

36. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 13. bis 16. Oktober 2014 in Balaclava, Mauritius

### **Erklärung von Mauritius zum Internet der Dinge**

Das Internet der Dinge wird bleiben. Immer mehr Gegenstände sind mit dem Internet verbunden und in der Lage, miteinander zu kommunizieren, manchmal ohne dass die Nutzenden dies bemerken. Diese Gegenstände können unser Leben sehr viel einfacher machen. Zum Beispiel bei der Gesundheitsversorgung, beim Transport oder der Energieversorgung können die verbundenen Gegenstände die Art und Weise verändern, mit der wir etwas erledigen. Das Internet der Dinge kann allerdings auch intime Details über das Handeln und die Bewegungen der Eigentümer von Gegenständen mithilfe der in ihnen enthaltenen Sensoren offenbaren.

Selbstbestimmung ist ein unveräußerliches Recht aller Menschen. Die persönliche Entwicklung sollte nicht dadurch festgelegt werden, was Unternehmen und Regierungen über den Einzelnen wissen. Die Ausbreitung des Internets der Dinge vergrößert allerdings das Risiko, dass dies geschehen wird. Die versammelten Beauftragten für Datenschutz und Privatsphäre haben deshalb die Möglichkeiten des Internets der Dinge und seine Konsequenzen während der 36. Internationalen Datenschutzkonferenz diskutiert, die in Balaclava, Mauritius am 13. und 14. Oktober 2014 stattfand. Vier Redner, die sowohl den wirtschaftlichen Sektor als auch die Wissenschaft repräsentierten, stellten den Beauftragten die positiven Veränderungen wie auch die Risiken vor, die das Internet der Dinge in unser tägliches Leben bringen kann. Die Redner gaben außerdem einen Überblick darüber, was getan werden muss, um den weiteren Schutz unserer personenbezogenen Daten wie auch unseres Privatlebens sicherzustellen.

Die anschließende Diskussion führte zu den folgenden Empfehlungen:

- Die beim Internet der Dinge verwendeten Sensoren erzeugen Daten in hoher Quantität, Qualität und Sensitivität. Dies bedeutet, dass sehr viel weiterreichende und sensitivere Folgerungen gezogen werden können und die Herstellung eines Personenbezugs wahrscheinlicher ist als dessen Vermeidung. Angesichts der Tatsache, dass die Personenbeziehbarkeit und der Datenschutz im Zusammenhang mit „Big Data“ an sich schon eine große Herausforderung sind, ist es deutlich, dass große Datenmengen, die von Gegenständen im Internet der Dinge gewonnen werden, diese Herausforderungen um ein Vielfaches vergrößern. Deshalb sollten solche Daten als personenbezogen angesehen werden.
- Obwohl für viele Unternehmen das Geschäftsmodell noch unbekannt ist, liegt der Wert des Internets der Dinge eindeutig nicht nur in den Geräten selbst. Das finanzielle Interesse liegt in den neuen Diensten im Zusammenhang mit dem Internet der Dinge und in den Daten.
- Jeder, der heute lebt, wird erkennen, dass Konnektivität allgegenwärtig ist. Dies mag noch mehr der Fall sein für die junge und zukünftige Generationen, die sich keine Welt ohne Vernetzung vorstellen können. Es sollte aber nicht allein ihre Aufgabe sein, ob ihre Daten geschützt werden oder nicht. Es ist eine gemeinsame Verantwortung aller Handelnden in der Gesellschaft, damit das Vertrauen in vernetzte Systeme aufrechterhalten werden kann. Dafür ist Transparenz von entscheidender Bedeutung: Wer Dienstleistungen im Internet der Dinge anbietet, sollte klar sagen, welche Daten er sammelt, für welche Zwecke und wie lange diese Daten gespeichert werden. Er sollte Überraschungen für Verbraucher ausschließen. Beim Kauf von Gegenständen des Internets der Dinge oder entsprechender Programme sollte eine angemessene ausreichende und verständliche Information zur Verfügung stehen. Gegenwärtige Da-

tenschutzerklärungen vermitteln nicht immer die Information in einer klaren, verständlichen Weise. Einwilligungen, die auf der Basis solcher Datenschutzerklärungen erteilt werden, können kaum als informierte Einwilligungen angesehen werden. Unternehmen müssen ihre Herangehensweise grundlegend verändern, damit Datenschutzerklärungen nicht länger in erster Linie dem Zweck dienen, sie vor Klagen zu schützen.

- Die Datenverarbeitung beginnt in dem Moment der Datenerhebung. Alle Schutzmaßnahmen sollten ab diesem Zeitpunkt greifen. Wir ermutigen zur Entwicklung von Technologien, die neue Wege der Einbeziehung von Datenschutz und Verbraucherschutz von Anfang an ermöglichen. „Privacy by Design and Default“ sollte nicht länger als etwas Abseitiges betrachtet werden. Beide Prinzipien sollten ein wesentliches Verkaufsargument für innovative Technologien werden.
- Das Internet der Dinge wirft auch wesentliche Sicherheitsrisiken auf, die beherrscht werden müssen. Eine einfache Firewall reicht längst nicht mehr aus. Ein Weg, um das Risiko für Betroffene zu begrenzen, liegt darin, dass man die Datenverarbeitung auf das Endgerät selbst beschränkt (lokale Verarbeitung). Wenn dies nicht möglich ist, sollten Unternehmen Ende-zu-Ende-Verschlüsselung vorsehen, um die Daten vor ungerechtfertigter Einwirkung oder Manipulation zu schützen.
- Die Datenschutz- und Privatsphäre-Behörden werden weiterhin die Entwicklungen beim Internet der Dinge beobachten. Sie machen es sich zur Aufgabe, die Befolgung der Datenschutzgesetze in ihren jeweiligen Ländern sicherzustellen, ebenso wie die Einhaltung der international akzeptierten Prinzipien. Wenn Rechtsverstöße festgestellt werden, werden sie angemessene Sanktionsmaßnahmen ergreifen, entweder einseitig oder durch internationale Zusammenarbeit.
- Angesichts der großen Herausforderungen, denen sich die Entwickler im Internet der Dinge, die Datenschutzbehörden und die Betroffenen gegenübersehen, sollten sich alle Beteiligten an einer starken, aktiven und konstruktiven Debatte zu den Konsequenzen des Internets der Dinge und der aus ihm gewonnenen großen Datenmenge beteiligen, um das Bewusstsein für die zu treffenden Entscheidungen zu erhöhen.

*Jacob Kohnstamm*

(Vorsitzender des Exekutivkomitees der Internationalen Datenschutzkonferenz)

*Drudeisha Madhub*

(Vorsitzende der Datenschutzbehörde von Mauritius)