nutzung von Daten ist hierbei an die allgemeinen Regeln zur Beendigung von Verträgen, je nach Rechtsnatur durch Kündigung, Aufhebung, Widerruf oder Rücktritt vom Vertrag, gebunden. Hierbei sind Ansprüche auf Schadensersatz der Gegenseite denkbar. Zum anderen muss eine Beendigung von langlaufenden Verträgen, d. h. die Lösung aus einem Dauerschuldverhältnis gem. § 314 BGB, immer möglich sein. Es fehlt also an einer Qualifizierung des Rückrufs der datenschutzrechtlichen Einwilligung als Kündigung, Rücktritt oder Widerruf des Vertragsschlusses.

Im Lichte des dem Datenschutz zugrundeliegenden Verbraucherschutzes bedarf es zudem einer Diskussion über die Hierarchie der Nutzungszwecke, da für die Zulässigkeit der Datennutzung unter anderem der vom Unternehmen kommunizierte Zweck im Mittelpunkt stehen soll. Da der Zweck einer Datenverarbeitung sowohl von Zielen des öffentlichen Interesses (wie dem Katastrophenschutz) als auch von gewerblichen oder sonstigen privaten Interessen getragen sein kann, sollten die Anforderungen an die Transparenz- und Informationspflichten der Art. 12, 13 DS-GVO daran gemessen werden, wie viele Informationen erforderlich sind, damit die Souveränität und Kontrolle über die eigenen Daten gewahrt und die Entscheidungsfreiheit im Marktgeschehen nicht unlauter beeinträchtigt wird. Bei einer Hierarchisierung der Nutzungszwecke kann mehr Kommerzialisierung mehr individuelle Kontrolle und Information erfordern. Diese Restriktion dient der Aufrechterhaltung eines fairen Leistungswettbewerbs. Nicht Verbot der Nutzung ist dann das Ziel, sondern Herstellung von Privatautonomie bei der Nutzung und Schutz des Verbrauchers bei einer Informations- und Kontrollinadäquanz. Unternehmen dürfen dann mehr kommerzialisieren, d. h. mehr Daten für unternehmerische Zwecke einsetzen, wenn sie dem Kunden mehr Transparenz und Kontrolle über seine Daten und deren Verwendung einräumen.

Für den Bereich des Datenschutzes stellt die Datenschutzgrundverordnung einen neuen und grundsätzlich innovationsoffenen Rahmen dar. In den Details und konkreten Ausgestaltungen bleiben jedoch viele Fragen offen. So entsteht Rechtsunsicherheit in einem Bereich, der sowohl für Bürger als auch für Unternehmen nach hoher Rechtssicherheit verlangt. Eine schnelle Standardisierung könnte hierfür einen ersten Lösungsansatz bieten. So wären etwa standardisierte Einwilligungserklärungen für bestimmte Geschäftsmodelle durch Gesetz oder Branchenvereinbarung (vergleichbar der Widerrufserklärung im Fernabsatz), ggf. verbunden mit Zertifizierungsmodellen, ein gangbarer Weg, um

Rechtsunsicherheit im Zusammenhang mit den hohen Anforderungen an die Einwilligung von betroffenen Personen zu gewährleisten.

Notwendig ist über den Datenschutz hinaus die Abstimmung der einzelnen Gesetze innerhalb des gesamten Ordnungsrahmens. Recht in der digitalen Welt ist nicht nur Datenschutz und Datenschutz nicht nur die Datenschutzgrundverordnung sowie das BDSG-neu. Die Ziele des Datenschutzes müssen mit den Zielen aus anderen Rechtsbereichen in einen kohärenten Rechtsrahmen gebracht werden. Dazu sollten die Anwendungsgebiete möglichst klar voneinander getrennt werden.

Im Bereich des Wettbewerbsrechts wurden durch die 9. GWB-Novelle im Juni 2017 die Anforderungen der voranschreitenden Digitalisierung des Wirtschaftslebens adressiert. Für die Beurteilung, ob ein Unternehmen marktbeherrschend ist, wird zukünftig gemäß § 18 Abs. 2a GWB n.F. klargestellt, dass der Annahme eines Marktes nicht entgegensteht, dass eine Leistung unentgeltlich erbracht wird. Hierdurch sollen die Besonderheiten der digitalen Geschäftsmodelle überhaupt erfasst werden. Die Abgrenzung der entgeltlichen und unentgeltlichen Leistungen sowie die Kriterien hierfür bleiben für die Rechtsanwendung jedoch offen. Sie sollen der Einzelfallwürdigung überlassen bleiben, was im Ergebnis eine Rechtsunsicherheit für Unternehmen bedeutet. Dementsprechend besteht hier weiterer Konkretisierungsbedarf.

Auch das aus dem Wettbewerbsrecht stammende Recht auf Daten-Portabilität des Art. 20 DS-GVO, dessen Ziel die Bekämpfung von Lock-in-Effekten ist, bedarf einiger Konkretisierung. Insbesondere eine klare Benennung „maschinenlesbarer Formate“ und der für die Datenübertragbarkeit zu betreibende Aufwand müssen für die Praxis definiert werden.

Fazit

Grundsätzlich vereinfacht es die Software- und Komponentenentwicklung, wenn die Datenschutz-konzeption (mit dem Fokus auf „Privacy-by-Design“) erstellt wird, sobald das Systemkonzept steht, da eine nachgelagerte Datenschutzbetrachtung im Anschluss an die Softwareentwicklung u.U. ein zeit- und ressourcenaufwändiges Re-Design erfordert. In der Praxis des Forschungsprojekts hat sich allerdings gezeigt, dass sich dies nicht 1:1 umsetzen ließ: ursprüngliche Ideen wurden wieder verworfen und neue aufgenommen, Anpassungen unterschiedlichster Art wurden erforderlich. Für Forschungs- und Entwicklungsprojekte mit hoher Dynamik wird daher ein iteratives Vorgehen vorgeschlagen. Dies wurde in sd-kama auch so gehandhabt und hat sich bewährt.

Darüber hinaus wurde deutlich, dass durch die Anforderungen der Datenschutzgrundverordnung hinsichtlich des Privacy-by-Design-Ansatzes die Grenzen zwischen Datenschutz und Datensicherheit zunehmend verschwimmen. Durch die explizite Aufnahme der Sicherheit der Verarbeitung in Art. 32 DS-GVO ist die Verbindung von sicherheitstechnischen und datenschutztechnischen Maßnahmen stärker in den Fokus gerückt worden. Dadurch wird ein enger Austausch zwischen Informatikern und Juristen in den Bereichen notwendig. Ohne Datensicherheit ist Datenschutz nicht realisierbar, ohne Datenschutz ist technische Datensicherheit wertlos. Auch diese Erkenntnis wurde in sd-kama bereits erfolgreich umgesetzt.

Das Projekt SmartRegio

Ziel

SmartRegio ist darauf gerichtet, eine Big-Data-unterstützte Hilfeleistung für die Entscheidung von kleinen und mittleren Unternehmen anzubieten, die zentral den Bereich der Dienste zur Ausbauplanung regionaler Verteilnetze im Energiebereich sowie neuer Dienstleistungen für regionale Energieversorger abdeckt. Dazu werden eine Vielzahl von verschiedenen Datenquellen herangezogen, ausgewertet, aggregiert und zu neuen Aussagen verknüpft. Insbesondere statistische Erkenntnisse sollen ermittelbar werden, um auf dieser Basis Trends und Entwicklungen, aber auch generelle Aussagen über Präferenzen der Bevölkerung, der Nutzer, der Konkurrenten oder Dritter treffen zu können. Damit soll insgesamt eine bessere Steuerung durch eine bessere Entscheidungsgrundlage möglich werden.

Herausforderungen

Aus den Zielen des Forschungsvorhabens ergibt sich auch gleich das Problemfeld aus rechtswissenschaftlicher und insbesondere datenschutzrechtlicher Sicht, das im Teilprojekt behandelt wird. Die Vielzahl der verschiedenen Quellen und die Breite der nachgesuchten Informationen sowie die Zusammenfassung und Neuausrichtung der Informationen zu neuen Bedeutungsgehalten bedingt fast zwangsläufig, dass personenbezogene Daten und damit vom Datenschutzrecht erfasste Informationen automatisiert erfasst und verwendet werden. Daher muss nicht nur die Qualität der verwendeten Einzeldaten in ihrer Aussagekraft sichergestellt werden, sondern auch, dass die verwendeten Daten rechtmäßig verwendet werden können, was grundsätzlich entweder durch eine Einwilligung oder einen gesetzlichen Erlaubnistatbestand sichergestellt werden kann. Deshalb ist zu überprüfen, welche Daten überhaupt in welchem Zustand anfallen, ob also überhaupt von personenbezogenen Daten gesprochen werden kann oder möglicherweise bereits ein solcher Grad an Verallgemeinerung stattgefunden hat, dass Datenschutzrecht nicht (mehr) einschlägig ist. Die Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten ist dabei bereits aus rechtswissenschaftlicher Sicht nicht unproblematisch. Deshalb müssen Konzepte entwickelt werden, wie eine rechtmäßige Einbeziehung möglich gemacht werden kann. Diese technische Lösung bedarf dazu der präzisen datenschutzrechtlichen Bestimmung der Anforderungen und einer exakten Begleitung in der Entwicklung.

Lösung

Bereits die rechtlichen Herausforderungen haben gezeigt, dass viele rechtliche Fragen beim Einsatz von Smart-Data-Technologien bisher ungeklärt sind, für eine rechtskonforme Ausgestaltung aber zwingend beachtet werden müssen. In einem ersten Schritt erfolgte deshalb zunächst eine grundlegende Rechtsanalyse datenschutzrechtlicher Compliance-by-Design-Anforderungen bei der Nutzung von Smart Data im Energiesektor. Darauf aufbauend wurden Smart-Data-Analysen im Anwendungsbereich der kommenden Europäischen Datenschutzgrundverordnung (DS-GVO) spezifiziert. Um personenbezogene Daten verarbeiten zu können, wurden verschiedene Lösungsoptionen erwogen. Eine Lösung bestand darin, dass bestimmte Datengruppen per se nicht einbezogen werden, was allerdings gleichzeitig zu erheblichen Einbußen bezüglich der Aussagekraft der Entscheidungsdaten geführt hat. Eine andere technisch-rechtliche Lösungsoption bei Smart-Data-Analysen war der Einsatz von technischen Mitteln zur Anonymisierung, um so den Personenbezug bereits frühzeitig auszuschließen bzw. das Risiko einer Identifizierung zu minimieren. Zwar kennt die DS-GVO die Anonymisierung als Mittel für einen datenschutzschonenden Umgang nicht unmittelbar, allerdings wird die Anonymisierung zumindest in Erwägungsgrund 26 angesprochen. Dieser Erwägungsgrund kann zur Auslegung einzelner Normen der DS-GVO mittelbar herangezogen werden. Ferner wurde auf die personenbezogene Datenverarbeitung in Smart Metering Systemen einge-

gangen, wobei rechtlich hier insbesondere die Abgrenzung zwischen DS-GVO und Messstellenbetriebsgesetz (MsbG) virulent ist. Schließlich wurden grundlegende rechtliche Überlegungen zu datenschutzrechtlichen Anforderungen im Kontext des kommenden intelligenten gesteuerten Energieinformationsnetzes – dem Smart Grid – angestellt, da dort eine Vielzahl an Informationen ausgetauscht wird. Auch die dortige Erhebung, Verarbeitung, Analyse und Auswertung von (personenbezogenen) Daten erfolgt mit Smart Data Technologien. Dabei konnten verschiedene rechtliche Problemfelder identifiziert und analysiert werden.

Empfehlungen

Zusammenfassend konnte in SmartRegio deutlich gemacht werden, dass der Einsatz von modernen Smart Data Technologien mit erheblichen Rechtsunsicherheiten für den Datenverarbeiter verbunden ist. Gleichwohl wurden rechtliche Lösungsmöglichkeiten deutlich gemacht. Mangels fehlender Judikate wird die Rechtsunsicherheit aber auch noch in den nächsten Jahren bestehen bleiben, da bisher keine eindeutige rechtliche Tendenz erkennbar ist. Konkretisierungen aufgrund von Leitlinien sind deshalb erforderlich (etwa durch den künftigen Europäischen Datenschutzausschuss, vgl. Art. 68 ff. DS-GVO), um einen rechtssicheren Datenumgang insbesondere für Smart Data Technologieanbieter zu ermöglichen. Dem Gesetzgeber sowie künftigen Projekten sei deshalb angeraten, die rechtlichen und insbesondere datenschutzrechtlichen Anforderungen bei der Entwicklung neuer technischer Lösungen bereits frühzeitig zu berücksichtigen. Die kommende DS-GVO macht hier mit Art. 25 DS-GVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) einen ersten richtigen Schritt; ebenso das kommende BDSG-neu mit § 71 BDSG-neu (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen).

Fazit

Da die rechtlichen Fragestellungen oftmals sehr komplex sind und gerade die (datenschutz-)rechtlichen Probleme häufig nicht oder erst spät erkannt werden, weil aktiver Rechtsrat bei KMU sich zumeist auf vertragliche Rechtsberatung beschränkt, ist die Entwicklung von rechtssicheren oder zumindest rechtssichereren Vorgehensweisen von erheblicher Bedeutung, um KMU in ihrer Kompetitivität zu stärken, ihnen gleichzeitig aber die Vorzüge von Big Data/Smart Data nutzbar zu machen. Indem das Projekt SmartRegio von vorneherein datenschutzrechtliche Implikationen aufgreift, werden die technischen Lösungen darauf basierend entwickelt und möglichst datenschutzfreundlich ausgestaltet. Damit wird gleichzeitig gewährleistet, dass die Verfügbarmachung der Big Data/Smart Data Anwendungen zu einem späteren Zeitpunkt möglichst geringe Akzeptanzhürden zu überwinden hat: Wenn gezeigt werden kann, dass Datenschutz ernst genommen und aktiv integriert wurde, bestehen bessere Möglichkeiten, dass die darauf basierenden Dienste auch für Unternehmen nutzbar werden, ohne dass damit Qualitätseinbußen in der Aussagefähigkeit zwingend einhergehen müssen.

2 Smart Industry

Typische Datenquellen
- Maschinensensoren
- Produktionsumgebungen
- Kundendaten (B2B, B2C)

Aufgrund der zunehmenden Prozessautomatisierung im Maschinenbau entstehen durch eine Vielzahl von Sensoren pro Maschine riesige Datenmengen. Durch die intelligente Verarbeitung dieser Datenmengen können Produktionsabläufe noch zuverlässiger und effektiver geplant und durchgeführt werden.

Daneben spielt die Arbeitsteilung in der industriellen Produktion eine große Rolle. Für die Wettbewerbsfähigkeit des Endprodukts kann dank der anfallenden Daten die Produkt- und Prozessqualität über die gesamte Lieferkette hinweg optimiert werden. Die digitale Vernetzung aller beteiligten Unternehmen muss sich auch rechtlichen Herausforderungen stellen. Beim Erheben, Teilen und Verarbeiten der Daten stellt sich zunächst die Frage, ob personenbezogene Daten vorliegen und damit das Datenschutzrecht anwendbar ist. Soweit dies der Fall sein sollte, müssen die Rechte der Arbeitnehmer gewahrt werden. Daneben kann die Befürchtung der unkontrollierbaren Offenlegung von Geschäfts- und Betriebsgeheimnissen Unternehmen davon abhalten, sogenannten „Smart Ecosystems“ beizutreten und ihre Daten entlang von Lieferketten oder mit Konkurrenten zu teilen. Der Zugang zu Daten kann zu einer entscheidenden Wettbewerbsvoraussetzung werden.

Potentiell relevante Rechtsgebiete
- Datenschutzrecht
- Arbeitsrecht
- Urheberrecht und verwandte Schutzrechte
- Wettbewerbsrecht
- Lauterkeitsrecht

Potentiell anzuwendende Regularien
- Datenschutzgrundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG-neu)
- Betriebsverfassungsgesetz (BetrVG)
- Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)
- Gesetz gegen Wettbewerbsbeschränkungen (GWB)
- Gesetz gegen den unlauteren Wettbewerb (UWG)

Typische Herausforderungen und Rechtsfragen
- Anwendbarkeit Datenschutzrecht
- Arbeitnehmerdatenschutz
- Gemeinsame Verantwortlichkeit bei unternehmensübergreifender Datenverarbeitung
- Auftragsdatenverarbeitung
- Betriebs- und Geschäftsgeheimnisse
- Lizenzvereinbarungen für gemeinsame Datenbanknutzung

Mögliche Lösungsansätze
- Technisch-organisatorische Maßnahmen
- Datenzugriffs- und Datennutzungskontrolle (Access und Usage Control)
- Einsatz von Anonymisierungstechniken
- Standardverträge für unternehmensübergreifende Datennutzung

Die präsentierten Rechtsfragen stehen exemplarisch für den Anwendungsfall Industrie und können – müssen aber nicht – in einzelnen Projekten des Technologieprogramms Smart Data - Innovationen aus Daten aufgetreten sein.

Wann sind „Maschinendaten“ anonym?

Forschungsprojekte, die Daten verarbeiten, sollten sich zunächst die Frage stellen, ob datenschutzrechtliche Vorgaben einschlägig sind. Das Datenschutzrecht ist nur anwendbar auf personenbezogene Daten. Enthalten die Daten lediglich Informationen über Sachen wie Maschinen oder Ereignisse, liegt kein Personenbezug vor. Der Begriff „Maschinendaten“[9] kann jedoch täuschen, wenn diese Daten auch Rückschlüsse auf die Personen zulassen, die die Maschinen bedienen.

Personenbezogene Daten liegen vor, wenn sich die Informationen auf eine identifizierte oder identifizierbare natürliche Person beziehen.[10] Als identifizierbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann. Die Möglichkeit einer Identifizierung unter verhältnismäßigem Aufwand ist somit ausreichend.[11] Als Beispiele wie diese erfolgen kann, nennt die DS-GVO die Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.[12] Eine Person kann somit bereits dann identifiziert werden, wenn sie sich von allen anderen Personen einer Gruppe eindeutig unterscheiden lässt (Aussondern).[13] Für die Feststellung der Identifizierbarkeit sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden.[14] Eine ähnliche Formulierung fand sich bereits in der Datenschutzrichtlinie.[15] Auf Grundlage der bisherigen Rechtslage entschied der EuGH[16], dass:

- es nicht relevant ist, ob das jeweilige Datum für sich genommen identifizierend ist, sondern mögliche Verknüpfungen mit weiteren Informationen berücksichtigt werden müssen. Ein Datensatz kann somit durch ein Identifikationsmerkmal „infiziert“ werden.[17]
- es nicht relevant ist, ob sich die zur Identifizierung erforderlichen Informationen in der Hand des Verantwortlichen befinden. Wissen in den Händen Dritter ist ebenfalls zu berücksichtigen, wenn der Verantwortliche eine Möglichkeit hat auf legalem Wege Zugang zu diesen Daten zu erhalten und dies keinen unverhältnismäßigen Aufwand erfordern würde. Das Risiko einer Identifizierung ist de facto vernachlässigbar, wenn sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde.

Die Schwierigkeit bei der Bestimmung der Re-Identifizierungsrisiken liegt darin, dass durch fortschreitende Verknüpfung mit weiteren Datenbeständen, die Gefahr eines dynamischen „Hineinwachsens“ in den Personenbezug droht.[18] Zum Erhebungszeitpunkt anonyme Daten könnten somit im Laufe ihrer Verarbeitung zu personenbezogenen Daten werden.

Nach der DS-GVO sind alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, zu berücksichtigen, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie aber auch die technologische Entwicklung zu bedenken sind. Der Aufwand einer (Re-)Identifizierung sinkt mit der Entwicklung effizienterer Datenauswertungsmöglichkeiten. Entscheidend ist somit eine regelmäßige Bewertung der Verhältnismäßigkeit des Aufwands der De-Anonymisierung.[19]

Sachbezogene Daten können oftmals einen indirekten Personenbezug haben. Liegt der Zweck der Erhebung in der Zuordnung zu einer Person wird ebenfalls die Annahme des Personenbezugs gefordert.[20]

Einige Schutzmaßnahmen können ergriffen werden, um das (Re-)Identifizierungsrisiko zu senken:

- Die Verknüpfung von Datenbeständen mit weiteren Daten sollte kontrolliert und bei Bedarf begrenzt werden. Mit jedem zusätzlichen Informationszufluss zu einem bestehenden Datenbestand sollte die Identifizierbarkeit erneut geprüft werden.[21] Mittels Risikoanalyse sollte eine Prognose (auch künftig entstehenden) Personenbezugs erstellt werden.[22]
- Neben dem sachgerechten Einsatz von Anonymisierungstechniken,[23] können Zugriffsmöglichkeiten für Dritte technisch für bestimmte Zwecke und Zeiträume beschränkt werden.[24]
- Zugriffmöglichkeiten für Dritte sollten davon abhängig gemacht werden, dass sich Empfänger sanktionsbewehrt verpflichten keine (Re-)Identifizierung durchzuführen und Verstöße zu melden.[25] Bloße Absichtserklärungen können zwar die Anwendbarkeit des Datenschutzrechts nicht ausschließen,[26] jedoch könnten Vertragsstrafeklauseln bei der Verhältnismäßigkeit des Aufwands berücksichtigt werden.[27] Von anonymen Daten kann ausgegangen werden, wenn die Kosten einer De-Anonymisierung unter Berücksichtigung personeller, zeitlicher und technologischer Möglichkeiten so hoch sind, dass vernünftigerweise mit einer Re-Identifizierung nicht gerechnet werden muss.[28]

Einige Experten empfehlen, vorsorglich von einem Personenbezug auszugehen und die datenschutzrechtlichen Vorschriften zu beachten.[29] Dies macht aber nicht in jedem Fall Sinn. Ist der Eingriff in das Recht auf informationelle Selbstbestimmung mangels tatsächlicher Identifizierbarkeit gering, könne dieser Umstand nach der Rechtsprechung des BGH im Rahmen der Interessenabwägung berücksichtigt werden.[30] Werden externe Dienstleister als „Datenveredler“ mit der Smart-Data-Analyse beauftragt, müsste bei Personenbezug der Daten eine Auftragsdatenverarbeitung vereinbart werden. Zudem könnten mehrere Unternehmen berechtigtes Interesse daran haben auf die Daten zuzugreifen: Hersteller einzelner Komponenten einer Maschine benötigen Daten zur Produktoptimierung, während die Nutzer der Maschine Wartungsintervalle prognostizieren oder Anwendungsfehler detektieren möchten. Bei unternehmensübergreifender Verarbeitung personenbezogener Daten müssten gemeinsam Verantwortliche festlegen, wer von ihnen welche datenschutzrechtlichen Verpflichtungen erfüllt. Hier stellt sich die Frage, ob dieser Weg praktikabler ist, als ein „angemessenes Risikoniveau“[31] im Hinblick auf Anonymität der Daten sicherzustellen. Insbesondere wenn die Zuordnung der Daten zu individualisierbaren Personen zur Zielerreichung der Produkt- und Prozessoptimierung nicht erforderlich ist, dürfte die Vermeidung des Personenbezugs sowohl dem Schutz der betroffenen Grundrechte als auch den Datenverwertungsinteressen der Beteiligten eher entsprechen.

Wie sieht Arbeitnehmerdatenschutz 4.0 aus?

Auch wenn die Automatisierung im Rahmen von Industrie 4.0 die Notwendigkeit menschlicher Interaktion reduziert, besteht bei der Auswertung von Maschinendaten oftmals die Gefahr, dass auch Rückschlüsse auf Mitarbeiterinnen und Mitarbeiter gezogen werden könnten. Trotz direkter Anwendbarkeit der DS-GVO, ist die Rechtmäßigkeit der Verwendung von Arbeitnehmerdaten in § 26 BDSG-neu geregelt, da Art. 88 DS-GVO den Mitgliedstaaten ermöglicht spezifischere Vorschriften im Beschäftigungskontext zu erlassen. Inhaltlich wurde die bisherige Regelung[32] fortgeführt und erweitert.[33]

Soweit erforderlich können Arbeitnehmerdaten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden. Die Erforderlichkeit ist unter Abwägung der widerstreitenden Grundrechtspositionen im Einzelfall zu bestimmen.[34] Insbesondere sollte die Ausübung des Direktionsrechts des Arbeitgebers im Interesse der

datengestützten Prozessoptimierung nicht zu einem unzumutbaren Überwachungsdruck der Arbeitnehmerinnen und Arbeitnehmer führen.[35] Ob Beschäftigte in die Datenverarbeitung wirksam einwilligen können, ist aufgrund der Zweifel an der Freiwilligkeit in einem weisungsgebundenen Abhängigkeitsverhältnis umstritten.[36] Das BDSG-neu sieht eine Einwilligungsmöglichkeit vor, wenn unter Berücksichtigung des Machtungleichgewichts und der Umstände des Einzelfalls eine freiwillige Entscheidung angenommen werden kann.[37] Dies sei insbesondere dann der Fall, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Der Verantwortliche muss geeignete Maßnahmen ergreifen um die Datenschutzgrundsätze der DS-GVO einzuhalten.[38] Diese sind:

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Die Zulässigkeit von Datenverarbeitung im Beschäftigungsverhältnis kann auch in Kollektivvereinbarungen festgelegt werden. Dazu gehören Tarifverträge sowie Betriebs- und Dienstvereinbarungen. Arbeitgeber sollten zusätzlich die Beteiligungsrechte der Interessenvertretungen der Beschäftigten beachten. Das Betriebsverfassungsgesetz (BetrVG) sieht Mitbestimmungsrechte des Betriebsrats vor, wenn technische Einrichtungen eingeführt werden, die zur Überwachung der Arbeitnehmer bestimmt sind. Entscheidend ist hierbei jedoch die Überwachungseignung.[39]

Wem „gehören“ die Daten?

Werden Daten über Unternehmensgrenzen hinweg geteilt, stellen Beteiligte oftmals die Frage, wem Daten „gehören“. Grundsätzlich gilt, dass mangels Sachqualität kein Eigentum im rechtlichen Sinne an Daten bestehen kann.[40] Denn Sachen sind lediglich körperliche Gegenstände.[41] Ebenfalls nicht möglich ist ein „Datenbesitz“, da auch der Besitz eine tatsächliche Sachherrschaft und damit eine Sache voraussetzt.

Dennoch werden häufig Modelle wie das „Data Ownership“ diskutiert.[42] Da die Schaffung eines übertragbaren Ausschließlichkeitsrechts an personenbezogenen Daten mit dem Kern der Menschenwürdegarantie kollidieren würde,[43] fokussiert sich die Diskussion insbesondere auf anonyme, maschinengenerierte Daten.[44] Folgende Problemstellungen würde die Schaffung eines „Dateneigentums“ jedoch generieren oder verschärfen:

- Risikobewertung bei der Abgrenzung anonymer von personenbezogenen Daten,
- eindeutige Zuordnung zu einem „Urheber“ bei vernetzter Sensorik und zusammengesetzten Daten aus unterschiedlichsten Quellen,
- Abgrenzung zum Allgemeinwissen,
- Feststellung eines Lizenzberechtigten bei unbegrenzter Reproduzierbarkeit, und
- Wechselwirkungen zum bestehenden Rechtsrahmen (Datenschutzrecht, Schutz von Betriebs- und Geschäftsgeheimnissen, Urheberrecht und Recht des Datenbankherstellers).

Sowohl aus juristischer, ökonomischer wie gesellschaftspolitischer Sicht wird vor der Umsetzung eines „Dateneigentums“ gewarnt.[45] Daten befinden sich

dadurch keinesfalls in einem rechtsfreien Raum. Auch abseits des Datenschutzrechts finden sich wichtige Rechtsfragen, die die Nutzung von Daten beeinflussen können. So können Datenbanken dem Urheberrecht[46] oder Datenbankherstellerrecht sui generis unterliegen.[47] Daneben können Daten als Betriebs- und Geschäftsgeheimnis rechtlich geschützt sein.[48] Erwähnung finden sollte ebenfalls die Strafbarkeit des Abfangens und Ausspähens von Daten.[49] Mangels einer „One-Size-Fits-all-Lösung" für eine eigentumsrechtliche Zuordnung, bieten Datennutzungsverträge die erforderliche Flexibilität um auf dynamische Entwicklungen einer datengetriebenen Wertschöpfungsgesellschaft zu reagieren.[50] In einer Gesamtbetrachtung erscheint es deshalb sinnvoller über die Etablierung einer (europäischen) Wettbewerbsordnung für Zugang zu Daten (und Plattformen) anzusetzen, wie das in anderen Netzwirtschaften zum Teil auch der Fall ist.

Wie kann diskriminierungsfreier Zugang zu Daten erreicht werden?

Indem von Maschinen generierte Daten geteilt und wiederverwendet werden, können sie Wertschöpfung begründen, zu Innovationsquellen werden und damit unterschiedlichste Geschäftsmodelle ermöglichen. Der Zugang zu diesen Daten kann einen entscheidenden Wettbewerbsvorteil generieren, aber auf der anderen Seite zu Markteintrittshemmnissen führen, wenn Wettbewerbern vergleichbare Informationen bzw. Informationsquellen fehlen.[51]

Die 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen, die am 9. Juni 2017 in Kraft getreten ist, verfolgt das Ziel, ein modernes Wettbewerbsrecht im Zeitalter der Digitalisierung zu erreichen. Die Reform soll vor allem auf Daten basierende Netzwerk- und Skaleneffekte adressieren, die zu Marktkonzentration führen können, sowie den Zugang zu wettbewerbsrelevanten Daten besser berücksichtigen. Dadurch sollen die Kartellbehörden im Rahmen ihrer Missbrauchsaufsicht die Marktstellung eines Unternehmens besser beurteilen können und damit den sich verändernden internetbasierten Angeboten Rechnung tragen.

Entscheidend für wettbewerbsrechtliche Pflichten ist die „marktbeherrschende Stellung". Diese kann nun auch bei einem auf unentgeltlicher Leistung beruhenden Markt bestehen.[52] Dies betrifft insbesondere zwei- oder mehrseitige Märkte.[53] Werden hingegen unentgeltliche Leistungen aus nicht-wirtschaftlichen Motiven angeboten, die nicht auf eine Erwerbsstrategie zurückgehen, fehlt die wettbewerbsrechtliche Relevanz.[54] Bei der Bewertung der Marktstellung eines Unternehmens sind folgende Regelbeispiele hinzugekommen:[55]

- direkte und indirekte Netzwerkeffekte,
- die parallele Nutzung mehrerer Dienste und der Wechselaufwand für die Nutzer,
- seine Größenvorteile im Zusammenhang mit Netzwerkeffekten,
- sein Zugang zu wettbewerbsrelevanten Daten,
- innovationsgetriebener Wettbewerbsdruck.

Somit werden auch datengetriebene Geschäftsmodelle der Missbrauchs- und Fusionskontrolle unterworfen. Ein Missbrauch kann u.a. in folgenden Fällen vorliegen (vgl. § 19 GWB):

- Behinderung oder Diskriminierung anderer Unternehmen
- Forderung überhöhter Entgelte oder sonstigen Geschäftsbedingungen
- Unbegründete Zugangsverweigerung
- Unbegründete Aufforderung zur Vorteilsgewährung

Zur Prüfung, ob Daten(-plattformen) wettbewerbsrechtliche Relevanz zukommt, sind zwei Aspekte von besonderer Relevanz: Können auch Wettbewerber entsprechende Daten einfach beschaffen und welche Bedeutung, Menge und Breite kommt den Daten zu?[56]

Einen weiteren Diskussionspunkt bildet die Frage, ob es ein allgemeines Recht auf Datenportabilität, vergleichbar mit Art. 20 der Datenschutz-Grundverordnung („Recht auf Datenübertragbarkeit"), geben sollte.

Einige Smart-Data-Projekte verfolgen das Ziel, offene Plattformen für den unternehmensübergreifenden Datenaustausch zu realisieren. Herausforderungen, die sich u.a. dabei stellen, sind die Interessen der Unternehmen, ihre Betriebs- und Geschäftsgeheimnisse zu schützen und keine personenbezogenen Daten ohne Legitimationsgrundlage herauszugeben. Die Entwicklung intelligenter Filtermechanismen, Anonymisierungswerkzeuge sowie Konzepte der Datennutzungskontrolle könnten Lösungen bieten.

Über die Auswertung von Sensordaten, beispielsweise aus Maschinen, können Rückschlüsse auf die Herstellung von Maschinen und Produkten oder den Einsatz dieser Maschinen im Betrieb hergeleitet werden. Somit könnten Betriebs- und Geschäftsgeheimnisse sowohl der Maschinenhersteller als auch der Maschinenbetreiber hergeleitet werden und unternehmensbezogenes Wissen abfließen.

Die bisherige Regelung in §§ 17, 18 UWG dürfte mit der Neuregelung der Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (EU) 2016/943 einige Anpassungen erfahren. Insbesondere werden Daten rechtlichen Schutz als Geschäftsgeheimnis genießen, wenn sie Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen sind. Um zu verhindern, dass Wettbewerber Kenntnis unternehmensbezogener Daten erhalten, könnten sich gegebenenfalls bekannte Mechanismen aus dem Datenschutzrecht anbieten, wie beispielsweise Datentrennung, Zugriffskontrolle und Anonymisierung (Entfernung des Unternehmensbezugs). Mit der Datennutzungskontrolle (Usage Control), die klassische Zugriffskontrollmechanismen (Access Control) mit zusätzlichen Kontroll- und Steuerungsmöglichkeiten zur Nutzungszeit erweitert, sollen Berechtigte bestimmen können, wie Daten nach Zugriff genutzt werden.[57]

Daneben engagiert sich die Smart-Data-Begleitforschung in der Förderung eines kulturellen Wandels hin zur Open-Data-Ökonomie für eine smarte Gesellschaft.[58] Der Begriff „Open Data" steht für technische und rechtliche Offenheit, d. h., Datensätze müssen in einem maschinenlesbaren und standardisierten Format vorliegen und frei von rechtlichen Beschränkungen nutzbar sein (d. h. allgemein zugänglichen bzw. nicht unverhältnismäßig einschränkenden Lizenzbestimmungen unterliegen). Offene, genormte und gut dokumentierte Programmierschnittstellen (API) können den Aufbau eines Ökosystems der Anwendungs- und Algorithmenentwicklung fördern und so den Zugang zu Daten, die sich in der Hand von Unternehmen oder Behörden befinden, vermitteln. Um sicherzustellen, dass der Zugang datenschutzkonform ist, sollte die Entwicklung von Anonymisierungswerkzeugen und -prüfverfahren, unterstützt durch technische Leitfäden, parallel gefördert werden.

Das Projekt SAKE: Semantische Analyse komplexer Ereignisse

SAKE
Semantische Analyse Komplexer Ereignisse

Ziel von SAKE ist es, eine Plattform für die effiziente Integration und Verarbeitung von Strömen heterogener Ereignisdaten in Produktionsanlagen im Bereich Maschinen- und Anlagenbau zu entwickeln. Durch die gewonnenen Analyse-Erkenntnisse können Ressourcen geschont und potenzielle Fehlerquellen erkannt und frühzeitig behoben werden.

Herausforderungen

Die intelligente Verarbeitung riesiger digitaler Informationsströme aus industriellen Maschinensensoren verschiedener Zulieferer ist die zentrale Herausforderung im Projekt SAKE. Hierbei können auch Daten mit Personenbezug vorkommen oder durch Kombination von Daten ein Personenbezug entstehen.

Lösung

Rechtliche Restriktionen werden durch die Nutzung anonymer Daten vermieden. Aus Maschinensensoren gewonnene Daten werden keinen Personen zugeordnet. Soweit Benutzer-Interaktionen erfasst werden, werden sie ohne Zuordnung zu einer individualisierbaren Person geloggt und nicht im Projekt (weiter-) verwendet oder anderen zur Verfügung gestellt.

Fazit

Der Einsatz von Smart-Data-Lösungen stellt eine enorme Chance für den Standort Deutschland dar. Leuchtturmprojekte wie das Projekt SAKE zeigen sowohl die große Vielfalt als auch das Potenzial von Anwendungen und Dienstleistungen, die auf dieser Technologie aufbauen.

3. Smart Public Data

Typische Datenquellen
- Öffentlich zugängliche Social-Media-Plattformen
- Informationen öffentlicher Stellen
- Presseerzeugnisse
- Unternehmensveröffentlichungen

Im World Wide Web findet sich eine Vielzahl an Informationen – die Nutzung dieser Daten kann jedoch auch rechtlichen Restriktionen und Unsicherheiten unterliegen. Sind die Daten personenbezogen, bedarf es einer datenschutzrechtlichen Legitimationsgrundlage, sowie der Einhaltung datenschutzrechtlicher Vorgaben wie der ausreichenden Information der betroffenen Personen. Bei einem gewissen Level an Kreativität (Schöpfungshöhe), können Werke wie Texte, Bilder oder Datenbanken Urheberrechtsschutz genießen. Urheber könnten die Unterlassung von Nutzungshandlungen wie der Vervielfältigung im Rahmen einer Smart-Data-Analyse verlangen.

Potentiell relevante Rechtsgebiete
- Datenschutzrecht
- Urheberrecht und verwandte Schutzrechte
- Presseverlegerleistungsschutzrecht
- Schuld-/Sachenrecht

Potentiell anzuwendende Regularien
- Datenschutzgrundverordnung (DS-GVO)
- Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)
- Bürgerliches Gesetzbuch (BGB)

Typische Herausforderungen und Rechtsfragen
- Anwendbarkeit Datenschutzrecht
- Datenschutzrechtliche Legitimationsgrundlage
- Erfüllung Informationspflichten
- Diskriminierungsfreier Zugang zu veröffentlichten Informationen
- Vertrags-/Sachenrechtliche Unterlassungsansprüche von Plattformbetreibern
- Unterlassungsansprüche von Urhebern
- Unterlassungsansprüche von Presseverlegern

Mögliche Lösungsansätze
- Text- und Data-Mining-Schranke
- Automatisierung Information, Einwilligung/Lizenzerteilung und Widerspruch
- Förderung von Open Data
- Anonymisierung
- Framing/Verlinkung von Inhalten

Die präsentierten Rechtsfragen stehen exemplarisch für den Anwendungsfall „Verwendung öffentlicher Daten“ und können – müssen aber nicht – in einzelnen Projekten des Technologieprogramms Smart Data - Innovationen aus Daten aufgetreten sein.

Wie weit dürfen öffentlich zugängliche Daten genutzt werden?

Solange Daten Personenbezug aufweisen, unterliegt die Datenverarbeitung den geltenden Datenschutzbestimmungen.[59] Jede Datenverarbeitung bedarf dann einer Legitimationsgrundlage. Dies kann nach der DS-GVO sein:[60]

- Einwilligung der betroffenen Person für einen oder mehrere bestimmte Zwecke,
- Datenverarbeitung ist zur Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen erforderlich,
- Erfüllung einer rechtlichen Verpflichtung,
- Schutz lebenswichtiger Interessen natürlicher Personen,
- Wahrnehmung von Aufgaben im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde,
- Datenverarbeitung ist zur Wahrnehmung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere bei Kindern.

Nach bisherigem Recht bestand im Bundesdatenschutzgesetz eine gewisse Privilegierung für die Verwendung öffentlich zugänglicher personenbezogener Daten.[61] Unter öffentlich zugänglichen Daten sind solche zu verstehen, die aufgrund ihrer Zielsetzung, Natur oder Publikationsform für eine unbestimmte Anzahl an Personen erreichbar sind.[62] Beispiele sind Massenmedien und Internetseiten aber auch User Generated Content auf Social Media Plattformen, wenn die Inhalte ohne rechtliche oder technische Zugangsbarrieren wahrnehmbar sind und nicht für einen bestimmten Nutzerkreis beschränkt wurden.[63] Öffentlich zugängliche Daten durften genutzt werden, soweit die schutzwürdigen Belange der betroffenen Personen die Datenverarbeitungsinteressen nicht „offensichtlich überwiegen".[64]

Diese Regelung wird nun durch die direkte Anwendbarkeit der DS-GVO abgelöst, die keine vergleichbare Privilegierung enthält. Eine Legitimation könnte über die Auffangklausel der Interessenabwägung[65] erfolgen, wenn folgende Voraussetzungen vorliegen:

1. Berechtigtes Interesse: rechtmäßiges rechtliches, tatsächliches, wirtschaftliches oder immaterielles Interesse.[66] Als Beispiele nennt die DS-GVO Betrugsprävention, Direktwerbung, Übermittlung innerhalb von Unternehmensgruppen sowie Netz und Informationssicherheit.[67]
2. Erforderlichkeit: kein milderes, gleich effizientes Mittel.[68]
3. Kein Überwiegen der Betroffeneninteressen unter Berücksichtigung der potenziellen Folgen und vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zum Verantwortlichen beruhen.[69] Der Schutz von Kindern wird besonders hervorgehoben.[70]

Bei der sorgfältigen Abwägung ist zudem zu prüfen, ob die Betroffenen zum Zeitpunkt der Erhebung und angesichts der Umstände des Einzelfalls vernünftigerweise absehen können, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Bei der Erfassung öffentlich zugänglicher Daten mittels Web-Crawling-Methoden[71] besteht jedoch keine Beziehung zwischen Betroffenem und Verantwortlichem. Fraglich bleibt, inwieweit die Tatsache der öffentlichen Zugänglichkeit in die Abwägung mit einbezogen werden kann.

Eine Besonderheit findet sich im Zusammenhang mit „besonderen Kategorien personenbezogener Daten", d.h. Daten, die besonders sensibel und eines besonderen Schutzes bedürfen.[72] Die Verarbeitung dieser Daten ist zunächst untersagt, die DS-GVO enthält jedoch einen Katalog von Ausnahmen.[73] Einer dieser Ausnahmen greift, wenn sich die Verarbeitung auf personenbezogene Daten bezieht, die die betroffene Per-

son offensichtlich öffentlich gemacht hat. Diese Ausnahme des Verarbeitungsverbots kann jedoch nicht als eigenständige Legitimationsgrundlage gelesen werden. Andernfalls unterlägen im Fall der öffentlichen Zugänglichkeit sensible Daten mangels Güterabwägung einem niedrigeren Schutzniveau als andere personenbezogene Daten. Daher muss zusätzlich einer der Legitimationsgründe des Art. 6 Abs. 1 DS-GVO vorliegen.[74] In Betracht kommt wiederum die Interessenabwägung. Daneben kann die Frage aufgeworfen werden, ob aus der Ausnahme der öffentlichen Zugänglichkeit die Vermutung abgeleitet werden kann, dass die Verarbeitung dieser Daten dem Betroffenenинteresse seltener widerspricht[75] und eine derartige Wertung im Umkehrschluss in die Interessenabwägung für sämtliche personenbezogene Daten einbezogen werden könnte.

Sind die Voraussetzungen einer Legitimationsgrundlage erfüllt, müssen die weiteren datenschutzrechtlichen Pflichten eingehalten werden. Eine weitere Herausforderung besteht bei den Informationspflichten: mangels Beziehung zwischen Verantwortlichem und Betroffenen, besteht in der Regel auch keine direkte Ansprechmöglichkeit. Einerseits ist explizit zusätzlich darüber zu informieren, wenn die Daten aus öffentlich zugänglichen Quellen stammen.[76] Andererseits kann die Informationserteilung unterbleiben, wenn diese sich als unmöglich erweisen oder einen unverhältnismäßigen Aufwand erfordern würde.[77] In diesem Fall sollten Informationen öffentlich bereitgestellt werden.

Welche Einschränkungen ergeben sich aus dem Urheberrecht?

Um Smart-Data-Analysen durchzuführen, müssen Daten oftmals zunächst aus Texten, Datenbanken, Bildern oder ähnlichem extrahiert werden. Beim sogenannten Text und Data Mining[78] erfordert dies aus technischer Sicht zumeist eine Zwischenkopie der Ursprungsdaten sowie der Anpassung an das entsprechende Format zur Datenextraktion.[79] Liegt ein urheberrechtlich geschütztes Werk vor, bedürfen bestimmte Nutzungshandlungen wie die Vervielfältigung grundsätzlich der Zustimmung des Urhebers, es sei denn eine gesetzliche Erlaubnis greift ein (Schranke).

Die Unterscheidung zwischen urheberrechtlich geschützten Werken und solchen, die nicht über die ausreichende geistig-individuelle Schöpfungshöhe verfügen, ist oft herausfordernd.[80] Denn auch die sogenannte „kleine Münze“, also Werke mit geringerer schöpferischer Leistung sind grundsätzlich schutzfähig.[81] Ausschließlich beschreibender Text oder die reine Informationsdarstellung in Alltagssprache sind nicht schutzfähig.[82] Somit könnten gerade im Bereich User Generated Content Abgrenzungsschwierigkeiten entstehen, da es auch nicht entscheidend auf die Länge eines Textes ankommt.[83]

Bei Datenbanken kann neben dem Schutz als urheberrechtliches Werk auch der Investitionsschutz nach dem sui-generis-Recht des Datenbankherstellers greifen.[84] Hierbei kommt es gerade nicht auf die gestalterische Anordnung an, sondern ob eine wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung getätigt wurde.[85] Die Vervielfältigung, Verbreitung oder öffentliche Wiedergabe der gesamten Datenbank oder wesentlicher Teile bedarf grundsätzlich der Zustimmung des Datenbankherstellers, soweit keine Ausnahme greift.[86]

Zulässig sind vorübergehende Vervielfältigungshandlungen, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen und deren alleiniger Zweck es ist, eine Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder eine rechtmäßige Nutzung eines Werkes oder sonstigen Schutzgegenstands zu ermöglichen, und die keine eigenständige wirtschaftliche Bedeutung haben.[87] Liegt der Zweck in der Informationsextraktion und -analyse, die keinerlei

permanente Kopien erfordert, könnten Datenanalyse-Aktivitäten zustimmungsfrei durchgeführt werden.[88] Nach geltendem Rechtsverständnis ist die Analyse und Extraktion von Informationen erlaubnisfrei,[89] vergleichbar mit dem menschlichen Werkgenuss.[90] Ebenfalls frei nutzbar sind die Erkenntnisse, die aus diesen Analysen generiert werden.

Für die wissenschaftliche Forschung besteht ab 01. März 2018 eine Schranke für Text- und Data-Mining.[91] Danach dürfen Werke vervielfältigt werden und diese Kopien einem bestimmt abgegrenzten Kreis von Personen für die gemeinsame wissenschaftliche Forschung sowie einzelnen Dritten zur Überprüfung der Qualität wissenschaftlicher Forschung öffentlich zugänglich gemacht werden, wobei nur nicht-kommerzielle Zwecke verfolgt werden dürfen. Rechtsunsicherheit besteht, wenn Forschungsprojekte in spätere kommerzielle Anwendungen münden sollen.

Auf europäischer Ebene soll eine vergleichbare Forschungsausnahme geschaffen werden.[92] Befürchtet wird, dass wenn im Umkehrschluss europäische Anbieter von Webanalysen und Suchtechnologien mit sämtlichen Urhebern Lizenzen abschließen müssen, die praktischen wie wirtschaftlichen Hürden das Ende für viele Anbieter von Datenanalysen in Europa bedeuten würden.[93]

Im Gegensatz dazu bietet im amerikanischen Rechtsrahmen die sogenannte Fair-Use-Doktrin[94] eine Abwägungsmöglichkeit zwischen den berechtigten Interessen der Urheber an der wirtschaftlichen Verwertung ihres Werkes und der Möglichkeit einer freien Nutzung. Ein an der Fair-Use-Doktrin orientierter Vorschlag einer Text- und Data-Mining-Schranke[95] für Forschungs- wie auch kommerzielle Zwecke könnte sicherstellen, dass die jeweiligen Urheber durch die Nutzung ihrer Werke im Rahmen des Text- und Data-Mining nicht bei der wirtschaftlichen Verwertung ihrer Schöpfungsleistung oder in ihrem Urheberpersönlichkeitsrechts beeinträchtigt werden.

Wann muss das Presseverlegerleistungsschutzrecht beachtet werden?

Das deutsche Presseverlegerleistungsschutzrecht besteht nicht gegenüber jedermann, sondern nur gegenüber gewerblichen Anbietern von Suchmaschinen sowie gewerblichen Anbietern von Diensten, die Inhalte entsprechend aufbereiten.[96] Es gewährt Herstellern eines Presseerzeugnisses ab Veröffentlichung für ein Jahr das ausschließliche Recht, das Presseerzeugnis oder Teile davon zu gewerblichen Zwecken öffentlich zugänglich zu machen.[97] Zu Presseerzeugnissen zählen „redaktionell-technische Festlegungen journalistischer Beiträge im Rahmen einer unter einem Titel auf beliebigen Trägern periodisch veröffentlichten Sammlung, die bei Würdigung der Gesamtumstände als überwiegend verlagstypisch anzusehen ist und die nicht überwiegend der Eigenwerbung dient. Journalistische Beiträge sind insbesondere Artikel und Abbildungen, die der Informationsvermittlung, Meinungsbildung oder Unterhaltung dienen“.

Auch Blogs können Presseerzeugnisse darstellen, wenn sie als eine redaktionell ausgewählte Sammlung journalistischer Beiträge gewertet werden können.[98] Dem Presseverleger steht nur das Recht der öffentlichen Zugänglichmachung des Originals zu gewerblichen Zwecken zu, wodurch die Vervielfältigung ausdrücklich nicht eingeschränkt wird.[99] Sobald Presseerzeugnisse die Schöpfungshöhe erreichen, können sie aber Urheberrechtsschutz genießen.

Eine Verlinkung bleibt jedoch weiterhin möglich,[100] hierfür erstreckt sich das neue Schutzrecht nicht auf einzelne Wörter und kleinste Textausschnitte.[101] Umstritten ist die zulässige Länge dieser „kleinsten Textausschnitte“, insbesondere im Zusammenhang mit der Anzeige sogenannter Snippets.[102]

Das im Vorschlag der EU-Kommission vorgesehene Leistungsschutzrecht im Entwurf der Richtlinie über

das Urheberrecht im digitalen Binnenmarkt[103] würde weiter gehen, da im Entwurf keine Beschränkungen auf bestimmte Verpflichtete oder Textlängen enthalten sind sowie auch das Recht der Vervielfältigung „bei digitaler Nutzung“ den Presseverlagen vorbehalten sein soll. Zusätzlich würde sich die Schutzdauer von einem Jahr auf 20 Jahre verlängern, wenn dieser Entwurf in Kraft treten würde. Die Möglichkeit Wertschöpfungsketten auf Grundlage von Informationen aufzubauen, die ursprünglich aus Presseerzeugnissen stammen, könnten damit erheblich eingeschränkt werden.

Da die Erteilung von Nutzungslizenzen grundsätzlich der Dispositionsfreiheit privatautonomer Marktteilnehmer unterliegt, besteht unterhalb der wettbewerbs- und kartellrechtlichen Missbrauchstatbestände kein Kontrahierungszwang. Große Marktteilnehmer könnten insofern bessere Konditionen erhalten, da z. B. Verlage auf die Indexierung durch Suchmaschinen angewiesen sind, wodurch weniger marktmächtige Anbieter diskriminiert werden.[104] Daneben besteht die Gefahr, dass Verlage Exklusivverträge einfordern (bzw. die Garantie, dass mit bestimmten Konkurrenten keine vergleichbaren Lizenzvereinbarungen getroffen werden) und Konkurrenzverhältnisse auf Sekundärmärkte verlagern. Die zentrale Schlüsselfrage ist daher, wie die rechtliche Regulierung im Bereich „Smart Data“ effektiv Diskriminierungsfreiheit herstellen kann. Diese Problematik würde sich nicht stellen, wenn eine generelle Erlaubnis für Text- und Data-Mining (eine sogenannte Schranke) ausschließlich zur Informationsextraktion erfolgende Vervielfältigungen zustimmungsfrei ermöglichen würde. Alternativ müssten wettbewerbsrechtliche Mechanismen etabliert werden, um die Gewährung des Zugangs zu Informationen unter diskriminierungsfreien Konditionen festzuschreiben.

Das Projekt iTesa: Intelligent Traveller Early Situation Awareness

Ziel

In einer globalisierten Welt gehören Geschäftsreisen mittlerweile zum Alltag vieler Branchen. Doch das Reisen birgt immer auch Risiken: In manchen Regionen muss mit Naturkatastrophen, Epidemien oder Terroranschlägen gerechnet werden. Bei Ausbruch einer Krise kann zuweilen viel Zeit verstreichen, bis es einen vollständigen Überblick über die genaue Lage vor Ort gibt. Dadurch verlieren Unternehmen wertvolle Zeit, um für ihre Mitarbeiter geeignete Schutzmaßnahmen zu ergreifen. Derartige Schutzmaßnahmen, wie auch grundsätzliche Informationspflichten in Bezug auf Dienstreisen und insbesondere Auslandsentsendungen, sind aber Teil der Fürsorgepflichten im Rahmen der vertraglichen Nebenpflichten aus § 241 Abs. 2 BGB des Arbeitsverhältnisses.

Das Smart-Data-Projekt „iTESA – Intelligent Traveller Early Situation Awareness“ möchte dieses Defizit beheben und es Unternehmen und Reisenden ermöglichen, im Ernstfall schneller zu reagieren. Hierfür durchsucht iTESA mithilfe spezieller Datenanalysen und selbstlernender Algorithmen weltweit zahlreiche Quellen wie Internetseiten, soziale Netzwerke, Agentur- und Pressemeldungen sowie Nachrichten und Informationen von Behörden nach möglichen Reiserisiken.

In der nächsten Stufe prüft iTESA die Meldungen auf ihre Glaubwürdigkeit und mögliche Auswirkungen und ordnet einem Vorfall einen Bedrohlichkeitsgrad zu. Auf diese Weise kann der nötige Handlungsbedarf realistisch eingeschätzt werden. Neben der Analyse von Ereignissen stellt iTESA einen möglichst genauen geographischen Bezug her – bis hin zum betroffenen Straßenzug. Durch einen Abgleich mit Reisedaten aus Traveller-Systemen ist iTESA in der Lage zu ermitteln, welche Mitarbeiter oder Kunden sich in der Gefahrenzone befinden oder planen, dorthin zu reisen. Per Mitteilung können diese anschließend gewarnt werden.

Lösungsoptionen

Im Rahmen des iTESA-Projektes wurde aus datenschutzrechtlicher Sicht ein Rechtsgutachten der geplanten Datenverarbeitungsvorgänge erstellt. Hierbei wurde der technische status quo der im Projekt geplanten Tätigkeiten dargestellt, die möglichen Rechtsgrundlagen für die Datenverarbeitungsvorgänge geprüft und sodann ein umfassender Katalog an technischen und organisatorischen Maßnahmen erstellt, um bei den Datenverarbeitungsvorgängen ein möglichst geringes Risiko für die Grundrechte und Grundfreiheiten der betroffenen Personen zu gewährleisten.

Es wurde besonderes Augenmerk auf die Problematik der Verarbeitung allgemein zugänglicher personenbezogener Daten gelegt: Wenn der Verantwortliche ein Crawling solcher Daten durchführt, wird er sich in der Regel auch auf sein Grundrecht auf Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 2. Alt. GG sowie Art. 10 Abs. 1 Satz 2 2. Alt. EMRK berufen können. Während des Crawlings besteht aber auch das Problem, dass der Verantwortliche den Inhalt der abzurufenden Website nicht antizipieren kann, sodass er unter Umständen nicht nur personenbezogene Daten, sondern auch besondere Kategorien personenbezogener Daten verarbeiten würde. Für die Verarbeitung dieser Daten besteht in einer Vielzahl von Fällen in dieser Konstellation allerdings keine Rechtsgrundlage. Das mit der Verarbeitung dieser Daten einhergehende datenschutzrechtliche Problem ist zwar kein spezifisches Problem für das iTESA-Projekt, wurde aber bisher in der Wissenschaft kaum berücksichtigt. Insbesondere ist für eine Vielzahl an heute bereits alltäglichen Datenverarbeitungsvorgängen nach aktuellem Recht keine Rechtsgrundlage unmittelbar anwendbar. Diese konkrete Lücke wird auch durch das neue harmonisierte Recht nicht geschlossen werden, weshalb im Anwendungsfall von iTESA unter Berücksichtigung der Interessen der einzelnen von der Datenverarbeitung betroffenen und profitierenden Personen eine abwägende Betrachtung durchgeführt und das neue Recht entsprechend grundrechtskonform ausgelegt werden musste.

Empfehlungen

Gerade im Hinblick auf den Einsatz neuer Technologien sollten Datenschutz und die Aspekte datenschutzfreundlicher Technikgestaltung so früh wie möglich Einzug in den Planungsprozess halten. Bei der Schaffung neuer rechtlicher Rahmenwerke sollte der Gesetzgeber den Fokus auf Technologieneutralität bei hinreichender Konkretisierung setzen, damit die Zukunftsfähigkeit sichergestellt ist und auch künftige technologische Weiterentwicklungen noch adäquat umfasst werden.

4 Smart Mobility

Typische Datenquellen
- Verkehrsteilnehmer
- Mobilitätsanbieter
- Behördliche Informationen
- Sensorik im Verkehrsnetz
- Umweltdaten

Der zunehmende Verkehr in deutschen Städten sorgt für lange Staus, eine hohe Feinstaubbelastung und verursacht Kosten für Wirtschaft und Bürger. Daneben sind für eine Reise von der Haustür zum endgültigen Ziel meist mehrere Transportmittel nötig. Der Anspruch, eine kontinuierliche Reisekette zu gewährleisten, stellt den Mobilitätssektor jedoch vor diverse Herausforderungen, weil die Nutzung von Mobilitätsangeboten oft stark schwankt und die verschiedenen Anbieter im Mobilitätsbereich nur selten aufeinander abgestimmt sind. Daneben birgt das Reisen immer auch Risiken: Mit Naturkatastrophen, Epidemien oder Terroranschlägen muss in manchen Regionen gerechnet werden. Unternehmen müssen ihrer gesetzlichen Informations- und Fürsorgepflicht gegenüber ihren Mitarbeiterinnen und Mitarbeitern nachkommen und sie vor solchen Vorfällen schützen. Um die Wettbewerbsfähigkeit zu erhalten, ist deshalb eine neue Mobilität gefragt. Um die hierfür erforderlichen Daten nutzen zu können, sind wiederum die Anforderungen des Datenschutzrechts zu beachten.

Potentiell relevante Rechtsgebiete
- Datenschutzrecht
- Arbeitsrecht
- Urheberrecht und verwandte Schutzrechte
- Wettbewerbsrecht
- Lauterkeitsrecht

Potentiell anzuwendende Regularien
- Datenschutzgrundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG-neu)
- Betriebsverfassungsgesetz (BetrVG)
- Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)
- Gesetz gegen Wettbewerbsbeschränkungen (GWB)
- Gesetz gegen den unlauteren Wettbewerb (UWG)

Typische Herausforderungen und Rechtsfragen
- Anwendbarkeit Datenschutzrecht
- Besonderheiten Standortdaten
- Arbeitnehmerdatenschutz
- Gemeinsame Verantwortlichkeit bei unternehmensübergreifender Datenverarbeitung
- Diskriminierungsfreier Zugang zu mobilitätsbezogenen Daten
- Betriebs- und Geschäftsgeheimnisse
- Lizenzvereinbarungen zur Nutzung von Datenbanken

Mögliche Lösungsansätze
- Technisch-organisatorische Maßnahmen
- Datenzugriffs- und Datennutzungskontrolle (Access und Usage Control)
- Datenminimierung durch Pseudonymisierung, Generalisierung und Randomisierung
- Privacy Management
- Standardverträge für unternehmensübergreifende Datennutzung

Die präsentierten Rechtsfragen stehen exemplarisch für den Anwendungsfall Mobilität und können – müssen aber nicht – in einzelnen Projekten des Technologieprogramms Smart Data - Innovationen aus Daten aufgetreten sein.

Wie können Standortdaten datenschutzkonform genutzt werden?

Aus engmaschigen Standortdaten lassen sich Bewegungsprofile erstellen, die wiederum sehr detaillierte Einblicke in den persönlichen Lebensablauf ermöglichen. Können sich Betroffene einer lückenlosen Erfassung ihrer Positionsdaten nicht entziehen, ist eine Verhaltensänderung der Betroffenen zu befürchten, wodurch weitere Grundrechte betroffen sein können wie die Versammlungsfreiheit oder die Freizügigkeit.[105] Soweit sich Standortdaten einer identifizierbaren Person zuordnen lassen, bedarf die Verarbeitung einer datenschutzrechtlichen Legitimation. Welche Rechtsgrundlage in Frage kommt, hängt von den Umständen des Einzelfalls ab.

Anonymisierung

Ist die Identifizierung einzelner Individuen für die Erreichung der Optimierungsziele nicht erforderlich, so könnte die Anonymisierung eine Option sein um eine rechtssichere Nutzbarkeit der Daten im Rahmen von Smart Data Analysen zu ermöglichen. Insbesondere bei Geodaten ist die Trennlinie zwischen Sach- und Personendaten oftmals nur schwer zu ziehen.[106] So steigt das (Re-)Identifizierungspotential, wenn aussagekräftige Bewegungsprofile und damit typische Bewegungsmuster individueller Personen aus den Daten ableitbar sind.[107] Mit der Aufnahme der Standortdaten in den Katalog der möglichen Identifizierungskennzeichen bei der Definition des personenbezogenen Datums,[108] macht der europäische Gesetzgeber die Relevanz des Standorts für die Identifizierbarkeit deutlich.[109]

Zur Feststellung wirksamer Anonymisierung stellen sich die bereits unter „Fall 1: Smart Industry“ (Wann sind „Maschinendaten“ anonym?) beschriebenen Herausforderungen. Soweit eine Anonymisierung im Rechtssinne nicht erreicht werden kann, kann der Einsatz von Anonymisierungstechniken die Eingriffsintensität senken und somit dem Ziel der Datenminimierung dienen. Mit den Konzepten Privacy-by-Design und Privacy-by-Default verpflichtet die DS-GVO sanktionsbewehrt technisch mögliche und wirtschaftlich zumutbare Datenminimierungsmaßnahmen umzusetzen sowie den Nutzern privatsphärenfreundliche Voreinstellungen zu gewähren.[110] Als Beispiel nennt die DS-GVO die Pseudonymisierung.

Pseudonymisierung

Pseudonym sind Daten, die „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.[111] Diese Definition geht über das bloße Ersetzen des Namens durch ein Kennzeichen hinaus.[112] Ferner sollte bedacht werden, dass Pseudonyme personenbezogene Daten sind, soweit sie durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten.[113] Risiken entstehen sowohl durch Zugriffsmöglichkeiten auf Zuordnungstabellen oder -regeln als auch durch die Analyse der gesammelten Standortdaten, insbesondere wenn feste Pseudonyme über längere Zeiträume verwendet werden.

Liegen personenbezogene Daten vor, ist eine datenschutzrechtliche Legitimation erforderlich. Besonderheiten bestehen, wenn personenbezogene Daten von Arbeitnehmerinnen und Arbeitnehmern betroffen sind.

Beschäftigtendatenschutz

In der Logistik kann es für Unternehmen entscheidende Vorteile bringen, genaue Kenntnis über die exakte Lokalisation ihrer Fahrzeuge oder Mitarbeiterinnen und Mitarbeiter zu haben. Gerade bei einem lücken-

losen Tracking steigt jedoch die persönlichkeitsrechtliche Relevanz, insbesondere wenn die Daten auch Zustands-, Verhaltens- oder Leistungskontrollen ermöglichen.[114] Im Abschnitt „Fall 1: Smart Industry" wurden die grundsätzlichen Herausforderungen des Arbeitnehmerdatenschutzes bereits skizziert. Je nach Fallszenario können Beschäftigte verpflichtet sein, Standortmeldungen abzugeben, ein Beispiel ist der rechtlich vorgeschriebene elektronische Fahrtenschreiber für bestimmte Lastwagen oder Busse.[115] Sollen Standorterfassungen über eine Einwilligung legitimiert werden, setzt das Gebot der Freiwilligkeit mindestens voraus, dass Mitarbeiter das Ortungssystem, ohne Nachteile befürchten zu müssen, ausschalten können.[116] Daneben könnte sich eine Rechtfertigung je nach Kontext und Zielsetzung aus arbeitsvertraglichen Kontrollrechten des Arbeitgebers ergeben.[117] Eine vollständige Überwachung des Arbeitsverhaltens könnte jedoch mit dem Persönlichkeitsrechtschutz unvereinbar sein.[118] Bei Überwachungseignung sollten zusätzlich die Mitbestimmungsrechte des Betriebsrats berücksichtigt werden.[119]

Welche Rechtsfragen können bei Auswertung von Datenbanken und unternehmensbezogenen Daten relevant werden?

Datenbanken

Viele mobilitätsbezogene Informationen sind in öffentlich zugänglichen Datenbanken aufbereitet. Neben dem urheberrechtlichen Schutz von Datenbanken, deren Anordnung und Gestaltung eine entsprechende Schöpfungshöhe erreicht,[120] sind mit dem Datenbankherstellerecht sui generis[121] in Europa auch Investitionen in Datenbanken grundsätzlich geschützt. Dies bedeutet, dass die systematische Auswertung einer Datenbank von der Lizenzerteilung durch den jeweiligen Hersteller abhängen kann. Dies betrifft nur solche Datenbanken, deren Daten systematisch oder methodisch angeordnet sowie einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und ihre Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert.[122] Eine ggf. ungeordnete interne Datenablage ist unerheblich, wenn das Abfragesystem eine systematische oder methodische Ordnung herbeiführt.[123] Entscheidend ist die Verbindung eines Datenbestands mit einem Abfragesystem, das zielgerichtete Recherchen nach Einzelelementen in diesem Datenbestand ermöglicht.[124]

Die wesentliche Investition kann finanzieller Natur sein oder im Einsatz von Zeit, Arbeit und Energie bestehen.[125] Berücksichtigungsfähig sind z. B. Investitionen in die Aufbereitung des Datenbestandes, die Konzeption von Verknüpfungen und die Erarbeitung von Abfrageoptionen, nicht jedoch die zur Erzeugung der Daten selbst eingesetzten Mittel.[126] Geschützt sind nicht die in der Datenbank enthaltenen Informationen, denn der sui-generis-Schutz des Datenbankherstellers soll nicht zur Entstehung eines neuen Rechts an den einzelnen in der Datenbank gesammelten Elementen als solchen führen.[127] Hersteller ist, wer das wirtschaftliche Risiko trägt.

Der Hersteller kann für 15 Jahre ab Veröffentlichung die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Datenbank insgesamt oder nach Art/Umfang wesentlicher Teile untersagen. Dem steht die wiederholte und systematische Nutzung unwesentlicher Teile gleich, sofern „diese Handlungen einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen". Nach dem Investitionsschutzgedanken der Regelung sollen insbesondere Handlungen unterbunden werden, die die Amortisation der Investition in die Datenbank behindern könnten.[128] Beim Einsatz von Web-Harvesting-Methoden sollte daher zunächst geprüft werden, ob eine schutzfähige Datenbank vorliegt, wer als Hersteller einzuordnen ist und welche Lizenzbedingungen bestehen.

Betriebs- und Geschäftsgeheimnisse

Der Schutz von Betriebs- und Geschäftsgeheimnissen kann dann relevant werden, wenn Mobilitätsdaten weitere Informationen offenbaren wie Standorte oder Bewegungen von Unternehmens-Assets. Beispielsweise ist es einer Fitness-App gelungen, geheime Militärstandorte zu enthüllen.[129]

Mit der im Juli 2016 in Kraft getretenen europäischen Trade-Secrets-Richtlinie[130] werden gewisse Neuerungen im deutschen Rechtsrahmen umzusetzen sein. Danach ist ein Geschäftsgeheimnis definiert als:[131]

- geheim (nicht allgemein bekannt oder nicht ohne weiteres zugänglich),
- von kommerziellem Wert, weil geheim, und
- Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen.

Möchten nach der künftigen Rechtslage Beteiligte Daten als Betriebs- oder Geschäftsgeheimnisse schützen, wird ein Geheimhaltungsinteresse nicht bereits vermutet, sondern es müssen aktiv „angemessene" Geheimhaltungsmaßnahmen ergriffen werden. Sind Daten jedoch öffentlich zugänglich bzw. von jedermann erfassbar, dürften keine geheimen Daten vorliegen. Abgrenzungsprobleme könnten sich aber stellen, wenn zwar Einzeldaten allgemein erfassbar sind (wie z. B. der Standort eines Lieferfahrzeuges), die Daten(-sammlung) in ihrer Gesamtheit oder kontextuellen Zusammenstellung jedoch geheim ist (wie z. B. Standorte der gesamten Lieferkette).

Das Projekt ExCELL: Echtzeitanalyse und Crowdsourcing für eine selbstorganisierte City-Logistic

Ziel

Das Ziel des Forschungsvorhabens ist der Aufbau einer offenen und modularen Plattform, die Services mit einem Mobilitätsbezug für externe Entwickler anbietet. Als beispielhafte Anwendungen für kleine und mittlere Unternehmen werden auf der Plattform Terminplanungs- und Terminüberwachungslösungen für Handwerksbetriebe und Pflegedienste angeboten.

Herausforderungen

- Speicherung von Kundendaten (nur für den jeweiligen Betrieb zugänglich)
- Speicherung von Mitarbeiterdaten (nur für den jeweiligen Betrieb zugänglich)
- Tracking der Mitarbeiter während des Arbeitstages, um Verspätungen zu erfassen
- Nutzung von personenbezogenen Positionsdaten

Lösung

- Anonymisierung der personenbezogenen Positionsdaten
- Einholung eines Rechtsgutachtens
- Vorsehen der Möglichkeit, dass Tracking stets an- und ausgeschaltet werden kann

Fazit

Bei Betrieben ist große Skepsis in Bezug auf rechtliche Bedenken bei Datennutzung vorhanden, obwohl die Datennutzung meist unter Beachtung einiger Vorgaben möglich ist.

Datenschutz ist wichtig, klare rechtliche Regelungen erleichtern die Entwicklung. Die Nutzerakzeptanz steigt mit hohem Datenschutz und hoher Transparenz bei Datenauswertung und -speicherung.

5 Smart Video Analysis

Typische Datenquellen
- (Video-)Überwachung öffentlicher Räume

Durch den zunehmenden Verkehr kommt es in zahlreichen Städten auch zu einem Mangel an Parkplätzen. Dabei belastet die Parkplatzsuche nicht nur die Fahrer, sondern auch andere Verkehrsteilnehmer, Anwohner und die Umwelt. Die bedarfsgesteuerte Nutzung öffentlicher Räume sowie die Erhöhung der Sicherheit mittels intelligenter Analyse vorhandener Videoüberwachung im öffentlichen Raum könnte eine Stadt „smart“ machen, soweit die datenschutzrechtlichen Anforderungen erfüllt werden.

Potentiell relevante Rechtsgebiete
- Datenschutzrecht
- Bürgerliches Recht

Potentiell anzuwendende Regularien
- Datenschutzgrundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG-neu)
- Bürgerliches Gesetzbuch (BGB)

Typische Herausforderungen und Rechtsfragen
- Rechtskonforme Installation öffentlicher (Video-)Überwachung
- Wahrnehmung des Hausrechts in privaten Räumen
- Erfüllung von Informationspflichten
- Kompatibilitätstest bei zweckändernder Weiterverarbeitung
- Datenschutz-Folgenabschätzung bei hohem Risiko der Datenverarbeitung
- Gemeinsame Verantwortlichkeit bei unternehmensübergreifender Datenverarbeitung
- Auftragsdatenverarbeitung bei Datenauslagerung in die Cloud

Mögliche Lösungsansätze
- Anonymisierung
- Unkenntlichmachung (mit-)erfasster Personen
- Absenkung der Eingriffsintensität durch anlassbezogene (Video-)Überwachung
- Zertifizierung von Cloud-Anbietern

Die präsentierten Rechtsfragen stehen exemplarisch für den Anwendungsfall Videoanalyse und können – müssen aber nicht – in einzelnen Projekten des Technologieprogramms Smart Data - Innovationen aus Daten aufgetreten sein.

Was ist bei öffentlicher Videoüberwachung zu beachten?

Das Datenschutzrecht ist anwendbar, soweit bei der bildlichen Erfassung des öffentlichen Raums nicht durch technische Vorkehrungen die Anonymität der möglicherweise (mit-)aufgezeichneten Personen gewährleistet ist.[132] Dabei ist es unerheblich, ob die Erfassung von Personen eine lediglich unvermeidliche Nebenfolge des eigentlichen Einsatzzweckes ist.[133]

Legitimationsgrundlage

Die DS-GVO enthält keine spezifischen Vorgaben zugeschnitten auf die Besonderheiten der öffentlichen Videoüberwachung. Dagegen wurde mit § 4 BDSG-neu eine Vorschrift zur Videoüberwachung öffentlich zugänglicher Räume aufgenommen. Ob und in welchem Umfang diese Regelung aufgrund des Anwendungsvorrangs der DS-GVO einschlägig ist, muss für den jeweiligen konkreten Einzelfall entschieden werden.[134] Die Vorschrift führt die bisherige Regelung mit einem Stufenverhältnis aus Beobachten und Speichern sowie Verwenden fort.[135] Die Überwachung ist danach nur zulässig

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts, oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.

Die Videoüberwachung muss erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein besonders wichtiges Interesse kann der Schutz von Leben und Gesundheit sein, womit die Abwägungsentscheidung zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmaßnahme geprägt wird.[136] Die Tatsache der Überwachung ist kenntlich zu machen.

Nach Ansicht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder könnten nicht-öffentliche Stellen hingegen den Einsatz von Videoüberwachungsanlagen auf die Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f) VO (EU) 2016/679 (DS-GVO) stützen, mit den folgenden Prüfungskriterien:[137]

- Berechtigtes Interesse
- Erforderlichkeit
- Kein überwiegen der Betroffeneninteressen

Da für den letzten Punkt auch die subjektiven Erwartungen der betroffenen Person maßgeblich sind, kann es von entscheidender Relevanz sein, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.[138]

Datenschutzfreundliche Gestaltung

Durch intelligente Aufnahme- und Bildbearbeitungstechnik können Informationen herausgefiltert und zielgerichtet verarbeitet werden, sodass nur noch die durch Detektionsalgorithmen aus Bildern selektierten Inhalte gespeichert werden müssten.[139] Durch diese Abstraktion der Bilddaten kann die Persönlichkeitsrelevanz erhöht (wenn zur Identifikation individuellen Verhaltens eingesetzt wie bspw. Gesichtserkennung) aber auch gesenkt werden (wenn individualisierende Merkmale von vornherein herausgefiltert werden). So könnte die Eingriffstiefe für (mit-)erfasste Personen gesenkt werden, wenn erst ein detektiertes Abweichen vom Normalverhalten (wie bspw. ein Sturz) eine gezielte Videoüberwachung auslöst.[140] Soweit darüber hinaus Daten nur ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisgewinn gelöscht werden, könnte (je nach Umständen) ein Grundrechtseingriff vermieden oder zumindest abgemildert werden.[141] Darüber hinaus sollte bereits bei der Beschaffung von Videotechnik im Sinne des Privacy-by-Design auf „eingebauten Datenschutz“ geachtet werden, und nicht erforderliche Funktionalitäten, die den Eingriff in die Grundrechte der Betroffenen intensivieren könnten, sollten nicht unterstützt oder

deaktiviert werden. Eine Speicherung ist nur bis zur Zweckerreichung zulässig, danach muss das Material gelöscht werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder empfiehlt 48 Stunden.[142]

Informationspflichten

Soweit sich die Transparenzanforderungen nach der DS-GVO richten, sind mindestens folgende Angaben gut sichtbar kenntlich zu machen:[143]

- Umstand der Beobachtung,
- Name und Kontaktdaten des Verantwortlichen,
- soweit vorhanden Kontaktdaten des Datenschutzbeauftragten,
- Zwecke und Rechtsgrundlage der Verarbeitung,
- Angabe des berechtigten Interesses,
- soweit eine Übermittlung erfolgt, die Empfänger oder Kategorien von Empfängern der Daten,
- Speicherdauer,
- Hinweis auf Auskunfts-, Lösch-, Widerspruchs- und Beschwerderecht.

Wann ist eine Zweckänderung zulässig?

Das Zweckbindungsprinzip stellt derzeit einen der Grundpfeiler des Datenschutzrechts dar.[144] Es setzt sich aus zwei Komponenten zusammen: der Festlegung eines bestimmten Zwecks sowie der grundsätzlichen Bindung an diesen einmal gewählten Zweck.[145] Um den Zielen des Datenschutzrechts zu genügen, dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden.[146] Die Zweckfestlegung ist Bemessungsgrundlage für die Feststellung der Rechtsmäßigkeit sowie Erforderlichkeit im Rahmen der Datenminimierung und Speicherbegrenzung. Zur Gewährleistung von Transparenz und Kontrollierbarkeit sollte die Zweckbestimmung unmissverständlich, einschätzbar und nachvollziehbar sein. So bestimmt der angegebene Zweck beispielsweise die Reichweite einer erteilten Einwilligung oder bildet die Grundlage für eine Interessenabwägung.

Die Bedeutung von Zweckbestimmung und Zweckbindung hängen entscheidend vom Risiko der Datenverarbeitung für die Betroffenen ab.[147] Je schwerer der Eingriff in die Privatsphäre ausfällt, desto konkreter sollte die Festlegung der Zweckbestimmung sein.[148] Sollen Daten zu einem anderen Zweck weiterverwendet werden als zum ursprünglichen Erhebungszweck, darf dieser nicht unvereinbar mit dem ursprünglichen Zweck sein.[149] Um zu prüfen, ob Unvereinbarkeit vorliegt, sind insbesondere die folgenden Aspekte zu berücksichtigen (Kompatibilitätstest):[150]

- Verbindungen zwischen altem und neuem Zweck
- Erhebungszusammenhang
- Verhältnis zwischen Verantwortlichem und Betroffenem
- Art der personenbezogenen Daten
- Vorliegen besonderer Kategorien personenbezogener Daten
- Vorliegen strafrechtsrelevanter Daten
- Mögliche Folgen der Weiterverarbeitung für die Betroffenen
- Einsatz geeigneter Schutzmaßnahmen wie Verschlüsselung und Pseudonymisierung

Diese Liste ist nicht abschließend. Daneben kann eine (erneute) Einwilligung des Betroffenen oder eine spezielle, gesetzliche Rechtsvorschrift eine Zweckänderung ermöglichen.[151] Ist der neue Zweck mit dem ursprünglichen vereinbar, soll nach Erwägungsgrund 50 Satz 2 hingegen keine „andere gesonderte“ Rechtsgrundlage erforderlich sein.[152] Mit Verweis auf die Entstehungsgeschichte der DS-GVO und grundrechtliche Verbürgung des Zweckbindungsprinzips wird hingegen gefordert, dass eine Weiterverarbeitung zu neuen Zwecken wie nach der bisherigen Rechtslage nur nach der Zwei-Stufenprüfung aus Kompatibilitätstest und zusätzlichem Eingreifen einer Rechtsgrundlage zulässig sein soll.[153]

Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt nicht als unvereinbar mit den ursprünglichen Zwecken, soweit diese in Übereinstimmung mit Art. 89 Abs. 1 DS-GVO erfolgen. Danach müssen Schutzmaßnahmen sicherstellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Soweit die Weiterverarbeitung die Identifizierung nicht erfordert, müssen Daten anonymisiert werden.[154]

Betroffene müssen über eine Zweckänderung gesondert informiert werden.[155]

In Bezug auf die Weiterverarbeitung gespeicherter Daten aus der Videoüberwachung durch öffentliche Stellen enthält § 4 Abs. 3 S. 3 BDSG-neu eine Einschränkung: Diese Daten dürfen für einen anderen Zweck nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Wann muss eine Datenschutz-Folgenabschätzung durchgeführt werden?

Bei solchen Datenverarbeitungen, die voraussichtlich ein hohes Risiko für die Grundrechtsausübung der betroffenen Bürger mit sich bringen werden, müssen die potentiellen Folgen vorab erfasst und bewertet sowie ggf. kompensierende Schutzmaßnahmen ergriffen oder die Datenschutzaufsichtsbehörden informiert werden. Ob eine Datenschutz-Folgenabschätzung durchzuführen ist, ergibt sich aus einer sogenannten „Schwellwertanalyse“, d. h. einer Abschätzung der Risiken der Verarbeitungsvorgänge. Diese Bewertung ist schriftlich zu dokumentieren. Die DS-GVO nennt einige Fälle, in denen die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist. Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche zählt zu diesen Fällen.[156] Die Aufsichtsbehörden sollen zudem Positiv- und Negativlisten aufstellen. Bei einer Folgenabschätzung müssen mindestens folgende Schritte befolgt werden:

- Systematische Beschreibung der geplanten Verarbeitungsvorgänge und verfolgten Zwecke
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug zum verfolgten Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Planung geeigneter Abhilfemaßnahmen zur Risikobewältigung wie Schutzvorrichtungen und Sicherheitsmaßnahmen.

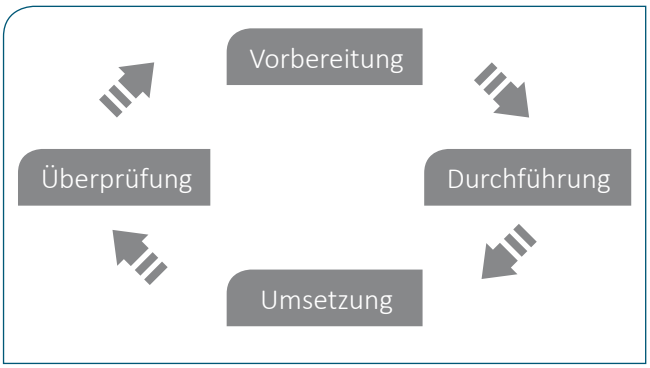


Abbildung 1: Orientierung der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Durchführung einer Datenschutz-Folgenabschätzung

Dabei gilt zu beachten, dass die Datenschutz-Folgenabschätzung kein einmaliger Vorgang ist, sondern bei Änderung des Verarbeitungsverfahrens, Auftreten neuer Risiken oder Änderung der Risikobewertung wiederholt und angepasst werden sollte. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder empfiehlt einen iterativen Prozess:[157]
Bei der Vorbereitung sollte das idealerweise interdisziplinäre Team zusammengestellt, eine Prüfplanung erarbeitet, der Beurteilungsumfang festgelegt, die relevanten Akteure und Betroffenen identifiziert, die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitungs-

vorgänge bezogen auf den Zweck bewertet sowie die einschlägige Rechtsgrundlage identifiziert werden. Bei der Durchführung sollten die Risikoquellen modelliert, eine Risikobeurteilung durchgeführt und eine Auswahl geeigneter Abhilfemaßnahmen getroffen werden sowie ein Bericht erstellt werden. Die Umsetzung der Abhilfemaßnahmen sollte auch einen Test der Wirksamkeit enthalten sowie eine Dokumentation zum Nachweis der Einhaltung der DS-GVO. Erst dann sollte eine Freigabe der Verarbeitungsvorgänge erfolgen. Zur Sicherstellung der ordnungsgemäßen Durchführung der Datenschutz-Folgenabschätzung kann es sinnvoll sein, den Bericht von einem unabhängigen Dritten überprüfen zu lassen. Die Notwendigkeit einer erneuten Durchführung muss während der gesamten Dauer der Verarbeitungsvorgänge fortlaufend überwacht werden.

Geht aus der Folgenabschätzung hervor, dass ein hohes Risiko besteht, muss die Aufsichtsbehörde konsultiert werden.[158] Die Behörde kann Empfehlungen aussprechen bis hin zum Verbot, wenn die geplante Datenverarbeitung gegen die DS-GVO verstoßen würde.[159]

Das Projekt VIRTUOSE-DE: Service-Plattform für echtzeitfähige Big-Data-Videoanalyse und -verarbeitung in der Cloud

Die Ziele des Projekts VIRTUOSE-DE liegen in der Schaffung eines intelligenten Parkraummanagements sowie der Steigerung der Sicherheit im öffentlichen Personennahverkehr (ÖPNV). Zur Erreichung dieser Ziele soll eine Service-Plattform für echtzeitfähige Big-Data-Videoanalyse und -verarbeitung in der Cloud geschaffen werden und für die Anwendungsfälle Parkraummanagement sowie video-basierte Sicherheit im ÖPNV genutzt werden.

Die Herausforderungen lagen generell in der Erfassung persönlicher Daten durch Videotechnik (Autokennzeichen, Personen, Gesichter, etc.). Hinzu kommt, dass zunächst die rechtlichen Grundlagen aufgefunden werden müssen, die eine Videoüberwachung im öffentlichen Raum und in Fahrzeugen des ÖPNV legitimieren. Hieraus entsteht Unsicherheit bei potentiellen Anwendern.

Juristische Themen sind aufgrund hoher Anforderungen an den Datenschutz herausfordernd. In Fahrzeugen dürfen nur elektronische Systeme mit speziellen Zulassungen und Zertifizierungen zum Einsatz kommen. Daraus resultieren große Hürden bei der Umsetzung (Datenschutz, rechtliche Sicherheit, etc.).

Die Lösung: Da die Verarbeitung der Fahrzeugkennzeichen nicht für den Anwendungsfall Parkraummanagement erforderlich ist, werden z. Z. Verfahren untersucht, um vor der Weiterverarbeitung der Bilder die Kennzeichen unkenntlich zu machen, z. B. durch Verpixelung. Außerdem sind Gespräche mit dem Sicherheitsbeauftragten und Betriebsrat geplant, in denen Maßnahmen abgeleitet werden, die den Schutz personenbezogener Daten sicherstellen.

Empfehlungen

- Effektive Informations- und Kommunikationspolitik (Flyer, Prospekte, etc.)
- Einbindung Datenschützer (Bund/Länder/Anwender/involvierte Parteien)

Fazit

- Bestehende Rechtsunsicherheit ist Hemmschwelle und wirkt akzeptanzhindernd.
- Die Einbindung von Datenschutzexperten und juristischen Instanzen ist nicht nur hilfreich, sondern unverzichtbar.

6 Smart Health

Typische Datenquellen
- Sensoren medizinischer Geräte
- Krankenhausinformationssysteme
- Patienten
- Medizinisches Personal
- Krankenkassen

Der Operationssaal ist das Herz eines Krankenhauses, da dort wichtige klinische, patientenbezogene und administrative Prozesse zusammenlaufen. Eine stärkere Vernetzung für Krankenhäuser, Klinikpersonal und Patientinnen und Patienten bietet das Potenzial, einen reibungslosen Betrieb zu gewährleisten, und die vielfältigen Prozesse ideal aufeinander abzustimmen. Auf der anderen Seite birgt die Digitalisierung bisher analog betriebener Prozesse und die Vernetzung über bisherige Systemgrenzen hinaus oftmals Datenschutzrisiken. Im medizinischen Kontext stellen sich nicht nur Fragen der datenschutzrechtlichen Zulässigkeit. Als besondere Kategorie personenbezogener Daten unterliegen Gesundheitsdaten ebenso wie genetische und biometrische Daten einem besonderen Schutz der Datenschutzgrundverordnung. Daneben verbietet § 203 Strafgesetzbuch die Offenlegung von Patientendaten ohne deren Einverständnis.

Potentiell relevante Rechtsgebiete
- Datenschutzrecht
- Medizinrecht
- Strafrecht

Potentiell anzuwendende Regularien
- Datenschutzgrundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG-neu)
- Landesdatenschutzgesetze
- Landeskrankenhausgesetze
- Sozialgesetzbuch (SGB V)
- Gesetz über Medizinprodukte (MPG)
- Strafgesetzbuch (StGB)

Typische Herausforderungen und Rechtsfragen
- Anwendbarkeit Datenschutzrecht
- Besonderheiten Gesundheitsdaten
- Arbeitnehmerdatenschutz
- Zweckvereinbarkeit bei Weiterverarbeitung zu neuen Zwecken
- Strafbarkeit bei Offenbarung von Privatgeheimnissen
- Sicherheitsanforderungen und Produktzulassungsregelungen bei Medizinprodukten

Mögliche Lösungsansätze
- Anonymisierung
- Datenminimierung durch Pseudonymisierung, Generalisierung und Randomisierung
- Technisch-organisatorische Maßnahmen
- Datenzugriffs- und Datennutzungskontrolle (Access und Usage Control)

Die präsentierten Rechtsfragen stehen exemplarisch für den Anwendungsfall Gesundheit und können – müssen aber nicht – in einzelnen Projekten des Technologieprogramms Smart Data - Innovationen aus Daten aufgetreten sein.

Wie sind Gesundheitsdaten geschützt?

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.[160]

Gesundheitsdaten geschützt als besondere Kategorien personenbezogener Daten

Gesundheitsdaten zählen zu den „besonderen Kategorien personenbezogener Daten", deren Verarbeitung zunächst verboten ist.[161] Ausnahmen von diesem Verbot enthält Art. 9 Abs. 2 DS-GVO, wobei hier oftmals Konkretisierungen im mitgliedstaatlichen Recht vorgenommen werden müssen. Die DS-GVO sieht grundsätzlich die Möglichkeit vor, dass betroffene Personen in die Verarbeitung einwilligen, wobei diese Möglichkeit durch Unionsrecht oder das Recht der Mitgliedsstaaten aufgehoben werden kann. Spezifische gesetzliche Erlaubnistatbestände können sich beispielsweise auf die Umsetzung des Arbeits- und Sozialschutzes, der Gesundheitsvorsorge, erhebliche öffentliche Interessen oder Archivierung und Forschung beziehen. Aufgrund der föderalen Struktur des Datenschutzrechts in Deutschland führt dies je nach Kontext dazu, dass Bundes- oder Landesdatenschutzrecht anwendbar sein kann. Daraus resultiert gerade für institutionsübergreifende Forschungsprojekte eine gewisse Rechtsunsicherheit. Da die Fragmentierung des Rechtsrahmens auch die praktische Umsetzung erschwert, sollte die Datenschutzgrundverordnung als Anlass genutzt werden, die bisher verstreuten Normen zugunsten eines einheitlichen Regelungsregimes für Forschung mit Gesundheitsdaten zu überarbeiten. Eine einheitliche Regulierung könnte durch einen Bund-Länder-Staatsvertrag erreicht werden.[162]

Einwilligung

Soll die Datenverarbeitung über die Einwilligung der Patientinnen und Patienten erfolgen, stellt sich oftmals folgendes Problem: Wissenschaftlich zu erforschende Fragestellungen können im Vorfeld eines Forschungsvorhabensoft nicht abschließend definiert werden, Einwilligungserklärungen dürfen aber nicht zu unbestimmt formuliert sein. Abhilfe könnten hier neue Konzepte der Einwilligung wie zum Beispiel ein zweistufiges Bewilligungsprinzip bieten, bei dem sich betroffene Personen damit einverstanden erklären, dass ihre Daten in eine Datenbank aufgenommen werden und eine bestimmte vertrauenswürdige Stelle später entscheidet, welche Forschungsprojekte Zugriff auf die Daten erhalten dürfen.[163] Daneben könnten gestufte Einwilligungsformulare, bei der Betroffene zwischen einem sehr spezifischen Forschungsprojekt bis hin zu einer weiten Erlaubnis für Forschungsrichtungen wählen können das notwendige Bewusstsein über Reichweite und die Freiwilligkeit bei der Entscheidung sicherstellen.[164]

☒ Ich willige in die Teilnahme an Studie XY ein.

☐ Ich willige darüber hinaus ein, dass meine Daten nach Abschluss der Studie für Forschungsprojekte zum Krankheitsgebiet XY genutzt werden.

☐ Ich willige darüber hinaus ein, dass meine Daten auch für weitere medizinische Forschungsprojekte verwendet werden.

Abbildung 2 Vereinfachtes Beispiel einer gestuften Einwilligungserklärung

Anonymisierung

Werden Patientendaten wirksam anonymisiert, bestehen grundsätzlich keine datenschutzrechtlichen Beschränkungen. Hierbei gilt jedoch zu bedenken, dass bei individuellen Körpermerkmalen und Krankheitsver-

läufen besonderes Augenmerk auf sehr hohe Re-Identifizierungsrisiken zu legen ist. Je nach Fallkonstellation kann eine Anonymisierbarkeit gänzlich ausgeschlossen sein. Der Einsatz von Anonymisierungstechniken könnte jedoch im Sinne der Datenminimierung die Risiken für die Betroffenen senken.

Wann droht Strafbarkeit für Berufsgeheimnisträger?

Angehörige von Heilberufen wie Ärzte, Krankenhauspersonal oder Apotheker unterliegen der sogenannten „ärztlichen Schweigepflicht". Das unbefugte Offenbaren von Patientendaten ist strafbar (§ 203 StGB). Sollen Daten aus dem medizinischen Kontext durch IT-Experten analysiert werden, bedurfte es bisher zunächst einer Offenbarungsvereinbarung mit dem Patienten.

Aufgrund der zunehmenden Digitalisierung erfolgte mit der Anpassung des § 203 StGB (Verletzung von Privatgeheimnissen) jüngst eine wesentliche gesetzliche Änderung.[165] So sollen auch IT-Dienstleister in den Geheimbereich einbezogen werden, wenn die Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen erforderlich ist. Dann liegt keine Offenbarung vor und die externen IT-Dienstleister unterliegen ebenfalls der Schweigepflicht. Für die Einbeziehung muss die „mitwirkende Person" unmittelbar mit der beruflichen Tätigkeit der schweigepflichtigen Person, ihrer Vorbereitung, Durchführung, Auswertung und Verwaltung befasst sein.[166] Als Beispiele solcher Tätigkeiten werden in der Gesetzesbegründung u.a. genannt:

- Einrichtung, Betrieb, (Fern-)Wartung und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art, beispielsweise auch von entsprechend ausgestatteten medizinischen Geräten,
- Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten.

Die rechtliche Herausforderung wird darin bestehen zu bestimmen, wann ein Einsatz externer Dienstleister „erforderlich" ist und wann nicht.[167]

Berufsgeheimnisträger müssen dafür Sorge tragen, dass mitwirkende Personen wie IT-Dienstleister sowie deren Mitarbeiterinnen und Mitarbeiter oder Subunternehmer sich zur Geheimhaltung verpflichten. Insoweit entscheidend ist eine lückenlose Vertragskette zwischen Berufsgeheimnisträger und den tätig werdenden Personen, die Kenntnis von den geschützten Daten erlangen könnten.

Wann gilt Software als Medizinprodukt?

Zum Schutz der Gesundheit von Patienten, Anwender und Dritten unterliegen Medizinprodukte den Vorgaben des Medizinproduktegesetz (MPG). Danach müssen spezifische medizinprodukterechtliche Sicherheitsanforderungen und Produktzulassungsregelungen beachtet werden. Auch Software kann gemäß § 3 Nr. 1 S. 1 MPG zu den Medizinprodukten zählen, soweit deren Funktion dazu bestimmt ist einem der folgenden Zwecke zu dienen:

- der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
- der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
- der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder
- der Empfängnisregelung.

Das Projekt InnOPlan: Innovative, datengetriebene Effizienz OP-übergreifender Prozesslandschaften

Ziel

InnOPlan entwickelt auf Basis von Big-Data-Technologien eine Smart-Data-Plattform für medizintechnische Geräte rund um den OP. Neuartige Anwendungen auf der Smart-Data-Plattform sollen durch Prognosen der OP-Abläufe und durch eine Teilautomatisierung der OP-Dokumentation die Koordination verbessern und Kosten im Krankenhaus senken.

Herausforderungen bestanden in der rechtssicheren Verwendung von Daten aus den medizintechnischen Geräten und möglicherweise Verknüpfung mit Daten aus dem Krankenhausinformationssystem.

Die technische Lösung fokussiert allein auf Daten von medizintechnischen Geräten. Die Smart-Data-Plattform ist eine Datenhaltungs-, Analyse- und Bereitstellungsinfrastruktur für diese Art von Daten. Die Infrastruktur wird von zwei Referenzapplikationen genutzt.

Die rechtliche Lösung besteht aus der Vermeidung von unmittelbar personenbezogenen Daten und damit bei der Verarbeitung verbundenen rechtlichen Regelungen im Rahmen der Smart Data Plattform. Für Forschungszwecke wurden darüber hinaus auch anonymisierte Daten aus dem Krankenhausinformationssystem analysiert.

Empfehlungen

Rechtliche Regelungen zum Datenschutz, die momentan im Rahmen der EU-Datenschutz-Grundverordnung weiter verschärft werden, stehen möglicherweise einer rechtssicheren Verwertung auf Big-Data-Basis entgegen. Im Sinne der Förderung von neuen datenbasierten Geschäftsmodellen verschafft das deutschen Firmen möglicherweise einen Wettbewerbsnachteil im internationalen Vergleich.

Fazit

Gerade im deutschen Gesundheitswesen ist das Potenzial für die Nutzung der Chancen der Digitalisierung enorm. Bislang existieren in typischen Krankenhäusern viele unterschiedliche Datenbanken. Insbesondere eine integrierte Sicht von historischen Gesundheitsdaten würde viele Möglichkeiten für die Gewinnung von neuartigen Erkenntnissen bieten. Organisatorische Hürden in Krankenhäusern und rechtliche Hürden stehen dieser Art von Wissensgewinnung jedoch oftmals entgegen. Aktuelle Lösungen beschränken sich deshalb oft auf einzelne Datenquellen und auf nicht-personenbezogene Daten.

7 Smart Energy

Typische Datenquellen
- Energiemessstellen
- Umweltdaten
- Energiemarkt
- Netzzustandsdaten

Intelligente Datenanalyse gewinnt auch im Bereich der Energieoptimierung eine immer stärkere Bedeutung. Für Teilnehmer am Energiesystem ist zunächst das informationelle Unbundling nach dem Energiewirtschaftsgesetz zu beachten, um den diskriminierungsfreien Zugang zu Informationen des Netzbetriebs und damit gleiche Wettbewerbschancen der Teilnehmer am Energiemarkt zu gewährleisten. Diese Entflechtungsregelungen tragen dem Umstand Rechnung, dass es sich bei dem Energienetz um ein natürliches Monopol handelt. Daneben sind im Rahmen der Digitalisierung der Energiewende Sektor-spezifische Datenschutz- und IT-Sicherheitsrechtliche Anforderungen geschaffen worden.

Potentiell relevante Rechtsgebiete
- Energierecht
- Datenschutzrecht
- IT-Sicherheitsrecht

Potentiell anzuwendende Regularien
- Energiewirtschaftsgesetz (EnWG)
- Datenschutzgrundverordnung (DS-GVO)
- Messstellenbetriebsgesetz (MsbG)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (KritisV)

Typische Herausforderungen und Rechtsfragen
- Anwendbarkeit Datenschutzrecht
- Bereichsspezifische Datenschutz- und Datensicherheitsanforderungen für Energiedaten
- Informationelles Unbundling
- Besondere IT-Sicherheitsanforderungen für kritische Infrastrukturen

Mögliche Lösungsansätze
- Anonymisierung, Datenaggregation
- Vereinbarungen zur IT-Sicherheit

Die präsentierten Rechtsfragen stehen exemplarisch für den Anwendungsfall Energie und können – müssen aber nicht – in einzelnen Projekten des Technologieprogramms Smart Data - Innovationen aus Daten aufgetreten sein.

Welche Datenschutzvorgaben aus dem Energierecht müssen beachtet werden?

Die Datenkommunikation in intelligenten Energienetzen unterliegt besonderen Datenschutz- und Datensicherheitsanforderungen nach dem Messstellenbetriebsgesetz (MsbG). Nach der Konzeption des MsbG dürfen personenbezogene Daten nur von sogenannten „berechtigten Stellen" verarbeitet werden. Stellen, die im Gesetz nicht benannt sind, bedürfen der Einwilligung des Anschlussnutzers. Sämtliche Daten aus Messsystemen und Messeinrichtungen dürfen nur mit Einwilligung des Anschlussnutzers oder zu einem der im Gesetz abschließend benannten Zwecke erfolgen. Diese Regelung gilt explizit sowohl für personenbezogene, personenbeziehbare und nicht-personenbezogene Daten.[168] Daneben enthält das Gesetz spezifische IT-Sicherheitsanforderungen.

Ab dem 25. Mai 2018 genießt die DS-GVO zwar grundsätzlich Anwendungsvorrang vor nationalen Datenschutzregelungen in ihrem sachlichen und räumlichen Anwendungsbereich.[169] Jedoch enthält die DS-GVO eine Vielzahl von Öffnungsklauseln, die mitgliedstaatliche Regelungen ermöglichen oder sogar erfordern.[170] Danach stellt sich die Frage, ob das MsbG neben der DS-GVO anwendbar bleiben wird. Die Mitgliedstaaten dürfen u. a. spezifischere Anforderungen und Präzisierungen zur Bestimmung erlassen, wann eine Datenverwendung im Rahmen einer rechtlichen Verpflichtung oder zur Wahrnehmung einer öffentlichen Aufgabe rechtmäßig sein soll.[171] Da Einbau und Betrieb einer Messstelle bestimmten Verpflichteten zugewiesen werden,[172] könnte das MsbG in den Anwendungsbereich dieser Öffnungsklausel fallen. Daneben handelt es sich bei der Energieversorgung um einen Bereich der Daseinsvorsorge, sodass ein öffentliches Interesse an der Durchführung eines intelligenten und effizienten Messstellenbetriebs bestehen dürfte.[173]

Jedoch könnte die abschließende Beschränkung auf vorab festgelegte Zwecke im Widerspruch zur Tragweite der von DS-GVO vorgesehenen Legitimationstatbestände stehen, die die Möglichkeit einer Interessenabwägung im Einzelfall vorsehen (jedoch nicht für Behörden). Damit soll den widerstreitenden, auch grundrechtlich geschützten Interessen an Durchführung bzw. Ausschluss der Verarbeitung Rechnung getragen werden.

Welche Besonderheiten gelten für Betreiber Kritischer Infrastrukturen?

Betreiber Kritischer Infrastrukturen trifft nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) die besondere Pflicht, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.[174] Angeregt wird der Vorschlag branchenspezifischer Sicherheitsstandards. Zudem obliegt den Betreibern kritischer Infrastrukturen die regelmäßige Nachweispflicht.

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.[175] Näheres ist in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) geregelt; für den Sektor Energie sind die Schwellenwerte zu beachten. Für den Sektor Transport soll eine Bestimmung in der BSI-KritisV im Jahr 2017 erfolgen.[176]

Soweit das BSIG anwendbar ist, müssen kritische Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht. Das im Einzelfall erforderliche Sicherheitsniveau ist somit relativ anhand einer Risikoabwägung zu bestimmen.

Bedienen sich Betreiber Kritischer Infrastrukturen externer Dienstleister zur Datenverarbeitung, könnten die Anforderungen des § 8a BSIG für diese mittelbare Wirkung entfalten.[177] Welche einzelnen Verpflichtungen externe IT-Dienstleister treffen, sollte daher im Einzelnen vertraglich festgelegt werden.

Das Projekt Smart Energy Hub: Datendrehscheibe für intelligente Energienutzung

SmartEnergyHub

Ziel

Das Projekt Smart Energy Hub widmete sich der Entwicklung einer Smart Data-Plattform für das prognose- und marktbasierte Energiemanagement von Infrastrukturbetreibern auf Basis von Sensordaten.

Herausforderung

Zur Optimierung des Lastverschiebepotentials von wichtigen und teilweise Kritischen Infrastrukturen wie Flughäfen, Seehäfen, Industrie- und Chemieparks, Fabriken und Fertigungsanlagen oder Bürogebäude mussten Daten aus Sensoren und externen Quellen wie dem Energiemarkt oder Wetterprognosen intelligent zusammengeführt und ausgewertet werden.

Die Datenkommunikation erfolgt mit gesicherten Webserviceschnittstellen, so dass alle Datenzugriffe autorisiert sind. Die vom Pilotanwender, dem Flughafen Stuttgart, bereitgestellten Daten über Fluggastaufkommen und Energieverbrauch sind nicht personenbezogen, da keine Rückschlüsse auf einzelne, identifizierbare Personen möglich sind. Herausforderungen bezüglich rechtlicher Aspekte sowie datenschutzrechtliche Implikationen waren in diesem Projekt daher nicht gegeben.

Lösung

Im Projekt erfolgte die Entwicklung eines IT-Toolkits für Infrastrukturbetreiber, welches in der Lage ist, die bestehenden Systeme und bereits erfasste Daten des Infrastrukturbetriebes zu integrieren.

Im Rahmen von „SmartEnergyHub“ wurden IT-Lösungen in einer cloudbasierten Architektur entwickelt und umgesetzt, die es ermöglichen, das komplette Energiemanagement für Betreiber unter Berücksichtigung der dezentraleren Energiesystemstruktur in einem mandantenfähigen System zu optimieren. In der zukünftigen Energiewelt steigt die Bedeutung einer aktiven Teilnahme am Energiemarkt im Zuge eines integrierten Energiemanagements für alle Akteure.

8 Ausblick: Sicheres Datenmanagement

Das Projekt EDV: Einfaches Digitales Vergessen

Ziel

Das Projekt EDV begann im Juni 2017 mit der Entwicklung einer Lösung zum selbstbestimmter Austausch von sensiblen Daten für Unternehmen. Mögliche Kernanwendungsfälle bilden der Austausch von sensiblen Projekt- oder Produktinformationen zwischen Unternehmen sowie das Einbinden von EDV in einen digitalen Bewerbungsprozess zum sicheren und gesetzeskonformen Austausch von Unterlagen.

Herausforderung

In Unternehmen erfolgt der Austausch von sensiblen Informationen wie Projektergebnissen, Informationen zur Geschäftsstrategie oder auch Bewerbungsunterlagen zunehmend per E-Mail oder über externe Speicherbereiche wie Cloud-Lösungen. Allerdings sollen diese Informationen häufig nur temporär oder in einem bestimmten Kontext verfügbar sein, um die Gefahr des Missbrauchs oder der unabsichtlichen Weitergabe der Daten im Unternehmen zu verringern.

Sensible Daten stehen jedoch oft dem Empfänger auch nach Ablauf von gesetzlichen Fristen oder vertraglich geregelten Gültigkeitszeiträumen zur Verfügung. Der Sender von Daten muss bei dem Versand einen Kontrollverlust über die Informationen hinnehmen. Nach dem Verschicken beispielsweise von Dokumenten besteht keine Möglichkeit mehr, die Zugriffsrechte des Empfängers zu verändern, also zu entziehen oder zu erweitern. Der Empfänger von sensiblen Daten ist ohne weiteres in der Lage, empfangene Daten (auch unabsichtlich) an Unbefugte weiterzuleiten. Daneben werden sensible Daten oft über unverschlüsselte Kanäle oder ungesicherte Systeme ausgetauscht, sodass ein Abfangen der Informationen von Unbefugten relativ einfach möglich ist. Bei vielen Datenaustauschverfahren (zum Beispiel Emails ohne digitale Signatur) ist es nicht möglich, die Identität des Absenders zu überprüfen. Viele gängige Datenaustauschverfahren sind jedoch nicht in bestehende IT-Systeme integrierbar.

Lösung

Das Projekt EDV entwickelt ein aus Soft- und Hardwarekomponenten bestehendes System, das einen selbstbestimmten Austausch sensibler Informationen sowie ein automatisches Löschen von Daten ermöglicht. Die eingesetzte Software soll einen sicheren Datenaustausch gewährleisten. So können durch eine Ende-zu-Ende-Verschlüsselung die übertragenen Daten auf Senderseite verschlüsselt und beim Empfänger wieder entschlüsselt werden.

Mit der Software-Lösung des Projekts EDV behält der Sender auch nach dem Versenden die Kontrolle über seine Daten. Auf diese Weise können Nutzungsrechte beispielsweise auch nachträglich geändert oder entzogen sowie Daten nach Ablauf einer bestimmten Frist gelöscht werden. Anwendungsbeispiele sind etwa digitale Bewerbungsunterlagen oder Zugriffsrechte bei Projektarbeiten, die nach einer festgelegten Frist entzogen werden.

EDV verhindert, dass nach dem Ablauf von Fristen beziehungsweise dem Überschreiten eines Zugriffsdatums der Empfänger die Daten einsehen und bearbeiten kann. Nach dem Versenden von Daten behält der Absender durch EDV die Möglichkeit, Zugriffsrechte des Empfängers zu verändern. Eine versehentliche oder unbeabsichtigte Weiterleitung von Daten an Unbefugte wird verhindert. EDV bietet den Nutzern eine Ende-zu-Ende Verschlüsselung, so dass Daten in lesbarer Form nur beim Absender und beim berechtigten Empfänger vorliegen. Darüber hinaus stellt EDV sicher, dass der Empfänger der Daten die Authentizität des Absenders überprüfen kann. Dabei soll der sichere

Datenaustausch durch eine einfach zu benutzende Software und unkomplizierte Integrationsmöglichkeiten in bestehende Datenaustauschprozesse gefördert werden. Das System wird durch offene Schnittstellen und ggf. durch Plugin-Konzepte die Integration in bestehende Softwaresysteme und Prozesse ermöglichen.

Fazit

Die erhöhte Sicherheit kann die Bereitschaft steigern, sensible Dokumente und Informationen digital auszutauschen.

Die Fachgruppe Rechtsrahmen – Key Findings

PD. Dr. iur. Oliver Raabe, Manuela Wagner, Karlsruher Institut für Technologie

Von Big zu Smart Data

Ausgehend von den typisierenden Phänomenen Volume, Variety und Velocity zeigen sich bei Big Data Konfliktlagen unterschiedlichen Ausmaßes zu allen Grundprinzipien des Datenschutzrechts, wie sie nun in Art. 5 DS-GVO kodifiziert vorliegen. So verstößt eine Datenhaltung auf „Vorrat" ohne konkretes Verwendungsziel dem Gedanken, dass personenbezogene Daten in quantitativer, qualitativer und zeitlicher Dimension stets zu einem bestimmten Zweck erhoben werden und sich auf das für die Zweckerreichung erforderliche Mindestmaß beschränken (Grundsatz der Datenminimierung, Zweckbindung und Speicherbegrenzung). Explorative Analysen, bei denen der Zweck der Verarbeitung sich erst aus den Erkenntnissen einer zunächst durchzuführenden, ergebnisoffenen Analyse ergeben soll, erscheinen unvereinbar mit dem Zweckbindungsgrundsatz. Zudem können eine Vielzahl von Akteuren und Verwendungskontexten Transparenz und Kontrolle gefährden.[178] Ein Verzicht auf diese Grundpfeiler des bestehenden Gesamtsystems, welches mit der Datenschutzgrundverordnung fortgeführt wird, wäre ohne die Entwicklung neuer Schutzkonzeptionen mit den Grundrechten der EU-Grundrechte-Charta (Art. 7, 8 EU-GrCh) und dem Grundgesetz (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) unvereinbar.

Aus datenschutzrechtlicher Perspektive lassen sich als wesentliche Unterschiede und Vorteile von „Smart Data" gegenüber dem Phänomen „Big Data" die Selektion „wertvoller" Inhalte anstelle der Sammlung bloßer Masse, die zielgerichtete Auswertung und Anwendung anstelle explorativer Analysen, sowie der Einsatz von Schutzmaßnahmen wie beispielsweise die Option der frühestmöglichen Anonymisierung oder Pseudonymisierung, der technische Datenschutz mittels Datennutzungskontrolle, oder Privacy-Preserving-Data-Mining nennen.[179]

Mit der DS-GVO kamen einige Veränderungen auf die laufenden Forschungsprojekte des Programmes zu. An dieser Stelle möchten wir kurz die Innovationen und Vorteile hervorheben. So führt die europaweite Harmonisierung mit der Verschärfung der Sanktionen und der Ausweitung des Anwendungsbereichs mit dem sogenannten „Marktortprinzip" zu einer gewissen Wettbewerbsgleichheit, da sich gerade internationale Player den Datenschutzvorschriften nicht mehr so einfach entziehen können wie bisher. Die Datensouveränität der Nutzer wird durch strenge Transparenzanforderungen, neue Konzepte wie der Datenportabilität sowie dem sogenannten „Kopplungsverbot" gestärkt, wodurch Anreize in die Entwicklung technischer Lösungen gesetzt werden. Den durchaus unterschiedlichen Risikoanlagen einer Datenverarbeitung in unterschiedlichen Kontexten kann mit den abgestuften Schutzkonzepten des „Privacy-by-Design und by-Default" sowie der Datenschutz-Folgenabschätzung begegnet werden. Für Forschungsprojekte bedeutet dies zunächst, dass das Datenschutzrecht bei der Entwicklung neuer Werkzeuge und Geschäftsmodelle der Datenanalyse von Beginn an mitgedacht werden muss. Entsprechend dem risikobasierten Ansatz sind die resultierenden Schutzmaßnahmen aber nun gleichzeitig grundsätzlich auch Kosten-Nutzen-Erwägungen zugänglich. Die neue Rechtslage bringt natürlich auch Herausforderungen mit sich – so wird das bereits recht ausdifferenzierte Datenschutzrecht teils durch einige noch ausfüllungsbedürftige, allgemeiner gehaltene Abwägungsklauseln ersetzt. Forscher wie Unternehmen sind nun dazu aufgerufen die DS-GVO durch die bestehenden Partizipationsmöglichkeiten wie die Erarbeitung von Verhaltensregeln oder die Zertifizierung mit Leben zu füllen.

Bausteine für einen verantwortlichen Einsatz von Smart Data

Als Key Findings der Zusammenarbeit in der Fachgruppe Recht lassen sich die folgenden zentralen Bausteine für einen verantwortlichen Einsatz von Smart Data zusammenfassen:[180]

- Zusammenwirken
  - Privacy-by-Design durch interdisziplinäre Zusammenarbeit aller Stakeholder realisieren,
  - gemeinsame Sprachen durch vereinfachende Modellierungs- und Visualisierungsmöglichkeiten schaffen.
- Souveränität
  - Auswahlmöglichkeiten und technische Kontroll-/Absicherungsmechanismen für Betroffene anbieten,
  - Akzeptanz durch Mitwirkungsrechte der Betroffenen sowie Transparenz durch Nachverfolgbarkeit steigern.
- Bewusster Datenumgang
  - Zielgerichtete und selektive Datenerhebung,
  - Risikobewusstsein und Abhilfemaßnahmen durch Datenschutzfolgenabschätzung rechtzeitig etablieren.
- Wettbewerbsfaktor Datenschutz
  - Innovationen zum technischen Datenschutz befördern,
  - Vertrauen in datenschutzkonforme Lösungen durch Standardisierung und Zertifizierung stärken und interdisziplinäre Forschung fördern.
- Regulierung und Rechtssicherheit
  - Multilaterale Mitwirkung an Regulierungsprozessen und
  - Entwicklung einheitlicher Standards etablieren.

Interdisziplinäre Zusammenarbeit

Zu den Erfahrungen der rechtlichen Begleitforschung zählt auch, dass es Projekte oftmals als Faktor großer Unsicherheit empfinden, wenn Sie feststellen, dass das Datenschutzrecht oder andere Regularien auf ihren Projektsachverhalt Anwendung finden, sie aber keine Juristen im Team haben um sich der Herausarbeitung der individuellen rechtlichen Anforderungen hin zur Entwicklung eines ausgewogenen, technisch-rechtlichen Gesamtkonzepts zu widmen. Ebenso sind reine technische Lösungen oftmals akzeptanzhindernd, wenn bei der Gestaltung noch keine Compliance-Erwägungen eingeflossen sind. Eine reibungslose Überführbarkeit der Forschungsergebnisse in praktische Innovationen, die sich am Markt behaupten sollen, macht die frühzeitige Einbeziehung auch rechtlichen Sachverstands gerade im Bereich der Forschung zu Smart Data sinnvoll. Denn Datenverarbeitung wirft, wie im Rahmen dieser Broschüre aufgezeigt, in den unterschiedlichsten Fallkonstellationen meist anspruchsvolle und teils noch ungelöste Rechtsfragen auf. Selbst die Vermeidung des Personenbezugs, welcher oftmals als Ausweg zur Minimierung rechtlicher Komplikationen gewählt wird, bedarf aber wegen der oft explorativen Forschungsfragestellungen einer korrekten Einschätzung von Identifizierungsrisiken und entsprechender die De-Anonymisierung hindernder Design-Entscheidungen. Ist das Datenschutzrecht anwendbar, liegt hierin noch keinesfalls eine endgültige Entscheidung über die Rechtskonformität eines Forschungsvorhabens. Dann gilt es zu prüfen, ob zum einen die Forschungstätigkeit legitim ist (und evt. Forschungsprivilegien eingreifen) sowie zum anderen ein späterer ggf. kommerzieller Einsatz rechtskonform umsetzbar wäre. Der rechtlichen Bewertung kommt insoweit eine bedeutsame Rolle bei der Entwicklung von Geschäftsmodellen zu.

Recht und Digitalisierung

Rechtliche Restriktionen, insbesondere durch den Datenschutz, werden von Unternehmen oft als „Klotz am Bein“ wahrgenommen, der Innovationen behindert und den Wirtschaftsstandort Deutschland schwächen würde. Daher dominierten Rufe nach Lockerungen im ordnungsrechtlichen Rechtsrahmen die rechtspolitische Diskussion der letzten Jahre.[181] Eine Abkehr vom konstituierenden Fundament des bestehenden Regelungsrahmens darf aber grundsätzlich nicht zu einer Schwächung des Grundrechtsschutzes führen. Insoweit bedarf es eher der Entwicklung neuer, ebenso effektiver (der technischen Entwicklung entsprechender) Schutzmechanismen. Der Fokus sollte deshalb darauf gerichtet werden, welche Anreize sinnvoll und notwendig sind, um den Einsatz technischer Lösungen zu befördern sowie die Erforschung weiterer Innovationen des Datenschutzes durch Technik anzuregen. Die Forschungsprojekte haben dafür den juristischen Mitwirkenden wertvolle Hinweise zu den realen Sachverhalten und (technischen) Lösungsoptionen geliefert, die ein zukünftiger Rechtsrahmen noch antizipieren sollte und die dazu beitragen, ausgeprägte rechtliche Debatten, die oftmals auf Missverständnissen zu tatsächlichen Grundlagen beruhen, abzukürzen.

Die Akzeptanz in der Bevölkerung steigt zwar mit dem gewährleisteten Datenschutzniveau, jedoch ist gleichzeitig ein gewisses Privacy-Paradoxon zu beobachten: Das tatsächliche Verhalten der Nutzerinnen und Nutzer digitaler Angebote steht im Widerspruch zu geäußerten Bedenken bezüglich datenintensiven Phänomenen wie Big Data.[182] Um die Datensouveränität der Betroffenen zu gewährleisten, wird es technischer Mechanismen bedürfen, wie dem Einsatz von Privacy-Management-Tools oder dem automatisierten Abgleich von Datenanfragen und persönlichen Präferenzen.[183] Die Sicherstellung der Freiwilligkeit der Datenpreisgabe kann auch positive Auswirkungen auf die Datenqualität sowie die Akzeptanz und Kundenzufriedenheit haben.

Im scheinbaren Widerspruch zur Forderung des Regulierungsabbaus im Datenschutzrecht vermehrten sich in den letzten Jahren Forderungen nach der Schaffung eines „Dateneigentums“.[184] Die ausschließliche und exklusive Zuweisung eines Datums oder einer Datensammlung - und damit die Grundlage der Wissensgenerierung - zu einem einzelnen „Eigentümer“ oder „Produzenten“ droht jedoch mit den Grundpfeilern einer Informationsgesellschaft zu kollidieren. In Anbetracht der Tatsache, dass die Schaffung eines derartigen „Datenrechts“ zu nachhaltigen Abgrenzungsschwierigkeiten führen dürfte, sind die wirtschaftlichen Auswirkungen in einer globalisierten, vernetzten Welt kaum absehbar.[185] Rechtswissenschaftler sollten es vermeiden, eine zeitintensive Scheindebatte um die Motivation von tatbestandlichen Anknüpfungen zu führen und damit die notwendige Erkundung von sinnvollen Rechtsfolgenregelungen für diese neue Klasse soziotechnischer Phänomene aus den Augen zu verlieren. Denn die Auseinandersetzung mit dieser aus rein juristisch-dogmatischem Blickwinkel getriebenen, eher unglücklichen Metapher, kostete und kostet Zeit, die von der eigentlichen Frage einer wettbewerbsrechtlichen Regelung zum diskriminierungsfreien Zugang (zu solchen Daten, die keinen datenschutzrechtlichen Restriktionen unterliegen) ablenkt. Diese Art einer vom tatsächlichen Lebenssachverhalt abgekoppelten Debatte kann sich eine Disziplin, die den Transformationsprozess zu einer auch digitalen Gesellschaftsordnung zu unterstützen berufen ist, zukünftig kaum noch leisten, wenn sie mit der technischen Entwick-

lung Schritt halten will. Denn „Datenproduzenten“, Aggregatoren und Informationsintermediäre, die Daten in ihren Händen halten, können den Zugang zu diesen Informationen zunächst auf vertraglicher Basis regeln. Ohne wettbewerbsrechtliche Regulierung, die an dem Datenzugang ansetzt, können aber Lock-in-Effekte oder Marktzutrittsbarrieren generiert und verfestigt werden.

Datenschutz und Wettbewerb

Mit den Innovationen der DS-GVO im Hinblick auf Kontroll- und Sanktionsmechanismen sowie der Ausweitung der Anwendbarkeit auch im internationalen Raum könnten erhebliche Durchsetzungsdefizite, welche zu einer Dissonanz zwischen Recht und Wirklichkeit führten, überwunden werden. Wettbewerbsverzerrungen durch die Entscheidung sich rechtskonform zu verhalten, dürften somit auch im internationalen Vergleich abgemildert werden. Es besteht erstmals die Chance gleiche Wettbewerbsbedingungen im Hinblick auf die kommerzielle Nutzung personenbezogener Daten zu erreichen, wenn die Nachteile der Nichteinhaltung der DS-GVO effektiv die Vorteile einer illegalen Datenkommerzialisierung überwiegen. Bedenkt man die Annahme erhöhter Nutzerakzeptanz datenschutzfreundlicher Angebote, so besteht die Aussicht, dass die Einhaltung eines effektiven und nachweisbaren Datenschutzniveaus einen Wettbewerbsvorteil begründen kann.

Fußnoten

1 Bretthauer ZD 2016, S. 267.

2 Vogel „Datenschutz und Smart Health Data“, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smartdata_publikation_smart_health_data.pdf;jsessionid=F02928DC3CEA753F069EC03364857D1C?__blob=publicationFile&v=1 [letzter Abruf 25.01.2018].

3 Rice „Going from Big Data to Smart Data“, abrufbar unter http://trepscore.com/big-data-to-smart-data/ [letzter Abruf 25.01.2018].

4 Initiative der Trusted Cloud Forschung „Smart Data - A Big Data Memorandum“, abrufbar unter http://smart-data.fzi.de/ [letzter Abruf 25.01.2018].

5 Bretthauer ZD 2016, S. 267.

6 Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data“, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

7 http://www.uni-kiel.de/medinfo/documents/TWMK%20Vorschlag%20DInfMedForsch%20v1.9%20170927.pdf.

8 Roßnagel ZD 2013, S. 562; Weichert ZD 2013, S. 251; Ulmer RDV 2013, S. 227; Bornemann RDV 2013, S. 232; Martini DVBl 2014, S. 1481; Schefzig K&R 2014, S. 772; Marnau DuD 2016, S. 428.

9 Die EU-Kommission definiert von Maschinen generierte Daten als „Daten werden von Maschinen ohne den unmittelbaren Eingriff eines Menschen im Rahmen von Computerprozessen, Anwendungen oder Diensten oder auch durch Sensoren erzeugt, die Informationen von virtuellen oder realen Geräten oder Maschinen oder von einer Software erhalten.” Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 17.01.2017, „Aufbau einer europäischen Datenwirtschaft“, COM(2017) 9 final.

10 Art. 4 Nr. 1 VO (EU) 2016/679 (DS-GVO).

11 Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ WP 136, S. 14; BGH Urteil vom 16. Mai 2017 – VI ZR 135/13; Bergt ZD 2015, S. 365 (369); Kring/Marosi K&R 2016, S. 773; Jensen/Knoke ZD-Aktuell 2016, 05416; Weinhold ZD-Aktuell 2016, 05366; Kühling/Klar Anm. zu EuGH ZD 2017, S. 24; Ernst in Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 11.

12 Diese Regelbeispiele sind nicht abschließend (Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. Nomos 2016, S. 32). Beispiele derartiger Kennungen sind IP Adressen, Cookies oder Funkfrequenzkennzeichnungen (Erwägungsgrund 30), Telefonnummern oder KfZ-Kennzeichen (Gola in Gola, DS-GVO Kommentar, 1. Aufl. 2017, Art. 4 Rn. 4), RFID-Tags, UDID-Nummern und Device Fingerprinting (Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation, Arbeitspapier zu Big Data und Datenschutz 2014, S. 3, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/BerlinGroup/55_DigData.html [letzter Abruf 25.01.2018]).

13 Hornung/Herfurth „Datenschutz bei Big Data“ in König/Schröder/Wiegand „Big Data“ Springer

2018, S. 149 (153); Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ WP 136, S. 14; Roßnagel ZD 2013, S. 562 (563); Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. Aufl. 2017, S. 58, 59.

14 Erwägungsgrund 26 der VO (EU) 2016/679 (DS-GVO).

15 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; insoweit lassen sich die bereits zur Richtlinie erlassenen Entscheidungen und vertretenen Meinungen auf die DS-GVO übertragen (Klar/Kühling in: Kühling/Buchner (Hrsg) DS-GVO Kommentar, 1. Auf. 2017, Art. 4 Nr. 1 Rn. 20).

16 EuGH (Urteil vom 19.10.2016 - C-582/14); BGH, Urteil vom 16. Mai 2017 – VIZR 135/13.

17 Weichert DuD 2007, S. 113 (117); Marnau DuD 2016, S. 428; Hornung/Herfurth „Datenschutz bei Big Data“ in König/Schröder/Wiegand „Big Data“ Springer 2018, S. 149 (165); Art. 29 Datenschutzgruppe Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ WP 136.

18 Marnau DuD 2016, S. 428 (429); Roßnagel ZD 2013, S.563, (566); Sarunski DuD 2016, S. 424 (427); Boehme-Neßler DuD 2016, S. 419 (422); Hornung/Herfurth „Datenschutz bei Big Data“ in König/Schröder/Wiegand „Big Data“ Springer 2018, S. 149 (165); Raabe/Wagner, DuD 2016, S. 434 (435); Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. Nomos 2016, S. 35.

19 Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. Nomos 2016, S. 35; Klabunde in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 13; Klar/Kühling in: Kühling/Buchner (Hrsg) DS-GVO Kommentar, 1. Auf. 2017, Art. 4 Nr. 1 Rn. 22.

20 Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ WP 136, S. 11; Forgó/Krügel MMR 2010, S. 17 (21); ähnlich Weichert DuD 2007, S. 113 (117); Klabunde in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 8; Klar/Kühling in Kühling/Buchner (Hrsg), DS-GVO Kommentar, 1. Aufl. 2017, Art. 4 Nr. 1 Rn. 13f.

21 Hornung/Herfurth „Datenschutz bei Big Data“ in König/Schröder/Wiegand „Big Data“ Springer 2018, S. 149 (166/167), Balaban/Wagner, Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: IoTBDS, 2017, S. 356; ähnlich Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. Nomos 2016, S. 35.

22 Roßnagel ZD 2013, S. 562 (566); Brisch/Pieper CR 2015, S. 724 (728).

23 Art. 29 Datenschutzgruppe, Stellungnahme 05/2014 zu Anonymisierungstechniken (WP 216), Buchmann DuD 2015, S. 510.

24 Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation, Arbeitspapier zu Big Data und Datenschutz 2014, S. 13, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/BerlinGroup/55_DigData.html [letzter Abruf 25.01.2018]; Forgó/Krügel, MMR 2010, S. 17 (18) empfehlen „geschlossene Netzwerke“.

25 Hornung/Herfurth „Datenschutz bei Big Data“ in König/Schröder/Wiegand „Big Data“ Sprin-

ger 2018, S. 149 (166/167); Brisch/Pieper CR 2015, S. 724 (729); Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation, Arbeitspapier zu Big Data und Datenschutz 2014, S. 13, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/BerlinGroup/55_DigData.html [letzter Abruf 25.01.2018]; FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, 2012, S. 21, abrufbar unter https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [letzter Abruf 25.01.2018].

26 Bergt ZD 2015, S. 365 (369), Dammann in Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 27 weist auf die Möglichkeit Geheimhaltungsvereinbarungen im Einverständnis der Vertragsparteien jederzeit (auch rückwirkend) wieder aufzuheben.

27 Brisch/Pieper CR 2015, S. 724 (728).

28 Boehme-Neßler DuD 2016, S. 419 (422).

29 Hornung/Herfurth „Datenschutz bei Big Data“ in König/Schröder/Wiegand „Big Data“ Springer 2018, S. 149 (166/167).

30 BGH, Urteil vom 16. Mai 2017 – VIZR 135/13 Rn. 43.

31 Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation, Arbeitspapier zu Big Data und Datenschutz 2014, S. 13, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/BerlinGroup/55_DigData.html [letzter Abruf 25.01.2018].

32 § 32 BDSG a.F.

33 Bundestags-Drucksache 18/11325, S. 97.

34 Bundestags-Drucksache 18/11325, S. 97; Riesenhuber in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht, 22. Edition 2017, § 26 BDSG 2018, Rn. 32; Seifert in Simitis, BDSG, 8. Aufl. 2014, § 32 BDSG, Rn. 11; Feige ZD 2015, S. 116 (118).

35 Brecht/Steinbrück/Wagner PinG 2018, 10.

36 Art. 29 Datenschutzgruppe, Opinion 2/2017 on data processing at work, WP 249, S. 23; Simitis, BDSG, 8. Aufl. 2014, § 4 BDSG, Rn. 62; VG des Saarlandes, Urteil vom 29.01.2016 - 1 K 1122/14; Vahlen DSB 2016, S. 172; Hofmann ZD 2016, S. 12 (14).

37 § 26 Abs. 2 BDSG-neu.

38 § 26 Abs. 5 BDSG-neu; Art. 5 VO (EU) 2016/679 (DS-GVO).

39 BAG, Beschluss vom 09. September 1975 – 1 ABR 20/74 –, BAGE 27, 256-263; BAG, Beschluss vom 10. Juli 1979 – 1 ABR 50/78 –, juris; Weichert NZA 2017, S. 565 (569); Göpfert/Papst DER BETRIEB, S. 1015 (1020).

40 Dorner, CR 2014, S. 617; Duisberg in: Eberspächer/Wohlmuth (Hrsg), Big Data Wird Neues Wissen. Münchener Kreis e.V., S. 36 ff.; Hornung/Göbel CR 2015, S. 265 (268); Peschel/Rockstroh MMR 2014, S. 571 (572); Zieger/Smirra MMR 2013, S. 418 (419).

41 § 90 BGB.

42 Analyse der Diskussion des „Rechts am Datum“: Duisberg in Smart Data Begleitforschung „Daten als Wirtschaftsgut“, S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/

Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].

43 Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: die zivilrechtliche Erfassung des Datenhandels, Karlsruher Schriften zum Wettbewerbs- und Immaterialgüterrecht. Heymanns, Köln 2012.

44 Siehe bspw. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 17.01.2017, „Aufbau einer europäischen Datenwirtschaft", COM(2017) 9 final.

45 Statt vieler: Jentsch, Dateneigentum –Eine gute Idee für die Datenökonomie?, 2018.

46 § 4 UrhG.

47 § 87a UrhG.

48 §§ 17, 18 UWG.

49 §§ 202a, 202b StGB.

50 Duisberg in Smart Data Begleitforschung „Daten als Wirtschaftsgut", S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].

51 Smart Data Begleitforschung „Daten als Wirtschaftsgut", abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].

52 § 18 Abs. 2a GWB.

53 Bundestags-Drucksache 18/10207, S. 47.

54 Bundestags-Drucksache 18/10207, S. 48.

55 § 18 Abs. 3a GWB.

56 Vgl. Autorité de la Concurrence / Bundeskartellamt "Competition Law and Data" vom 10. Mai. 2016, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=70D1F58933292EECE0ACEF8D1D363E0C.2_cid371?__blob=publicationFile&v=2 [letzter Abruf 03.07.2017].

57 Jung/Feth „Datennutzungskontrolle mit IND2UCE in Smart Data Begleitforschung „ Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data" S. 50, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

58 Fachgruppe „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz" der Smart-Data-Begleitforschung „Open Data in Deutschland" Sieben Forderungen, abrufbar unter: http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_open_data_deutschland.pdf?__blob=publicationFile&v=9 [letzter Abruf 25.01.2018].

59 Selbst wenn lediglich Sach- und Ereignisdaten verarbeitet werden sollen, ist zu prüfen, ob personenbezogene Daten zunächst (mit-)erhoben werden.

60 Art. 6 Abs. 1 S. 1 lit. a) – f) VO (EU) 2016/679 (DS-GVO).

61 § 28 Abs. 1 Nr. 3 BDSG (bzw. § 29 Abs. 1 S. 1 Nr. 2 BDSG)

62 Simitis in Simitis, BDSG, 8. Aufl. 2014, § 28 Rn. 151

63 Taeger in Taeger/Gabel (Hrsg), BDSG, 2. UAfl. 2013, § 28 Rn. 81; Born DSRITB 2017, S. 13 (19). Nicht hingegen zählen solche Informationen dazu, die lediglich für einen begrenzten Personenkreis wie Freunde und Familie freigegeben werden. Ob ein Anmeldeerfordernis auf einer Plattform den Charakter der öffentlichen Zugänglichkeit hindert, ist umstritten. Solange die Anmeldung grundsätzlich jedem frei steht, dürfte die Zugänglichkeit gegeben sein

64 Dies könnte beispielsweise der Fall sein, wenn unübersehbar keine Verarbeitung erwünscht ist oder bei der Erstellung von Persönlichkeitsprofilen.

65 Art. 6 Abs. 1 S. 1 lit. f) VO (EU) 2016/679 (DS-GVO).

66 Art. 29 Datenschutzgruppe, Stellungnahme 6/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, S. 30ff.; Heberlein in Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 6 Rn. 22; Bei der Abwägung können Grundrechte wie die Informations-, Presse- und Meinungsfreiheit oder die Berufsausübung eine Rolle spielen.

67 Erwägungsgründe 47, 48, 49 VO (EU) 2016/679 (DS-GVO).

68 Art. 29 Datenschutzgruppe, Stellungnahme 6/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, S. 37; Born DSRITB 2017, S. 13 (23).

69 Erwägungsgrund 47 VO (EU) 2016/679 (DS-GVO): „Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z.B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht.“

70 Born DSRITB 2017, S. 13 (24) geht bei Kindern von einem überwiegenden Betroffeneninteresse aus.

71 Unter „Crawling“ versteht man die automatisierte Auswertung von Onlinequellen des World Wide Web, wobei in der Regel Text- und Data-Mining-Technologien zum Einsatz kommen.

72 Daten über die rassische und ethische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten sowie Daten zum Sexuallaben oder der sexuellen Orientierung

73 Art. 9 Abs. 2 lit a) – j) VO (EU) 2016/679 (DS-GVO)

74 Schulz in Gola (Hrsg), DS-GVO, 1. Aufl. 2017, Art. 9 Rn. 23.

75 So die Rechtslage unter § 28 Abs. 1 Nr. 3 BDSG, wonach die Datenverarbeitung für eigene Geschäftszwecke zulässig war, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass

das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Daraus wurde die gesetzliche Vermutung abgeleitet, dass die Datenverarbeitung den Betroffeneninteressen nicht widerspricht, solange diese nicht offensichtlich erkennbar entgegenstehen, vgl. Kramer in Auernhammer, BDSG, § 28 Rn. 23 ff; Taeger in Taeger/Gabel, BDSG, § 28 Rn. 103 ff.

76 Art. 14 Abs. 2 lit. f) VO (EU) 2016/679 (DS-GVO).

77 Art. 14 Abs. 5 lit. b) VO (EU) 2016/679 (DS-GVO): Anhaltspunkte für unverhältnismäßigen Aufwand sind laut Erwägungsgrund 62 die Zahl der Betroffenen, das Alter der Daten oder etwaige geeignete Garantien. Ebenfalls in die Abwägung könnte einfließen, ob die Informationen aus öffentlich zugänglichen Quellen stammen (Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Teil 4 Rn. 7).

78 Text und Data Mining wird im EU-Kommissionsvorschlag einer Richtlinie über das Urheberrecht im digitalen Binnenmarkt COM(2016) 593 final definiert als „eine Technik für die automatisierte Auswertung von Texten und Daten in digitaler Form, mit deren Hilfe beispielsweise Erkenntnisse über Muster, Trends und Korrelationen gewonnen werden können".

79 Triaille/de Meeûs d'Argenteuil/de Francquen, Study on the legal framework of text and data mining (TDM), funded by the European Commission, March 2014.

80 Bisges GRUR 2015, 540.

81 BT-Drucksache IV/270, S. 38.

82 Bullinger in Wandtke/Bullinger, UrhG § 2 Rn. 159.

83 Nach EuGH, Urteil vom 16. Juli 2009 – C-5/08 könnten bereits Texte mit 11 Wörtern schutzfähig sein.

84 § 87a UrhG.

85 Zu einem Kurzüberblick siehe: Smart Data Begleitforschung „Daten als Wirtschaftsgut", abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].

86 §§ 87b, 87c UrhG.

87 § 44a UrhG.

88 Siehe zu den Anforderungen im Einzelnen: Triaille/de Meeûs d'Argenteuil/de Francquen, Study on the legal framework of text and data mining (TDM), funded by the European Commission, March 2014, S. 41 ff.

89 Bundestags-Drucksache 18/12329, S. 40: „Die automatisierte Auswertung selbst, der Kern des sogenannten Text und Data Mining, ist keine urheberrechtlich relevante Handlung." Die gesetzliche Erlaubnis des § 60d UrhG bezieht sich daher auf die Vervielfältigung, öffentliche Zugänglichmachung und Entnahme wesentlicher Teile aus geschützten Datenbanken.

90 Raue GRUR 2017, S. 11 (13).

91 Gesetz zur Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft (Urheberrechts-Wissensgesellschafts-Gesetz–UrhWissG): § 60d UrhG (Gültig ab 01.März 2018).

92 Europäische Kommission, Vorschlag für eine

Richtlinie des Europäischen Parlaments und des Rats über das Urheberrecht im digitalen Binnenmarkt vom 14.09.2016, COM (2016) 593 final.

93 Bundesrats-Drucksache 565/16 (Beschluss), S. 7.

94 17 U.S.C. § 107.

95 Bunk in: Smart Data Begleitforschung „Daten als Wirtschaftsgut", S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].

96 § 87g Abs. 4 UrhG.

97 §§ 87f, 87g Abs. 2 UrhG.

98 Bundestags-Drucksache 17/11470, S. 8.

99 Vgl. Bundestags-Drucksache 17/11470, 7.

100 Jani in Wandtke/Bullinger UrhG § 87f Rn. 12; Bundestags-Drucksache 17/11470, 6.

101 Dreier in Dreier/Schulze UrhG § 87f Rn. 3.

102 OLG München, Urteil vom 14. Juli 2016 – 29 U 953/16.

103 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht im digitalen Binnenmarkt vom 14.09.2016, COM(2016) 593 final.

104 Bunk in: Smart Data Begleitforschung „Daten als Wirtschaftsgut", S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].

105 Weichert DuD 2007, S. 113 (114).

106 Weichert DuD 2007, S. 113.

107 de Montjoye/Hidalgo/Verleysen/Blondel, Scientific Reports 3, Article number: 1376, 2013.

108 Art. 4 Nr. 1 VO (EU) 2016/679 (DS-GVO).

109 Klabunde in Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 12. In der DS-GVO selbst werden Standortdaten nicht definiert. Die Definition in Art. 2 lit. c) der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG ist spezifisch zugeschnitten auf elektronische Kommunikationsnetze und –dienste, sodass eine analoge Anwendbarkeit auch im Hinblick auf die kommende ePrivacy-VO zweifelhaft erscheint.

110 Art. 25 Abs. 1 und 2 VO (EU) 2016/679 (DS-GVO); Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" WP 136; Art. 29 Datenschutzgruppe, Opinion 03/2013 on purpose limitation WP 203.

111 Art. 4 Nr. 5 VO (EU) 2016/679 (DS-GVO).

112 § 3 Abs. 6a BDSG.

113 Erwägungsgrund 26 S. 2 VO (EU) 2016/679 (DS-GVO).

114 Weichert NZA 2017, S. 565.

115 Gola NZA 2007, S. 1139 (1142).

116 Gola NZA 2007, S. 1139 (1143), Weichert NZA 2017, S. 565 (567).

117 Gola NZA 2007, S. 1139 (1143).

118 Gola NZA 2007, S. 1139 (1142); Weichert NZA 2017, S. 565 (567).

119 BAG, Beschluss vom 09. September 1975 – 1 ABR 20/74 –, BAGE 27, 256-263; BAG, Beschluss vom 10. Juli 1979 – 1 ABR 50/78 –, juris; Weichert NZA 2017, S. 565 (569); Göpfert/Papst DER BETRIEB, S. 1015 (1020).

120 § 4 UrhG.

121 § 87a UrhG.

122 Auch bei Annahme eines Datenbankwerkes nach § 4 UrhG kann der Schutz des Datenbankherstellers grundsätzlich daneben bestehen (Dreier/Schulze, Teil 2. Verwandte Schutzrechte, Abschnitt 6. Schutz des Datenbankherstellers, Vorbemerkung, Rn. 8).

123 OLG Köln MMR 2007, 443.

124 Thum/Hermes in Wandtke/Bullinger(Hrsg), UrhG § 87a Rn. 19.

125 Erwägungsgrund 40 der Datenbankrichtlinie RL 96/9/EG.

126 EuGH, Urteil vom 9. 11. 2004 - C-203/02.

127 Erwägungsgrund 46 RL 96/9/EG; OLG Köln MMR 2007, 443; Thum/Hermes in Wandtke/Bullinger (Hrsg), UrhG § 87a Rn. 5.

128 Zieger/Smirra MMR 2013, S. 418 (420).

129 http://www.faz.net/aktuell/wirtschaft/diginomics/fitness-app-verraet-geheime-militaerstandorte-15422027.html [letzter Abruf 05.02.2018].

130 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

131 Art. 2 Nr. 1 (a)-(c) der Richtlinie (EU) 2016/943.

132 BVerfG, Stattgebender Kammerbeschluss vom 23. Februar 2007 – 1 BvR 2368/06; BVerfG, Stattgebender Kammerbeschluss vom 11. August 2009 – 2 BvR 941/08; LG Essen, Urteil vom 26. Juni 2014 – 10 S 37/14; VG Schwerin, Beschluss vom 18. Juni 2015 – 6 B 1637/15 SN; OVG des Saarlandes, Urteil vom 14. September 2017 – 2 A 197/16; Albrecht, jurisPR-ITR 9/2015 Anm. 2; Hornung/Desoi K&R 2011, S. 153 (154).

133 VG Schwerin, Beschluss vom 18. Juni 2015 – 6 B 1637/15 SN; OVG des Saarlandes, Urteil vom 14. September 2017 – 2 A 197/16.

134 DSK, Kurzpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung, Stand 01.08.2018, abrufbar unter https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DS-GVO/DSK_KPNr_15_Videoueberwachung.pdf [letzter Abruf 05.02.2018].

135 Bundestags-Drucksache 18/11325, S. 81.

136 Bundestags-Drucksache 18/11325, S. 81.

137 DSK, Kurzpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung, Stand 01.08.2018, abrufbar unter https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Lan-

desaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DS-GVO/DSK_KPNr_15_Videoueberwachung.pdf [letzter Abruf 05.02.2018].

138 DSK, Kurzpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung, Stand 01.08.2018, abrufbar unter https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DS-GVO/DSK_KPNr_15_Videoueberwachung.pdf [letzter Abruf 05.02.2018].

139 Spiecker gen. Döhmann K&R 2014, S. 549 (551); Bretthauer/Krempel in Schweighofer/Kummer/Hötzendorfer (Hrsg) Transparenz, Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014, S. 525; Bier/Spiecker gen. Döhmann CR 2012, S. 610; Hornung/Desoi K&R 2011, 153.

140 Spiecker gen. Döhmann K&R 2014, S. 549 (552); Bretthauer/Krempel in Schweighofer/Kummer/Hötzendorfer (Hrsg) Transparenz, Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014, S. 525; NurseEye: Datenschutzfreundliche Sturzdetektion und Alarmierung für die Pflege, abrufbar unter https://www.iosb.fraunhofer.de/servlet/is/69347/ [letzter Abruf 31.01.2018].

141 BVerfG, Beschluss vom 04. April 2006 – 1 BvR 518/02.

142 DSK, Kurzpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung, Stand 01.08.2018, abrufbar unter https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DS-GVO/DSK_KPNr_15_Videoueberwachung.pdf [letzter Abruf 05.02.2018].

143 Vgl. Art. 13 VO (EU) 2016/679 (DS-GVO)

144 Die Erhebung nur für „festgelegte Zwecke“ setzt bereits Art. 8 Abs. 2 der EU-Grundrechte-Charta voraus. Siehe zur Bedeutung der Zweckbindung auch: BVerfGE 65, 1 (Volkszählungsurteil); Frenzel in Paal/Pauly (Hrsg) Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 23; Dammann ZD 2016, S. 307 (311); Positionspapier der DSK zur Datenschutz-Grundverordnung 2015, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/DSKFordertVerbesserungDSGrundVO.html [letzter Abruf 25.01.2018]; Weichert/Schuler „Datenschutz contra Wirtschaft und Big Data, abrufbar unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/analyse_2015_12_bigdata.pdf [letzter Abruf 25.01.2018]; Raabe/Wagner in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data“ S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

145 Siehe ausführlich: Raabe/Wagner in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data“ S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

146 Art. 5 Abs. 1 lit. b) VO (EU) 2016/679 (DS-GVO).

147 Grafenstein DuD 2015, S. 789; Grafenstein in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data“ S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

148 Wolff in Wolff/Brink, BeckOK Datenschutzrecht, Syst A. Prinzipien, Rn. 19.

149 Art. 5 Abs. 1 lit. b) VO (EU) 2016/679 (DS-GVO).

150 Art. 6 Abs. 4 lit. a)-e) VO (EU) 2016/679 (DS-GVO); siehe auch Art. 29 Datenschutzgruppe, Opinion 03/2013 on purpose limitation, WP 203.

151 Art. 6 Abs. 4 VO (EU) 2016/679 (DS-GVO), die Rechtsvorschrift muss dem Schutz der in Art. 23 Abs. 1 genannten Ziele dienen, notwendig und verhältnismäßig sein.

152 Erwägungsgrund 50 S. 2 VO (EU) 2016/679 (DS-GVO). Richter DuD 2016, S. 581 (584); Frenzel in Paal/Pauly (Hrsg) Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 31 fordert kompensatorisch gesteigerte Anforderungen an Transparenz und Datenrichtigkeit.

153 Schantz NJW 2016, S. 1841 (1844), Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. Aufl. 2017, S. 76; ähnlich Gläß/Drepper in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data“, S. 23, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018], wonach es sich bei Erwägungsgrund 50 S. 2 VO (EU) 2016/679 (DS-GVO) um ein redaktionelles Versehen handeln könnte.

154 Art. 89 Abs. 1 S. 4 VO (EU) 2016/679 (DS-GVO); § 27 Abs. 3 BDSG-neu; siehe auch Albrecht CR 2016, S. 88 (91).

155 Art. 13 Abs. 3, Art. 14 Abs. 4 VO (EU) 2016/679 (DS-GVO).

156 Art. 35 Abs. 3 lit. c) VO (EU) 2016/679 (DS-GVO).

157 DSK Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Stand 24.07.2017, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_DatenschutzFolgeabschaetzung.pdf?__blob=publicationFile&v=2 [letzter Abruf 05.02.2018].

158 Art. 36 VO (EU) 2016/679 (DS-GVO).

159 Art. 58 VO (EU) 2016/679 (DS-GVO).

160 Art. 4 Nr. 15 VO (EU) 2016/679 (DS-GVO).

161 Art. 9 Abs. 1 VO (EU) 2016/679 (DS-GVO)

162 Weichert in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data“, S. 27, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

163 Reng/Debold/Specker/Pommerening „Generische Datenschutzkonzepte für die Forschungsnet-

ze in der Medizin"; Gläß/Drepper in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data", S. 23, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

164 Gläß/Drepper in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data", S. 23, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018].

165 Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (Bundestags-Drucksache 18/11936)

166 Bundestags-Drucksache 18/11936, S. 22.

167 Fechtner/Haßdenteufel CR 2017, S. 355 (360); Härting, "Gesetzentwurf soll Sicherheit für Anwälte Schaffen" in Legal Tribune Online, 20.2.2017, abrufbar unter: https://www.lto.de/recht/juristen/b/outsourcing-rechtsanwaelte-dienstleister-gesetz-entwurf-203-stgb-43e-brao/ [letzter Abruf 26.01.2018].

168 Bundestags-Drucksache 18/7555, S. 105.

169 Art. 2, 3 VO (EU) 2016/679 (DS-GVO).

170 Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel, Die Datenschutz-Grundverordnung und das nationale Recht, 2016; Roßnagel, Europäische Datenschutz-Grundverordnung – Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 2017.

171 Art. 6 Abs. 1 S. 1 lit. c) und e), Abs. 2 VO (EU) 2016/679 (DS-GVO).

172 vgl. §§ 3 ff., 29ff. MsbG.

173 Bretthauer EnWZ 2017, S. 56; Bräuchle, Datenschutzprinzipien in IKT-basierten kritischen Infrastrukturen, Dissertation, Baden-Baden, 2017.

174 § 8a BSIG.

175 § 2 Abs. 10 BSIG.

176 http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/04/kabinett-kritis-vo.html

177 so Gehrmann in DSRITB 2016, S. 263 (272).

178 Art. 29 Datenschutzgruppe, Opinion 03/2013 on purpose limitation WP 203, Annex 2 Big Data and Open Data, S. 45; Deutscher Ethikrat, Stellungnahme „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung" 2017, abrufbar unter http://www.ethikrat.org/dateien/pdf/stellungnahme-big-data-und-gesundheit.pdf [letzter Abruf 25.01.2018]; Roßnagel, ZD 2013, S. 562; Weichert, ZD 2013, S. 251; Martini, DVBl 2014, S. 1481; Raabe/Wagner DuD 2016, S. 434; Hornung / Herfurth „Datenschutz bei Big Data" in König/Schröder/Wiegand „Big Data" Springer 2018, S. 149.

179 Raabe/Wagner DuD 2016, S. 434.

180 Raabe/Wagner DuD 2016, S. 434 (439).

181 Krempl, „Reichtum statt Sparsamkeit: Dobrindt will Datenschutz lockern" 17.11.2016, abruf-

bar unter https://www.heise.de/newsticker/meldung/Reichtum-statt-Sparsamkeit-Dobrindt-will-Datenschutz-lockern-3490700.html [letzter Abruf 07.02.2018]; Dobrindt, „Grundsatz der Datensparsamkeit muss weg", abrufbar unter https://www.golem.de/news/alexander-dobrindt-grundsatz-der-datensparsamkeit-muss-weg-1511-117536.html [letzter Abruf 07.02.2018]; a.A. Schaar in Smart Data Begleitforschung „Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data", S. 23, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_zukunft_datenschutz.pdf?__blob=publicationFile&v=7 [letzter Abruf 25.01.2018]; siehe auch Forum Privatheit, „Datensparsamkeit oder Datenreichtum?", Policy Paper 2017, abrufbar unter https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/positionspapiere-policy-paper/PolicyPaper-Datensparsamkeit.pdf [letzter Abruf 07.02.2018].

182 Norberg/ Horne/Horne: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: Journal of Consumer Affairs 41/1, S. 100–126, 2007.

183 Stiftung Datenschutz, Neue Wege in die Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen; Platform for Privacy Preferences (P3P) https://www.w3.org/P3P/.

184 Dachwitz „Dateneigentum: Merkel ist noch unsicher, ob unsere Daten Firma A oder Firma B gehören sollen" 20.03.207, abrufbar unter https://netzpolitik.org/2017/dateneigentum-merkel-ist-noch-unsicher-ob-unsere-daten-firma-a-oder-firma-b-gehoeren-sollen/ [letzter Abruf 07.02.2018]; Presse- und Informationsamt der Bundesregierung „Merkel: Eigentum an Daten regeln" Pressemitteilung, 18.03.2017, abrufbar unter https://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2017/03/2017-03-18-podcast.html [letzter Abruf 07.02.2018]; siehe auch Wiebe, CR 2017, S. 87; Ensthaler, NJW 2016, S. 3473; Specht, CR 2016, S. 288; Heymann, CR 2016, S. 650; Zech, CR 2015, S. 137; Fetzer, MMR 2015, S. 777; Heun/Assion, CR 2015, S. 812; Schwartmann/Hentsch, RDV 2015, S. 221; Peschel/Rockstroh, MMR 2014, S. 571; Dorner, CR 2014, S. 617; Seidel, ZG 2014, S. 153; Hoeren, MMR 2013, S. 486; Grosskopf, IP-Beratungspraxis 2011, S. 259; Redeker, CR 2011, S. 634.

185 Smart Data Begleitforschung „Daten als Wirtschaftsgut", S. 16, abrufbar unter https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 [letzter Abruf 25.01.2018].