Strafrechtliche Abhandlungen

Neue Folge · Band 321

Das Internet der Dinge und das Strafrecht

Herausforderungen vernetzter Geräte für das materielle Strafrecht und das Strafprozessrecht

Von

Florian Nicolai

Duncker & Humblot · Berlin

FLORIAN NICOLAI

Das Internet der Dinge und das Strafrecht

Strafrechtliche Abhandlungen · Neue Folge

Begründet von Dr. Eberhard Schmidhäuser (†)
em. ord. Prof. der Rechte an der Universität Hamburg

Herausgegeben von
Dr. Dres. h. c. Friedrich-Christian Schroeder (†)
em. ord. Prof. der Rechte an der Universität Regensburg
und
Dr. Andreas Hoyer
ord. Prof. der Rechte an der Universität Kiel

in Zusammenarbeit mit den Strafrechtslehrern der deutschen Universitäten

Band 321

Das Internet der Dinge und das Strafrecht

Herausforderungen vernetzter Geräte für
das materielle Strafrecht und das Strafprozessrecht

Von

Florian Nicolai

Duncker & Humblot · Berlin

Gedruckt mit Unterstützung der Deutschen Forschungsgemeinschaft (DFG)

Zur Aufnahme in die Reihe empfohlen von
Professor Dr. Hans Kudlich, Erlangen

Der Fachbereich Rechtswissenschaft
der Friedrich-Alexander-Universität Erlangen-Nürnberg hat
diese Arbeit im Jahre 2023 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: 3w+p GmbH, Rimpar
Druck: CPI Books GmbH, Leck
Printed in Germany

ISSN 0720-7271
ISBN 978-3-428-19056-0 (Print)
ISBN 978-3-428-59056-8 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

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

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde vom Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg im Sommer 2023 als Dissertation angenommen. Literatur und Rechtsprechung konnten bis Dezember 2023 berücksichtigt werden. Die Arbeit entstand im Rahmen des DFG-Graduiertenkollegs 2475 „Cyberkriminalität und Forensische Informatik“. Für den großzügigen Druckkostenzuschuss danke ich der Deutschen Forschungsgemeinschaft (DFG). Für die Aufnahme in die Schriftenreihe „Strafrechtliche Abhandlungen – Neue Folge“ danke ich den Herausgebern, den Verantwortlichen des Verlages Duncker & Humblot, namentlich Frau Anke Geidel, für die freundliche Betreuung bei der Publikation.

Die Anfertigung einer Dissertation ist, wie alles im Leben, nur möglich (jedenfalls aber leichter), wenn man das Glück hat von unterstützenden Menschen umgeben zu sein. Einigen von ihnen möchte ich im Folgenden meinen Dank aussprechen.

Mein tiefer Dank gilt meinem Doktorvater Herrn Prof. Dr. Hans Kudlich, der mir stets mit wertvollem Rat zur Seite stand und steht – sowohl wissenschaftlich als auch bei anderen Fragen des Lebens. Für die Gewährung größtmöglicher wissenschaftlicher Freiheit bei zugleich bestmöglicher Betreuung bin ich außerordentlich dankbar. Die familiäre, vertrauensvolle Atmosphäre an seinem Lehrstuhl ist von unschätzbarem Wert. Herzlich danken möchte ich zudem Frau Prof. Dr. Gabriele Kett-Straub nicht nur für die zügige Erstellung des Zweitgutachtens, sondern auch dafür, dass auch sie stets ein offenes Ohr hatte – und nicht zuletzt dafür, dass Sie bereits zu Beginn meines Studiums meine Freude am Strafrecht geweckt hat. Außerdem danke ich Herrn Prof. Dr. Christian Jäger, an dessen Lehrstuhl ich als studentische Hilfskraft meine ersten Erfahrungen in der wissenschaftlichen Welt sammeln durfte.

Die Arbeit im Graduiertenkolleg war v. a. aufgrund des steten Austauschs mit den anderen Mitgliedern sehr bereichernd. Aus den Reihen des Graduiertenkollegs danke ich daher besonders: Herrn Prof. Dr.-Ing. Jürgen Teich für die freundliche Unterstützung bei Fragen zu technischen Einzelheiten smarter Geräte, Herrn Prof. Dr. Christoph Safferling für seine kritischen Anregungen und unsere Diskussionen sowie Herrn Prof. Dr.-Ing. Felix Freiling, der mit seiner herzlichen und unkomplizierten Art die Arbeit im Graduiertenkolleg zu einer wahren Freude gemacht hat. Die „AG StPO und IT-Forensik“ ermöglichte regelmäßige interdisziplinäre Diskussionen, für die ich allen Mitgliedern – namentlich dem Initiator der AG, Herrn Prof. Dr. Christian Rückert – sehr dankbar bin. Ebenso denke ich sehr gerne an die GRK-Workshops mit Herrn Dr. Dominic Deuber, Frau Dr. Janine Schneider und Herrn Dr. Jens Trautmann zurück.

Herrn Moritz Gärber und Herrn Mathis Ohlig danke ich vielmals für die tatkräftige redaktionelle Unterstützung, ebenso danke ich Frau Muriel Brixner, Herrn Ali Demir, Herrn Luis Reinwald, Herrn Philipp Schnapp und Herrn Bill Yan, die mir bei der Endkontrolle vor der Drucklegung der Arbeit engagiert zur Seite standen.

Eine große Freude war mein Aufenthalt als Gastwissenschaftler am *Institutet för Rättsinformatik* der Universität Stockholm im Sommer 2022, bei dem eine fortwährende Zusammenarbeit entstand. Ich danke insbesondere Prof. Peter Wahlgren, LL.D. und Prof. Liane Colonna, LL.D. für die herzliche Aufnahme am Institut. Frau Marie Hessel danke ich dafür, dass sie mit ihrer offenen, zugewandten Art der Motor dafür war, Stockholm zu einem zweiten zu Hause für mich werden zu lassen. Tack så jättemycket!

Herzlich danken möchte ich zudem Frau Jana Kuhlmann, Frau Dr. Anna-Lena Nix, Frau Anna Sperber und Herrn Johannes Weichselbaum, die allesamt für eine juristische Sekunde „nur" meine Kollegen waren, doch sofort zu engen Freunden und lieben Begleitern durch Studium, Referendariat, Promotion und das Leben außerhalb des Juridicums wurden. Gleiches gilt für Prof. Dr. Mustafa Temmuz Oğlakcıoğlu, dem ich für unsere vielen inspirierenden und motivierenden Gespräche danken möchte. Ebenso danke ich Herrn Simon Kreiner, der nicht müde wurde, mich nach langen Tagen am Schreibtisch zum Sport zu motivieren.

Besonders danken möchte ich Herrn Bernhard Gahr, Herrn Stefan Gebhard und Frau Susanne Moseev. Unsere schon über Jahrzehnte währende Freundschaft hat mich immer beflügelt und ist mir eine fortwährende Energie- und Glücksquelle, für die ich unermesslich dankbar bin.

Der größte Dank gilt meinen Eltern und meinen Großeltern. Ihnen ist diese Arbeit gewidmet. Sie haben mir schon immer die Freiheit gewährt, mich frei zu entfalten und meine eigenen Ziele zu verfolgen. Ohne ihre Liebe und ihren Rückhalt wäre die Anfertigung dieser Arbeit nicht möglich gewesen. Die Dankbarkeit, die ich dafür empfinde, lässt sich nicht in Worte fassen.

Nürnberg, im Februar 2024 *Florian Nicolai*

Inhaltsübersicht

Inhaltsverzeichnis

Einleitung: Smarte Geräte – Smartes Strafrecht?

Die Welt ist digitalisiert. Vorgänge, die unter dem Topos der *Digitalisierung* stattfinden, sind eine Perpetuierung und Vertiefung einer Ordnung, die in ihrem Kern bereits zu einem Ist-Zustand geworden ist: Das Leben ist digital geworden, viele Abläufe des Alltags sind ohne Internetanbindung nur schwer vorstellbar oder kaum möglich. Selbst in zunächst spärlich in diesen Zustand versetzten Bereichen des Lebens dringt das Digitale immer weiter vor. Damit werden nunmehr auch in Behörden, Gerichten, Schulen und Hochschulen die Umstände und Prozesse an die Bedürfnisse der digitalen Welt angepasst.

Das Recht hingegen ist nicht digitalisiert. Die digitale Progression des Rechts verläuft langsamer. Dies hat nicht nur mit der nötigen Dauer von Gesetzgebungsverfahren und möglicher Scheu vor Veränderung zu tun. Es hängt auch damit zusammen, dass die Veränderungsbedürfnisse des Rechts oftmals erst mit Kenntnis der rechtstatsächlichen Veränderungen und ihren Auswirkungen offenbar, jedenfalls aber erst richtig konturiert, werden können.

Der Grad der Vernetzung des Lebens als Teil der fortschreitenden Digitalisierung hat in den letzten Jahren stetig zugenommen. Dieser Trend setzt sich fort. Fahrzeuge, sog. SmartCars, senden unablässig Daten über Fahrer und Fahrzeug an den Hersteller, der Ofen des sog. SmartHome wird über das Smartphone vorgeheizt, Kinderspielzeug wird zum SmartToy und kann aufgrund einer Internetverbindung mit dem Kind und anderen verbindungsfähigen Geräten kommunizieren, SmartWatches und smarte Gesundheitsgeräte haben ein Auge auf Gesundheit und Fitness des Trägers, Fabriken bestellen automatisch Bauteile für Fertigungsprozesse und in einer über allen Akteuren schwebenden Wolke – der Cloud – laufen sämtliche Informationen zusammen. Die Herausforderungen, die diese Entwicklung für das Recht im Allgemeinen sowie für das Strafrecht im Besonderen hervorbringt, sind vielseitig. Sie bestehen einerseits auf materieller Ebene, wenn die Gesellschaft sich fragen muss, ob diese Systeme sowie die produzierten und gespeicherten Daten strafrechtlich besonderen Schutz erfahren sollen – eine Diskussion, der v. a. die Frage vorauszugehen hat, wie es um den Schutz im materiellstrafrechtlichen *status quo* bestellt ist. Sie bestehen andererseits aber auch auf prozessualer Ebene. All das ließe sich zu einer pointierten Frage stilisieren: Haben wir für die Herausforderungen im Zusammenhang mit smarten Geräten ein smartes Strafrecht?

Schon vor mehreren Jahren wurden Begehrlichkeiten aus dem Bundesinnenministerium laut, denen zufolge Strafverfolgungsbehörden umfassenden Zugriff auf

Daten aus vernetzten Fahrzeugen gewährt werden soll.[1] Die Anpassung rechtlicher Rahmenbedingungen bedarf jedoch eines intensiven Blickes auf sowohl auf die rechtstatsächlichen Gegebenheiten als auch auf die Rechtslage. Chancen und Risiken müssen abgewogen werden, um beschreiben und bewerten zu können, inwieweit das Recht bereits jetzt universell auf neue rechtstatsächliche Entwicklungen angewendet werden kann. Dies gilt für das materielle Strafrecht einerseits, sowie das Strafprozessrecht andererseits.

Unter der rechtstatsächlichen Klammer des „Internets der Dinge" oder „Internet of Things" werden diese Aspekte in der vorliegenden Arbeit untersucht. In einem ersten Kapitel werden die rechtstatsächlichen Grundlagen des Internets der Dinge dargestellt und anhand der Darstellung dreier Anwendungsbereiche der Weg für die rechtliche Diskussion geebnet. Im zweiten Kapitel der Arbeit, wird der materiellrechtliche Zusammenhang zwischen dem Internet der Dinge und dem Strafrecht beleuchtet, wobei die Systeme und Geräte mitsamt den verarbeiteten Daten des Internets der Dinge in ihrer Eigenschaft als potenzielle Angriffsobjeke von Straftaten sowie die strafrechtlichen Ahndungsmöglichkeiten hierzu im Vordergrund stehen. Im dritten Kapitel steht das Internet der Dinge als Erkenntnisquelle der Ermittlungsbehörden im Fokus. Es wird betrachtet, inwieweit Strafverfolgungsbehörden nach der jetzigen Rechtslage Zugriff auf Daten und Systeme gewährt werden kann. Dies wird zudem in einen Kontext strafprozessualer Grundsätze – Verbot der Totalausforschung, Kernbereich höchstpersönlicher Lebensführung, Selbstbelastungsfreiheit – gestellt.

Im Rahmen der rechtlichen Diskussionen soll nicht nur deutlich gemacht werden, dass eine gesellschaftliche Auseinandersetzung mit diesen Fragen notwendig ist, sondern v. a. aufgezeigt werden, dass die rechtstatsächlichen Änderungen durch die Vernetzung des alltäglichen Lebens Auswirkungen auf die Vorschriften des Strafrechts haben und auch auf deren Lesart haben müssen, um die Grundgedanken der Vorschriften nicht auszuhöhlen und sie den Veränderungen der „echten Welt" gerechtwerdend anzuwenden. Die z. T. bereits in anderen Kontexten geführten rechtlichen Auseinandersetzungen mit bestimmten Auslegungs- und Anwendungsproblemen werden damit einerseits konkreter, öffnen andererseits jedoch auch neue Pforten zur Bewertung von Sachverhalten in einer smarten Welt.

[1] Der Spiegel, „Staatlicher Zugriff auf schlichtweg alles, jedes und jeden", abrufbar unter: https://www.spiegel.de/netzwelt/netzpolitik/thomas-de-maiziere-will-umfassenden-zugriff-auf-digitale-sicherungssysteme-a-1181209.html (zuletzt abgerufen am 28. 12. 2023).

Kapitel 1

Rechtstatsächliche Grundlagen

A. Das Internet der Dinge (IoT)

I. Hinführung

Das Internet der Dinge (IoT, von Englisch: Internet of Things) bezeichnet – diverse Definitionsansätze zusammenfassend – ein Netzwerk verschiedener Gegenstände, die eine eigene IP-Adresse haben, miteinander kommunizieren und deren Kommunikationsprozesse nicht ausschließlich menschlich veranlasst sein müssen.[1] Die Geräte weisen dabei verschiedene Sensoren, Steuerungsfunktionen und ggf. Speicher-, jedenfalls aber Übertragungsmöglichkeiten auf. Auf diese Weise können jegliche Gegenstände und Geräte Umweltinformationen, aus der physischen, aber auch aus der virtuellen Welt, aufnehmen, verarbeiten und weiter übermitteln.[2] IoT-Systeme zeichnen sich zudem dadurch aus, dass sie nach Set-Up und Aktivierung weitestgehend ohne menschliches Eingreifen oder Mensch-zu-Maschine-Kommunikation auskommen.[3] Zur Kommunikation untereinander müssen die Geräte miteinander verbunden sein, entweder direkt oder über einen Hub oder ein Endgerät, bspw. ein Smartphone, wobei die Verbindungen entweder kabelgebunden, meistens jedoch kabellos (bspw. über Bluetooth, WiFi, ZigBee, 5G) erfolgen.[4] Die massenhafte Erhebung und Verarbeitung von Daten, die durch zum Teil zahlreiche IoT-Geräte in den jeweiligen Systemen stattfindet, verwandelt „konventionelle" in smarte Infrastruktur.[5] Auf diese Weise können sodann auch solche Geräte und Maschinen miteinander kommunizieren, deren originäre Aufgabe nicht per se die Kommunikation ist. Der Daten- und Informationsaustausch lässt neue Möglichkeiten der Automatisierung zu und kann in sämtlichen Anwendungsbereichen zu Verbesserungen von Sicherheit, Komfort, wirtschaftlichen Aspekten und Nachhaltigkeit

[1] Vgl. zum Begriff auch *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, § 3 Rn. 431 ff.; IERC, Internet of Things, abrufbar unter: http://www.internet-of-things-research.eu/about_iot.htm (zuletzt abgerufen am 28. 12. 2023).

[2] *Onthoni/Sahoo/Neelakantam*, in: IoT Applications for Healthcare Systems, 33; BSI, Die Lage der IT-Sicherheit in Deutschland 2022, 108, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 28. 12. 2023).

[3] *Gleißner/Dotzler/Hartig/Aßmuth/Bulitta/Hamm*, in: Cloud Computing 2021, 1 (2).

[4] *Gleißner/Dotzler/Hartig/Aßmuth/Bulitta/Hamm*, in: Cloud Computing 2021, 1 (2).

[5] *Onthoni/Sahoo/Neelakantam*, in: IoT Applications for Healthcare Systems, 33.