Elektrotechnik & Informationstechnik (2016) 133/7: 345–347. DOI 10.1007/s00502-016-0431-9

Rechtliche Dimension und Lösungsansätze der Rechtsinformatik im Internet der Dinge bei industriellen Arbeitsbeziehungen

R.-D. Kargl, C. Tschohl, W. Hötzendorfer

Das „Internet der Dinge" bringt vor allem für die Industrie ein enormes Entwicklungspotential und schafft neue Sachverhalte, die in verschiedensten Bereichen eine rechtliche Beurteilung erfordern. Der Beitrag soll vor allem die industrielle Dimension des „IoT" fokussieren und einen Überblick bieten, welche Rechtsfragen damit einhergehen, die mit den klassischen Instrumenten des Rechts nur schwer oder bislang gar nicht zu beantworten sind. Dabei wird auch ein Ausblick geboten, welche Möglichkeiten die Disziplin der Rechtsinformatik durch partielle Automatisierung der Rechtsanwendung zu eröffnen vermag. Schließlich wird hervorgehoben, zu welchen Themen diesbezüglich spezieller Forschungsbedarf besteht.

Schlüsselwörter: Internet der Dinge; Industrie 4.0; Haftung; Datenschutz; Zivilrecht

The legal dimension and provided solutions for the Internet of Things and industrial working relationship.

The "Internet of Things" brings an enormous potential for development, especially for industry and creates new situations that require a legal assessment in various fields. The article principally focuses on the industrial dimension of "IoT" and provides an overview of legal issues which will need a rethink of our classical law. It also presents an outlook on the options provided by the field of legal informatics (e.g. partial automation of legal applications). Finally, it will highlight the need for legal research in the field of "IoT".

Keywords: Internet of Things; smart production; liability; data protection; smart contracting; civil law

Eingegangen am 26. Juli 2016, angenommen am 25. August 2016, online publiziert am 14. Oktober 2016

1. Internet of Things in der Smart Production

Das Internet der Dinge ist zur Realität geworden. Einst eine Vision, hielt es in den letzten Jahren Einzug in die heimische Industrie. Sogenannte „Cyber-Physical-Systems" (CPS) sind untereinander vernetzt und tauschen eigenständig Informationen aus. Der automatisierte Vertragsabschluss unter Maschinen (Machine to Machine – M2M) ist nur ein Teil der Möglichkeiten, die sich mit dieser Technologie verwirklichen lassen können. Innerhalb definierter Prozesse reagieren hier Software-Agenten mit einer gewissen Intelligenz auf vordefinierte Ereignisse. Somit ist es möglich, bei Erreichung eines kritischen Lagerbestandes innerhalb von Mikrosekunden just-in-time automatisch die benötigten Rohstoffe für die Produktion nachzubestellen. Die dafür benötigten Technologien stehen zur Verfügung und sind auch bereits im Einsatz. Beispielsweise ist diese Art des Vertragsabschlusses beim High-Frequency-Trading an den internationalen Börsen zum Alltag geworden. Dadurch können mittels Algorithmen innerhalb von Mikrosekunden Transaktionen von Hochleistungsrechnern getätigt und damit rechtsverbindliche Geschäfte abgeschlossen werden.

Der wirtschaftliche Mehrwert durch die Implementierung dieser neuartigen Technologien besteht in einem enormen Kostenreduktionspotential. Durch just-in-time-Bestellungen lassen sich der Lagerbestand und somit die Kosten minimieren. Durch moderne Sensortechnologien und die Vernetzung von CPS lassen sich z. B. auch optimale Umwelt- und Produktionsbedingungen in der Fabrik von Morgen ermitteln und einstellen. Zentrale Kontrollstellen für Vertragsabschlüsse im B2B-Bereich können in Zukunft überflüssig werden, dank Smart Contracts[1] – basierend auf der Blockchain-Technologie.[2]

Aufgrund dieser Vielzahl von technologischen Neuerungen stehen auch die rechtlichen Regelungen vor einem Wandel. Hierbei sind vor allem die zivilrechtlichen Grundlagen des Vertragsabschlusses im Rahmen der Digitalisierung zu analysieren.[3] In weiterer Folge werden die Zurechnung und der Zugang der Willenserklärung fokussiert. Das Internet der Dinge zeichnet sich vor allem durch eine vermehrte Vernetzung von Sensoren aus, welche am Arbeitsplatz installiert werden können. Durch diese Vernetzung werden immer mehr Daten verarbeitet und miteinander verknüpft. Diese Verarbeitung und Verknüpfung in Hintergrundsystemen wird in weiterer

[1] Smart Contracts sind Programm- bzw. Transaktionsprotokolle, welche autonom die Bedingungen eines Vertrags kontrollieren und dessen Bestimmungen bei Eintreten eines vorweg definierten Ereignisses automatisch ausführen können.

[2] Dabei handelt es sich um ein dezentrales, öffentliches, digitales Register. Dabei wird eine Reihe von Datenblöcken, welche Transaktionen beinhalten, mit Prüfsummen versehen. Die Teilnehmer an der Blockchain besitzen Kopien der Eintragungen, die wie eine Kette untereinander verbunden sind. Dabei prüft das Netzwerk an Teilnehmern („Miner") die einzelnen Blöcke autonom. Somit bedarf es keines Mittelsmanns bzw keiner zentralen Kontrollstelle mehr.

[3] U. a. Zurechnung, Zugang, Widerruf und Irrtum nach ABGB.

Kargl, Rolf-Dieter, Research Institute AG & Co KG – Smart.Rights.Consulting, Amundsenstraße 9, 1170 Wien, Österreich (E-Mail: rolf-dieter.kargl@researchinstitute.at); **Tschohl, Christof,** Research Institute AG & Co KG – Smart.Rights.Consulting, Amundsenstraße 9, 1170 Wien, Österreich; **Hötzendorfer, Walter,** Research Institute AG & Co KG – Smart.Rights.Consulting, Amundsenstraße 9, 1170 Wien, Österreich

Folge aus datenschutzrechtlicher Sicht beleuchtet. Die Disziplin der Rechtsinformatik vermag Lösungsansätze für diese Herausforderungen zu liefern, wie in der Folge mit Beispielen gezeigt wird.

2. Zivilrechtliche Herausforderungen[4]

2.1 Zurechnung

Um einen Vertrag wirksam abschließen zu können, bedarf es der Willenserklärungen der Vertragsparteien. Diese müssen nach den allgemeinen Regeln des österreichischen Zivilrechts einer natürlichen oder juristischen Person zurechenbar sein. Wenn nun Software-Agenten für ihre Geschäftsherren Verträge abschließen, muss das Zivilrecht diese Form der Vertretung regeln. Es muss somit festgelegt werden, ob es sich hierbei um einen Boten oder um einen Stellvertreter handelt.[5] Da die Software-Agenten (noch) keine eigenständigen Erklärungen abgeben können, sondern nur die Erklärungen ihres Geschäftsherrn übermitteln können, bedarf es der Programmierung und der dahinterstehenden Person. Erforderlich sind somit ein menschlicher Erklärungstatbestand und ein Willensakt. Im Ergebnis wird man die Software-Agenten als Boten ansehen können, da sie keine eigenen Willenserklärungen abgeben können. Wenn aber Software-Agenten innerhalb bestimmter Parameter eigenständig agieren und in weiterer Folge auch keine unmittelbare Steuerung mehr durch ein menschliches Individuum notwendig ist, muss jeweils im Hinblick auf die konkreten Fähigkeiten des Systems beurteilt werden, ob Software-Agenten unter gewissen Umständen doch als Stellvertreter einzuordnen sind und ob sie sich mit künstlicher Intelligenz zivilrechtlich in einem allenfalls zu definierenden Rahmen sogar selbst verpflichten können. Mit der Zurechnung ist die wirtschaftlich entscheidende Frage verbunden, wer zivilrechtlich für den Vertragsabschluss haftet. Für die Hersteller solcher Systeme ist dabei vor allem das Ausmaß einer allfälligen Produkthaftung von größter Bedeutung.

2.2 Zugang

Willenserklärungen werden erst mit ihrem Zugang im Machtbereich des Erklärungsempfängers wirksam. Dabei wird der Zugang angenommen, wenn die Erklärung derart in den Machtbereich des Erklärungsempfängers gelangt ist, dass nach regelmäßigen Umständen mit Kenntnisnahme durch ihn gerechnet werden kann.[6] Während es bisher eines menschlichen Zutuns bedarf, um Verträge abzuschließen, langt nun die Willenserklärung innerhalb von Mikrosekunden beim Software-Agenten des Erklärungsempfängers ein und es muss damit gerechnet werden, dass die Willenserklärung unter gewöhnlichen Umständen sofort zur Kenntnis genommen wird. Dies führt zu weiteren Problemstellungen beim Widerruf und der Irrtumsanfechtung, denen jedoch weniger mit Technologie sondern vielmehr mit einer Fortentwicklung der Zivilrechtsordnung zu begegnen sein wird.

3. Datenschutzrechtliche Herausforderungen

3.1 Verarbeitung und Verkettung im Hintergrund

Das Internet der Dinge zeichnet sich durch eine vermehrte Vernetzung von Sensoren aus, welche am Arbeitsplatz installiert werden können oder am Körper der Mitarbeiter getragen werden.[7] Durch diese Vernetzung werden immer mehr Daten verarbeitet und miteinander verknüpft. Durch die gesteigerte Anzahl an Verknüpfungsmöglichkeiten steigt auch die Wahrscheinlichkeit eines Personenbezugs, selbst wenn die einzelnen Daten an sich nicht einer Person zugeordnet werden können. Es werden somit – bewusst oder unbewusst – häufig personenbezogene Daten[8] verarbeitet. Hierdurch können Mitarbeiter systematisch überwacht werden, was zu einem datenschutzrechtlichen Problem führen könnte. Das Prinzip der Transparenz fordert, dass personenbezogene Daten „auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“[9] müssen. Das Arbeitsverfassungsgesetz[10] statuiert, dass Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer welche „die Menschenwürde berühren“ nur mit Zustimmung des Betriebsrates zulässig und Gegenstand einer erzwingbaren Betriebsvereinbarung sein sollen.[11] Somit soll die Verarbeitung und Verkettung von personenbezogenen Daten in Hintergrundsystemen zumindest transparent gestaltet werden. Ein weiterer Ansatz zum Schutz vor unbemerktem Auslesen wäre ein Gerät, das die Aktivität von Sensoren, Kameras, Mikrophonen oder Lesegeräten erkennt und diese dem Nutzer anzeigt.[12]

3.2 Privacy by Design

Ein systematischer Ansatz, datenschutzrechtlichen Problemen im Vorhinein entgegenzuwirken und für die Einhaltung der Datenschutzbestimmungen zu sorgen, ist das moderne Prinzip „Privacy by Design“. Dieser von der Datenschutzcommunity entwickelte Grundsatz wird mit der Datenschutz Grundverordnung (DSGVO)[13], die ab 25. Mai 2018 wirksam werden wird, zu einer gesetzlichen Verpflichtung. Art 25 DSGVO verpflichtet unter der Überschrift „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ den Verantwortlichen, dass dieser „geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen“ und „die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.“ Dies erfordert vor allem, bereits bei der Gestaltung von Systemen dafür zu sorgen, dass diese von sich aus möglichst wenig in die Privatsphäre der Betroffenen eingreifen und Eingriffe, die nicht dem Zweck des Systems entsprechen, faktisch wenn möglich gänzlich – oder ansonsten zumindest in den Grundeinstellungen – ausgeschlossen sind. Künftig haben sich also die Verantwortlichen bereits bei der Gestaltung von Systemen intensiv mit dem Datenschutz auseinanderzusetzen.

---

[4] Siehe *Kargl* in [1], Tagungsband des 19. Internationalen Rechtsinformatik Symposions, Die rechtlichen Implikationen bei einem automatisierten Vertragsabschluss – Machine to Machine (M2M) 563ff.

[5] Diese beiden Rechtsfiguren unterscheiden sich dadurch, dass der Bote bloß eine Erklärung überbringt, während der Stellvertreter eine eigene Willenserklärung abgibt.

[6] *Rummel* in [2], ABGB[4], § 862a Rz 2.

[7] Hier ist z. B. der „intelligente Handschuh“ zu erwähnen, welcher z. B. aufzeichnet, wie viele Schrauben ein Mitarbeiter pro Stunde verwendet hat, um so seine Arbeitsleistung zu analysieren und zu bewerten.

[8] Art 4 Abs 1 DSG 2000: „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist.

[9] Art 5 Abs 1 lit a DSGVO.

[10] § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz (ArbVG) idF BGBl. I Nr. 71/2013.

[11] Dazu detailliert *Tschohl*, Datenschutz, Informationssicherheit und DSG 2000, in WEKA Verlag Wien (Hrsg.), Praxishandbuch Betriebsratsarbeit, Kapitel 3, Mitarbeiterüberwachung [3] Loseblattsammlung Register 5.

[12] Siehe auch *Roßnagel*, Datenschutz in einem informatisierten Alltag [4] 160.

[13] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

3.3 Intelligenter automatisierter Datenschutz

Damit Betroffene von einer sie betreffenden Datenverarbeitung rechtzeitig erfahren und damit diese auch auf die Konsequenzen einer solchen aufmerksam gemacht werden, wäre es denkbar, eine Art Datenschutzagent zu entwickeln. Die Automatisierung von Anwendungen in der Industrie von Morgen könnte somit auch den Mitarbeitern und Kunden zu Gute kommen. In der einschlägigen Literaturfindet man dazu etwa die Beschreibung eines „Datenschutzagenten“[14] als eine software-technische Unterstützung, die dem Betroffenen Datenschutzarbeit abnimmt und ihm hilft, Datenverwendungen zu erkennen und auf sie zu reagieren. Denkbar wäre, dass der Benutzer seine Präferenzen zur Datenverarbeitung voreinstellt und der Agent bei einem vordefinierten Ereignis die Einwilligung in die Datenverarbeitung erteilt oder versagt. Da der Agent nach den Präferenzen seines Benutzers handelt, müsste dieser keine Datenschutzerklärungen mehr studieren und könnte auf die datenschutzfreundliche Voreinstellung vertrauen. Dies würde den Prozess der Datenverarbeitung auch in der Industrie transparenter und im Bereich Business to Customer sozial verantwortlicher gestalten.

4. Conclusio und Ausblick

Die Anpassung des Rechtsrahmens in Österreich auf die Automatisierung innerhalb der Digitalisierung wird in den nächsten Jahren von großer Bedeutung sein. Das Ausmaß der semantischen Fähigkeiten der Maschinen wird dabei wesentlich die Anforderungen an das Recht bestimmen. Abschließend sei gesagt, dass es eines Umdenkens bei gewissen Rechtsfiguren bedarf und eine rechtliche Fortentwicklung, bevorzugter Weise in derselben Geschwindigkeit wie die technologische, die nächsten Jahre der juristischen IT-Forschung prägen wird.

Literatur

1. Schweighofer, E., Kummer, F., Hötzendorfer, W., Borges, G. (Hrsg.) (2016): Netzwerke – Networks, In: Tagungsband des 19. Internationalen Rechtsinformatik Symposions, IRIS 2016. Wien: OCG.
2. Rummel, P., Lukas, M. (2015): ABGB Kommentar zum Allgemeinen bürgerlichen Gesetzbuch. Wien: Manz.
3. Praxishandbuch Betriebsratsarbeit (2015): Loseblattsammlung. Wien: Weka.
4. Roßnagel (2007): Datenschutz in einem informatisierten Alltag. Berlin: Friedrich-Ebert-Stiftung.

Autoren

Rolf-Dieter Kargl
hat 2015 an der Wirtschaftsuniversität Wien das Masterstudium „Wirtschaftsrecht“ abgeschlossen und arbeitet seit 2014 als wissenschaftlicher Mitarbeiter des Research Institute. Sein fachlicher Schwerpunkt liegt im Bereich Wirtschaft und Wirtschaftsrecht mit besonderem Fokus auf Datenschutz und IT-Recht. Derzeit studiert er Wirtschaftsinformatik an der Wirtschaftsuniversität Wien und ist am Beginn seines Doktoratsstudiums der Rechtswissenschaften an der Universität Wien. Er ist aktives Mitglied im IoT Austria – The Austrian Internet of Things Network und Co-Organizer von IoT Vienna – The Internet of Things Group of Vienna.

Christof Tschohl
ist Nachrichtentechniker und promovierter Jurist mit Spezialisierung auf IT-Recht und Menschenrechte in der Informationsgesellschaft. Er ist Co-Gesellschafter und wissenschaftlicher Leiter des Research Institute. Er hat unter anderem mit dem Konzept zur „Durchlaufstelle“ und der Datensicherheitsverordnung zum Telekommunikationsgesetz im Auftrag des BMVIT eine „Privacy by Design“-Lösung erarbeitet, die 2012 durch die Bundesregierung umgesetzt wurde und seither dem Datenaustausch zwischen Sicherheitsbehörden und Telekom-Providern dient. Er ist u. a. Obmann des Arbeitskreises Vorratsdaten Österreich (AKVorrat), Vorstandsmitglied und Arbeitskreisleiter in der Österreichischen Computergesellschaft (OCG) sowie Mitglied des Wiener Zentrum für Rechtsinformatik (WZRI).

Walter Hötzendorfer
ist Senior Researcher und Consultant in der Research Institute AG & Co KG in Wien. Er verfügt über Berufserfahrung in der Rechtsberatung und im Software Engineering, war von 2011 bis 2016 in der Arbeitsgruppe Rechtsinformatik der Universität Wien (Institut für Europarecht, Internationales Recht und Rechtsvergleichung) in mehreren großen Forschungsprojekten tätig und promovierte dort zum Thema „Datenschutz und Privacy by Design im föderierten Identitätsmanagement“. Walter Hötzendorfer ist Co-Programmvorsitzender des jährlichen Internationalen Rechtsinformatik Symposions (IRIS) in Salzburg, Geschäftsführer des Wiener Zentrums für Rechtsinformatik, Vorstandsmitglied der Österreichischen Computergesellschaft (OCG) und Co-Leiter des OCG Forum Privacy.

[14] Roßnagel [4]: Datenschutz in einem informatisierten Alltag 159.