Internetrecht und Digitale Gesellschaft

Band 16

IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme

Event Data Recording und integrierte Produktbeobachtung als Maßnahmen der IT-Risikominimierung am Beispiel automatisierter und vernetzter Luft- und Straßenfahrzeuge

Von

Alexander Schmid

Duncker & Humblot · Berlin

ALEXANDER SCHMID

IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 16

IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme

Event Data Recording und integrierte Produktbeobachtung als Maßnahmen der IT-Risikominimierung am Beispiel automatisierter und vernetzter Luft- und Straßenfahrzeuge

Von

Alexander Schmid

Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Passau
hat diese Arbeit im Jahre 2018 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

Satz: TextFormA(r)t, Daniela Weiland, Göttingen
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-15633-7 (Print)
ISBN 978-3-428-55633-5 (E-Book)
ISBN 978-3-428-85633-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

„1 –
A robot may not injure a human being, or, through inaction, allow a human being to come to harm.

2 –
A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

3 –
A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.“

Isaac Asimov, 1920–1992
I, Robot, vor Introduction

Vorwort

In Zeiten, in denen Algorithmen eigenständig Musik komponieren oder Bilder malen, in denen jeder Alltagsgegenstand vernetzt zu werden scheint und cyber-physische Systeme wie selbstfahrende Straßenfahrzeuge oder selbstfliegende Drohnen allmählich unsere Straßen und unseren Himmel bevölkern, steht es mehr denn je in der Verantwortung des Rechts, mit diesen Entwicklungen Schritt zu halten und den sich hieraus ergebenden Gefahren effektiv entgegenzuwirken.

Zwei mögliche Instrumente der Risikominimierung stellen in diesem Kontext das Event Data Recording und die Produktbeobachtung dar, für die sich im Anwendungsbereich automatisierter und vernetzter Systeme zukünftig völlig neuartige Möglichkeiten ergeben werden. Während die Produktbeobachtung dabei dem präventiven Gefahrenschutz dient, bezweckt das Event Data Recording die Aufrechterhaltung der Rechtssicherheit, sollte es dennoch zu einem Unfall kommen.

Ausgehend von der Erkenntnis, dass Technik und Recht untrennbar miteinander verzahnt sind, versucht diese Arbeit, neue technische Ansätze für das Event Data Recording und die Produktbeobachtung in der „smartifizierten" Welt von morgen auszuloten und rechtlich einzuordnen. Dabei soll insbesondere das derzeit geltende Recht betrachtet, ergänzend aber auch Anforderungen an zukünftige Rechtsreformen aufgezeigt werden. Zur Veranschaulichung dienen hierfür in erster Linie automatisierte und vernetzte Straßen- und Luftfahrzeuge. Gleichwohl wird der Blick auch stets auf „das große Ganze", also auf automatisierte und vernetzte Systeme im übergeordneten Kontext, geweitet.

Die Arbeit wurde im April 2018 fertiggestellt und von der Juristischen Fakultät der Universität Passau im August 2018 als Dissertation angenommen. Neuere Gesetzgebung und Literatur wurden im Wesentlichen bis Oktober 2018 berücksichtigt.

Mein besonderer Dank gilt meinem Doktorvater Herrn Professor Dr. Dirk Heckmann für seine kontinuierliche Förderung und Unterstützung während meiner Zeit an seinem Lehrstuhl als studentische Hilfskraft, wissenschaftlicher Mitarbeiter und Doktorand sowie für seine wertvollen Ratschläge und inspirierenden Anregungen.

Herrn Professor Dr. Michael Beurskens danke ich für die rekordverdächtig schnelle Erstellung des Zweitgutachtens sowie für die äußerst hilfreichen Anmerkungen und Hinweise.

Ebenso danke ich meinen ehemaligen Arbeitskollegen des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht sowie allen Studienkollegen und Freunden, die meine Studienzeit in Passau unvergesslich gemacht haben.

Allen voran danke ich von Herzen aber meiner Familie sowie meiner lieben Freundin Mina und ihrer Familie, die mich in der Verwirklichung meiner Ziele in jeglicher Hinsicht uneingeschränkt unterstützt haben und unterstützen. Ohne deren stete Motivation wäre diese Arbeit sicherlich nicht in dieser Form möglich gewesen.

München, Oktober 2018 *Alexander Schmid*

Inhaltsübersicht

Inhaltsverzeichnis

4. Teil

Rechtspflicht zum Event Data Recording und zur integrierten Produktbeobachtung bei CPS 105

Kapitel 1

Event Data Recording als Rechtspflicht 105

Kapitel 2

Abkürzungsverzeichnis

ABS	Antiblockiersystem
ACPS	Automatisiertes cyber-physisches System
AI	Artifizielle Intelligenz
ATS	Air Traffic Service
BASt	Bundesanstalt für Straßenwesen
BAuA	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMW	Bayerische Motoren Werke (Kfz-Hersteller)
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVCP	Bundesverband Copterpiloten
C2C	Car-to-Car (Kommunikation)
C2I	Car-to-Infrastructure (Kommunikation)
CAT	Commercial Air Transport Operation
CD	Compact Disc
CEFIC	Conseil Européen de l'Industrie Chimique (Verband der Europäischen chemischen Industrie)
CPS	Cyber-physisches System
CVR	Cockpit Voice Recorder
DFS	Deutsche Flugsicherung GmbH
DJI	Dà-Jiāng Innovations (UAS-Hersteller)
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DrohnenVO	Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten
DVD	Digital Versatile Disc
EDR	Event Data Recorder
EDV	Elektronische Datenverarbeitung
EEPROM	Electrically Erasable Programmable Read-only Memory
ESP	Elektronisches Stabilitätsprogramm
EXE	Executable (Dateiformat)
FDR	Flight Data Recorder
FUEGO	Fire Urgency Estimator in Geosynchronous Orbit
GAU	Größter anzunehmender Unfall
GEN	General Requirements
GPS	Global Positioning System
GSG 9	Grenzschutzgruppe 9
GSM	Global System for Mobile Communications
HTML	Hypertext Markup Language
IBM	International Business Machines (EDV-Unternehmen)
ICAO	International Civil Aviation Organization
IDE	Instruments, Data, Equipment
IDS	Intrusion Detection System

ILS	Instrument Landing System
INDECT	Intelligent information system supporting observation, searching and detection for security of citizens in urban environment
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
KI	Künstliche Intelligenz
LTE	Long Term Evolution
M2I	Machine-to-Infrastructure (Kommunikation)
M2M	Machine-to-Machine (Kommunikation)
M2P	Machine-to-Pedestrian (Kommunikation)
M2V	Machine-to-Vehicle (Kommunikation)
MAC	Media Access Control
MCTOM	Maximum Certified Take-off Mass
MDP	Mobilitätsdiensteplattform
MOPSC	Maximum Operational Passenger Seating Configuration
MPA	Motor Powered Aircraft
OBD	On-Board-Diagnose-System
PDF	Portable Document Format
PWC	PricewaterhouseCoopers International
RAM	Random-Access Memory
RFID	Radio-Frequency Identification
ROS	Robot Operating System
SAA	Sense-and-Avoid
SAE	Society of Automotive Engineers
SIM	Subscriber Identity Module
SLC	Single-Level-Cell
SORA	Specific Operations Risk Assessment
SSD	Solid State Drive
sUAS	Small Unmanned Aircraft System
UAS	Unmanned Aircraft System
UAS-Pol	Unmanned Aircraft System-Police
UAV	Unmanned Aerial Vehicles
UPS	United Parcel Service
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure (Kommunikation)
V2N	Vehicle-to-Network (Kommunikation)
V2P	Vehicle-to-Pedestrians (Kommunikation)
V2V	Vehicle-to-Vehicle (Kommunikation)
VDA	Verband der deutschen Automobilindustrie
WHO	World Health Organization
WLAN	Wireless Local Area Network

Ansonsten werden die üblichen Abkürzungen gebraucht, vgl. *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 8. Aufl. 2015

1. Teil

Problemstellung und Gang der Untersuchung

„Suche nicht nach Fehlern, suche nach Lösungen."
Henry Ford, 1863–1947
Gründer der Ford Motor Company

„Zum Greifen nah ist die Gemütlichkeit des griechischen Bürgers, die durch unsere mechanischen Diener ermöglicht wird, die seine zwölf bis fünfzehn pro freiem Mann bei Weitem übertreffen. Diese mechanischen Diener springen uns zu Hilfe. Beim Betreten eines Raumes erhellen uns auf Knopfdruck ein Dutzend Lichtquellen den Weg. Ein anderer Diener sitzt vierundzwanzig Stunden am Tag an unserem Thermostat und reguliert die Wärme in unserem Haus. Ein anderer sitzt Tag und Nacht an unserem automatischen Kühlschrank. Sie starten unser Auto, treiben unsere Motoren an, putzen unsere Schuhe und kultivieren unsere Haare."[1]
(*Nash*, Jay B.: Spectatoritis, New York 1932, S. 265)

Nash hat Recht behalten: Automatisierung und Vernetzung halten heute zunehmend Einzug in alle Lebensbereiche, von der *„Kaffeemaschine am Morgen und dem Funkwecker am Abend"*[2] („Smart Home") über die intelligente Bekleidung („Smart Wearables") und die vernetzte Verkehrsinfrastruktur („Smart Road Infrastructure") bis hin zur vollständigen Automatisierung und Vernetzung der Industrie („Smart Factory"), unserer Stromversorgung („Smart Grids") oder sogar ganzer Städte („Smart Cities").[3] Selbst die Art und Weise, wie wir zukünftig Verträge abschließen und durchführen („Smart Contracts")[4], wird von dieser allgegenwärtigen und alleserfassenden „Smartifizierung"[5], die keinen Stein auf dem anderen zu lassen scheint, nicht verschont bleiben.

Angeführt wird diese disruptive digitale Transformation insbesondere durch automatisierte und vernetzte „cyber-physische Systeme" („CPS"). Unter einem

---

[1] Frei übersetzt ins Deutsche von: *„Within our grasp is the leisure of the Greek citizen, made possible by our mechanical slaves, which far outnumber his twelve to fifteen per free man. These mechanical slaves jump to our aid. As we step into a room, at the touch of a button a dozen light our way. Another slave sits twenty-four hours a day at our thermostat, regulating the heat of our home. Another sits night and day at our automatic refrigerator. They start our car; run our motors; shine our shoes, and cult our hair."*, *Nash*, Spectatoritis, S. 265.

[2] VK Baden-Württemberg, Beschl. v. 16.08.2017 – 1 VK 24/17, ZfBR 2018, 102.

[3] Vgl. zu dieser umfassenden Smartifizierung bereits *Heckmann/Schmid*, vbw Studie Datenschutz, IT-Sicherheit und Haftung bei automatisierten Systemen, S. 12.

[4] Vgl. hierzu *Heckmann*, vbw Studie Blockchain und Smart Contracts, S. 13 ff.

[5] Hierzu bereits *Heckmann/Schmid*, vbw Studie Datenschutz, IT-Sicherheit und Haftung bei automatisierten Systemen, S. 12; *Heckmann/Schmid*, Informatik-Spektrum 2017, 430, 431.

cyber-physischen System ist dabei eine digitalisierte Maschine zu verstehen, also eine informationstechnische Einheit, die sowohl aus einer mechanischen Komponente als auch aus Software zusammengesetzt und somit fähig ist, in physischer Form auf ihre Umwelt einzuwirken und mit dieser in Interaktion zu treten.[6] Neben der Automatisierung stellt dabei auch die Vernetzung eine wesentliche Eigenschaft cyber-physischer Systeme dar, die zusammen mit anderen IT-Systemen das sog. „Internet der Dinge" („Internet of Things"/„IoT") bilden.[7] Aufgrund dieser Vernetzung kann das cyber-physische System mit anderen CPS, sonstigen IT-Systemen oder Menschen Informationen austauschen oder Befehle von diesen entgegennehmen. Neben den bereits aufgezählten Beispielen fallen unter den Begriff des CPS etwa Roboter aller Art, zudem aber bspw. auch Staudämme, Atom- oder Windkraftwerke, Herzschrittmacher oder vernetztes Spielzeug. Trotz dieser schier unendlichen Palette an denkbaren Arten und Formen cyber-physischer Systeme existiert derzeit aber wohl keine CPS-Gattung, über die in der Gesellschaft und Politik dermaßen leidenschaftlich diskutiert wird wie automatisierte und vernetzte Straßen- und Luftfahrzeuge.

Während Straßenfahrzeuge dabei gefühlt seit jeher tief mit unserem Alltag verzahnt sind und die Automatisierung des Straßenverkehrs (nach der Einführung etwa des ABS, des ESP, des Tempomaten, des Abstandswarners und des Parklenkassistenten) den denklogisch nächsten Schritt darstellt, sind es vielmehr unbemannte Luftfahrzeuge („Unmanned Aircraft Systems"/„UAS"), die als technische Newcomer in den letzten Jahren ganze Industrie- und Technikzweige beflügelt haben. Egal ob im Transportwesen, in der Industrie, im Rahmen von Inspektion und Wartung, in der Land- und Forstwirtschaft oder im Polizei- und Sicherheitswesen – für zahlreiche Einsatzgebiete werden UAS derzeit entwickelt und getestet oder befinden sich bereits im Praxiseinsatz. Laut einer Studie von PricewaterhouseCoopers International („pwc") stellen UAS, neben dem Internet der Dinge, der Augmented und Virtual Reality, der Blockchain-Technologie, der artifiziellen Intelligenz, dem 3D-Druck und der Robotertechnik im Allgemeinen, gar eine der acht *„[t]ech breakthroughs megatrends"* der kommenden Jahre dar,[8] die *„Geschäftsmodelle und Geschäfte rund um den Globus umwälzen"* werden, worauf *„Unternehmen aller Größen und Branchen […] vorbereitet sein [sollten]"*.[9] Hält man sich vor Augen, dass bei automatisierten und vernetzten UAS sogar mehrere dieser Technologien gebündelt werden, wird die besondere Bedeutung und Brisanz dieser Technologie nochmals unterstrichen.

Neben den zahlreichen Chancen und Potentialen können sich als Schattenseite der Automatisierung und Vernetzung hieraus jedoch auch gesteigerte oder neuartige

---

[6] Vgl. *Bendel*, 300 Keywords Informationsethik, S. 208.
[7] Vgl. *Bendel*, 300 Keywords Informationsethik, S. 208.
[8] *Eckert/Curran/Bhardwaj*: pwc-Studie, Tech breakthroughs megatrend: how to prepare for its impact, S. 5.
[9] *Sieger*, pwc-Beitrag, Die gewaltigen Acht.

Risiken ergeben, da die Automatisierung stets mit Verselbstständigung und Kontrollverlust und die Vernetzung mit einer Öffnung des Systems für unberechtigte Dritte einhergeht. Insbesondere die letztgenannte Gefahr des Internets der Dinge wurde in den vergangenen Jahren bereits im Rahmen zahlreicher Sicherheitsvorfälle bei vernetzten Industrieanlagen (bspw. „Stuxnet“[10]), staatlichen Einrichtungen (bspw. „WannaCry“[11]) oder privaten „Smart Devices“ (bspw. „My Friend Cayla“[12]) anschaulich verdeutlicht.[13] Besondere Brisanz haben vor diesem Hintergrund aber erneut cyber-physische Systeme, die aufgrund ihrer mechanischen Komponente nicht nur eine Gefahr für die Informationssicherheit, sondern auch für die Funktionssicherheit darstellen können. Der sog. „Jeep Cherokee Hack“ aus dem Jahr 2014, bei dem auch sicherheitskritische Fahrfunktionen von Angreifern aus der Ferne übernommen werden konnten,[14] stellt nur eines von vielen Beispielen hierfür dar.

Dabei ist zunächst zu befürchten, dass die Komplexität und der mehrschichtige Aufbau von automatisierten und vernetzten CPS (einerseits aufgrund des multilateralen Zusammenwirkens unterschiedlicher Hersteller von Teilkomponenten bei der Entwicklung, andererseits aufgrund der Einbettung von CPS in das Internet der Dinge) sowie die Komplexität der Operationsumgebungen, in denen CPS betrieben werden sollen, eine abgeschlossene und sichere Produktentwicklung in der Herstellersphäre, also sozusagen *„am Reißbrett“*[15], immer weniger zulässt. Als Konsequenz könnte sich hieraus ergeben, dass automatisierte und vernetzte CPS künftig auch nach der Markteinführung und Inverkehrgabe noch unter zahlreichen, bislang unbekannten Produktfehlern leiden (im Rahmen dieser Arbeit daher als „Unknown Causes of Trouble“ bezeichnet), die nicht unter Laborbedingungen simulierbar sind, sondern erst im späteren Praxiseinsatz, also beim Kunden, zu Tage treten.[16] Auch das Europäische Parlament betont aus diesem Grund mittlerweile, *„dass die Prüfung von Robotern in lebensnahen Szenarien für die Ermittlung und Bewertung der Risiken, die mit ihnen verbunden sein können sowie für ihre technologische Entwicklung, die über eine reine Versuchsphase im Labor hinausgeht, von entscheidender Bedeutung ist“*[17].

---

[10] *Rieger*, FAZ-Beitrag v. 22.09.2010, Der digitale Erstschlag ist erfolgt.

[11] Spiegel Online-Beitrag v. 13.05.2017, „WannaCry“-Attacke – Fakten zum globalen Cyberangriff.

[12] *Kühl*, Zeit Online-Beitrag v. 17.02.2017, Vernichten Sie diese Puppe.

[13] Vgl. hierzu auch *Helmbrecht*, Redebeitrag Security and Liability in the Internet of Things, S. 2 ff.

[14] Siehe 3. Teil, Kapitel 2, B., III., 2.

[15] *Heckmann/Schmid*, Informatik-Spektrum 2017, 430, 432 f.; *Schmid/Wessels*, NZV 2017, 357, 359.

[16] Vgl. hierzu bereits *Heckmann/Schmid*, Informatik-Spektrum 2017, 430, 433; *Schmid/Wessels*, NZV 2017, 357, 359; *Jänich/Schrader/Reck*, NZV 2015, 313, 318; *Förster*, in: Bamberger/Roth/Hau/Poseck, BeckOK BGB, § 823 BGB Rn. 734.

[17] 2015/2103(INL), S. 9.