

# Was ist das Internet der Dinge?

---

von Jin Ye

---



---

Jin Ye, B. Sc. Wirtschaftsinformatik, studiert Jura an der Universität zu Köln. Sie ist als wissenschaftliche Hilfskraft am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung tätig.

Die Erfindung des Internets hat zu solch umfassenden Veränderungen in nahezu allen Lebensbereichen geführt wie kaum eine andere Erfindung der letzten Jahrzehnte. Als Internet wird ein weltumspannendes, heterogenes Computernetzwerk bezeichnet. Dieses Computernetzwerk ermöglicht den Datenaustausch zwischen den darüber verbundenen Rechnern und damit die Nutzung von Internetdiensten wie bspw. dem World Wide Web oder E-Mail. Mit zunehmender Modernisierung erlangten neben Computern auch weitere Gegenstände wie etwa Mobiltelefone, Uhren und Kühlschränke sowie industrielle Maschinen die Fähigkeit, sich mit dem Internet zu verbinden und darüber zu kommunizieren.

Das Internet der Dinge (engl. Internet of Things, IoT) bezeichnet ebendiese Vernetzung von Gegenständen untereinander über ein Netzwerk, typischerweise das Internet. Neben dem Begriff des Internet of Things ist auch häufig die Rede vom Internet of Everything (IoE) – teilweise werden diese Begriffe synonym, überwiegend jedoch unterschiedlich verwendet.

Ein verbreiteter Ansatz zur Abgrenzung beider Konzepte besteht darin, ausschließlich die Vernetzung von (alltäglichen) Dingen, also Objekten, in das Internet of Things einzubeziehen.

Demnach können im Internet of Things ausschließlich Maschinen mit anderen Maschinen (Machine to Machine, M2M) kommunizieren. Das IoE-Konzept erweitert das IoT-Konzept um die Komponenten Personen, Prozesse und Daten. Damit umfasse das IoE-Konzept neben der M2M-Kommunikation insbesondere auch Machine to People (M2P) sowie technologiegestützte People to People (P2P) -Interaktionen.

Nach einem anderen Ansatz beschreibt das IoT die Vernetzung aller Dinge, die bislang nicht online waren.

Mit dem IoT werde also die nicht digitale Welt digitalisiert bzw. digital abgebildet.<sup>1</sup> Sensoren sammeln Daten und liefern diese an Rechenzentren. Hier endet jedoch die Definition des Internet of Things. Die Analyse und weitergehende Verwertung dieser Daten sei – neben dem IoT – bereits Teil des Internet of Everything. Im IoE gehe es folglich nicht nur um die Digitalisierung, sondern auch und vor allem um eine aussagekräftige Analyse der Daten.

Einigkeit besteht also darüber, dass das Internet of Things keine Personen einbezieht und eine Vorstufe in der Entwicklung zum Internet of Everything bildet.

Dieser Konsens sollte genügen, um die Grundzüge des IoT und seine Anwendungsfelder<sup>2</sup> verstehen zu können.

Die Idee des Internets der Dinge, also einer Welt, in der Gegenstände vernetzt sind, existiert schon lange. Doch erst die Entwicklung einer Vielzahl von Technologien haben sie realisierbar gemacht. Wichtige Voraussetzungen dafür, dass Gegenstände über ein Netzwerk miteinander kommunizieren können ist, neben dem Netzwerk selbst die Ausstattung der physischen Objekte mit entsprechender Hardware wie Sensoren und

<sup>1</sup> Weiterführend zu dem damit verwandten Konzept der digitalen Repräsentanzen *Stark/Damerau*, Digital Twin, CIRP Encyclopedia of Production Engineering, 2019.

<sup>2</sup> Trotz der Einigkeit darüber, dass im IoT Gegenstände vernetzt sind, spielt der Mensch in den meisten Anwendungsfällen doch eine bedeutende Rolle, da jede Technologie letzten Endes dem Anwender zugute kommen soll.

Transpondern<sup>3</sup> sowie die Mikroprozessortechnik. Erst in den letzten Jahren wurden Sensoren erschwinglich und zuverlässig genug, um sie einem großen Abnehmermarkt zugänglich zu machen. Darüber hinaus hat die Entwicklung im Bereich des Natural Language Processing (NLP) ermöglicht, dass IoT-Geräte auch natürliche Sprache verarbeiten können.

Für ein funktionierendes IoT-System genügt allerdings nicht, dass sämtliche Objekte im Internet vernetzt sind und kommunizieren können, vielmehr müssen diesen auch eindeutige Identitäten zugewiesen sein.

Eine Technologie, die dies drahtlos ermöglicht ist die Radiofrequenzidentifikation (RFID).

Die Hardware eines RFID-Systems besteht aus einem Identifikations-Transponder, sog. „Tag“, der gelesen wird, sowie einem Lesegerät.

Der Transponder fungiert sowohl als „Transmitter“ als auch als „Responder“, d.h. er kann senden und empfangen. Das Lesegerät erzeugt ein elektromagnetisches Wechselfeld, dem der Transponder ausgesetzt wird.

Dadurch wird ein Mikrochip im Transponder aktiviert, welcher die vom Lesegerät gesendeten Befehle empfängt und decodiert. Der Transponder codiert die Antwort in das elektromagnetische Feld durch Feldschwächung und sendet damit seine Seriennummer sowie andere vom Lesegerät abgefragte Informationen. Er erzeugt also kein eigenes Feld, sondern antwortet, indem er das elektromagnetische Sendefeld des Lesegeräts beeinflusst.

Auf dieser Technologie basiert die Technik der Near Field Communication (NFC), die ebenfalls häufig im Zusammenhang mit IoT genannt wird. Die wichtigsten Unterschiede zu RFID sind, dass NFC nicht nur Tags lesen, sondern auch Informationen schreiben kann und somit die Übertragung von Daten in beide Richtungen möglich ist. Im deutschen Personalausweis sind beispielsweise Tags eingebaut, welche die elektronische Authentisierung ermöglichen. Auch der kontaktlose Zutritt – beispielsweise von Dauerparkern eines Parkhauses – wird häufig mittels RFID-

<sup>3</sup> Transponder: ein Funk-Kommunikationsgerät, das eingehende Signale aufnehmen und beantworten bzw. weiterleiten kann

Technologie umgesetzt. Der Dauerparker erhält einen Tag, welches vom Lesegerät erkannt wird, sobald er sich nähert, sodass die Schranke geöffnet wird. Bargeldloses Zahlen per Smartphone an der Supermarktkasse wird hingegen mit NFC ermöglicht.

Das Internet of Things kann grundsätzlich in nahezu allen Lebensbereichen eingesetzt werden. Im privaten Umfeld sollen IoT-Geräte vorrangig das Alltagsleben erleichtern.

In diesem Zusammenhang ist häufig die Rede von einem Smart Home-System.

Beispiel:

Lisa stellt im Supermarkt fest, dass sie ihre Einkaufsliste vergessen hat. Als Abendessen hatte sie Gemüseauflauf geplant – hat sie noch Käse zu Hause? Ist der Spinat noch frisch? Sie zieht ihr Handy aus der Tasche und sieht nach – Käse hat sie noch, Spinat sollte sie lieber neu kaufen. Als Lisa mit vollen Händen in ihr beleuchtetes Zuhause kommt, freut sie sich, nicht im Dunkeln nach dem Lichtschalter tasten zu müssen. Sie bittet Alexa<sup>4</sup> ihre Haushalts-Playlist zu spielen, während sie sich in die Küche begibt, um den Einkauf auszuräumen. Bei einem Blick in den Garten freut sie sich, nicht noch ihre Blumen gießen zu müssen.

Ein Szenario, das bei vielen Menschen bereits Alltag ist – doch wie funktioniert das Ganze?

Lisa konnte im Supermarkt in ihren Kühlschrank schauen, weil in diesem eine Kamera verbaut ist und dieser mit dem Internet verbunden ist, weshalb sie auch unterwegs darauf zugreifen konnte. Das Licht ging automatisch an, als Lisa so nahe war, dass ihr Handy sich im WLAN eingeloggt hatte. Der Zustand der Blumen wird über Sensoren gemessen, welche diesen an den Aktor kommunizieren. Ein Aktor ist eine Einheit, die ein elektrisches Signal – beispielsweise ‚1‘ für trocken – in mechanische Bewegungen bzw. Veränderungen physikalischer Größen wie Druck oder Temperatur umsetzt und damit aktiv in den gesteuerten Prozess eingreifen kann. Er dient sozusagen der Ausführung von Aktionen. In diesem Fall ist der Aktor die Bewässerungsanlage, die auf das Signal hin die Blumen gießt.

<sup>4</sup> Eine virtuelle, auf KI-Technologie gestützte Smart Home-Assistentin.

Neben dem Begriff des Internet of Things hat sich auch der Begriff des Industrial Internet of Things (IIoT) für die industriellen Anwendungen herausgebildet.

Beispielsweise kann durch IIoT in den Bereichen Fertigung, vorbeugende und vorausschauende Wartung sowie Logistik ein höherer Automatisierungsgrad, geringere Downtime und effizientere Prozesse gewährleistet werden.

Je umfassender die Vernetzung ist, desto mehr Vorteile können aus ihr gezogen werden. Allerdings kann jedes einzelne IoT-Gerät – wie auch jedes andere internetfähige Gerät – gehackt werden.

Mit jedem neuen internetfähigen Gerät, das einem Netzwerk hinzugefügt wird, entsteht also eine neue Angriffsfläche, die es abzusichern gilt. Weitere Aspekte, die vor Implementierung einer IoT-Lösung bedacht werden sollten, sind die Datenschutzbestimmungen des Anbieters sowie die Interoperabilität des Systems, aber auch, wie das System sich verhält, wenn beispielsweise das Internet oder der Cloud-Server ausfällt – sonst ärgert man sich, plötzlich im Dunkeln zu sitzen<sup>5</sup> oder wenn die Blumen vertrocknen.

Das Internet of Things zeichnet sich letzten Endes dadurch aus, dass es nicht „die eine“ Technologie ist, sondern erst ein Zusammenspiel unzähliger Technologien dieses vernetzte System bilden, das als Internet of Things oder Internet of Everything bezeichnet wird.

Wie jede Technologie sollte das Internet der Dinge in erster Linie ein Hilfsmittel für den Menschen sein. Bei der Anwendung von IoT-Geräten ist es demnach in vielen Fällen wichtig, dass der Anwender auch bei vollautomatisierten Abläufen zwischen zwei oder mehr Geräten eine Zugriffsmöglichkeit behält. Ob und inwieweit der Nutzen gegenüber den Risiken überwiegt, muss der einzelne Anwender von Fall zu Fall entscheiden.

<sup>5</sup> Das Start-up Emberlight entwickelte smarte Lampen-Sockel für eine Lichtsteuerung ohne Lichtschalter, dafür mit Verbindung zu Cloud-Servern des Unternehmens, die mit herkömmlichen Glühlampen funktioniert. Leider ging das Start-up in Konkurs, sodass die Server abgestellt wurden und die Lampen nicht mehr ein- und ausgeschaltet werden konnten, vgl. <https://netzpolitik.org/2020/internet-der-dinge-die-produkte-gehoren-gar-nicht-uns/> (zuletzt abgerufen am 19.01.2021).

**Weiterführend:**

Bei weiterführendem Interesse am Internet der Dinge ist zunächst eine Auseinandersetzung mit den Technologien RFID und NFC empfehlenswert, ebenso die Auseinandersetzung mit dem Konzept der digitalen Zwillinge und in diesem Zusammenhang mit sogenannten cyber-physical systems.

Zu digitalen Zwillingen: <https://www.iosb.fraunhofer.de/de/geschaeftsfelder/automatisierung-digitalisierung/anwendungsfelder/digitaler-zwilling.html>

Zu den Anwendungsbeispielen Wearables, Smart Home u.a. finden sich auch weitere Ausführungen auf der Seite des BSI:  
[https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/loT/loT\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/loT/loT_node.html)

Mehr zum Industrial Internet of Things:  
<https://www.iosb.fraunhofer.de/de/geschaeftsfelder/automatisierung-digitalisierung/anwendungsfelder/iiot.html>



1/21

1. Jahrgang, 1. Ausgabe  
[www.legaltechcologne.de/ctrl](http://www.legaltechcologne.de/ctrl)

# CTRL

Cologne Technology **R**&Law  
review

+  
Hier geht es  
zur ganzen Ausgabe.

Dort findest Du  
auf über 80 Seiten in  
15 Aufsätzen alles  
von Legal Tech über  
KI und Blockchain bis  
hin zu digitaler Lehre.