*Europäischer Wirtschafts- und Sozialausschuss*

**INT/846**
**Vertrauen, Privatsphäre und Sicherheit / Internet der Dinge**

# STELLUNGNAHME

Europäischer Wirtschafts- und Sozialausschuss

**Vertrauen, Privatsphäre und Sicherheit für Verbraucher und Unternehmen im Internet der Dinge**
[Initiativstellungnahme]

Berichterstatter: **Carlos TRIAS PINTÓ**
Mitberichterstatter: **Dimitris DIMITRIADIS**

| | |
|---|---|
| Beschluss des Plenums | 15/02/2018 |
| Rechtsgrundlage | Artikel 29 Absatz 2 der Geschäftsordnung<br>Initiativstellungnahme |
| Zuständige Fachgruppe | Fachgruppe Binnenmarkt, Produktion, Verbrauch |
| Annahme in der Fachgruppe | 04/09/2018 |
| Verabschiedung auf der Plenartagung | 19/09/2018 |
| Plenartagung Nr. | 537 |
| Ergebnis der Abstimmung<br>(Ja-Stimmen/Nein-Stimmen/Enthaltungen) | 182/3/2 |

1. **Schlussfolgerungen und Empfehlungen**

1.1 Das Internet der Dinge (Internet of Things, IoT) eröffnet Bürgern und Unternehmen durch die Interkonnektivität von Personen und Gegenständen ein riesiges Spektrum an Möglichkeiten. Für eine erfolgreiche Umsetzung ist allerdings eine Reihe von Garantien und Kontrollen notwendig.

1.2 Da einer der Grundpfeiler des IoT darin besteht, dass Entscheidungen automatisch getroffen werden, in die der Mensch nicht eingreift, sollte sichergestellt werden, dass die Entscheidungen nicht die Verbraucherrechte untergraben und weder mit ethischen Risiken verbunden sind noch im Konflikt mit Grundsätzen oder grundlegenden Menschenrechten stehen.

1.3 Der EWSA fordert die EU-Organe und die Mitgliedstaaten dazu auf:

1.3.1 zum Schutz der Sicherheit und der Privatsphäre einen angemessenen Rechtsrahmen zu erarbeiten, der strenge Überwachungs- und Kontrollmaßnahmen vorsieht;

1.3.2 die Haftung aller Akteure in der Produktlieferkette und die damit zusammenhängenden Informationsströme genau festzulegen, damit keine Rechtslücken entstehen, wenn verschiedene Hersteller und Händler gleichzeitig beteiligt sind;

1.3.3 angemessene Ressourcen bereitzustellen und wirksame Mechanismen für die Koordination zwischen der Europäischen Kommission und den Mitgliedstaaten einzuführen, mit denen die kohärente und einheitliche Umsetzung sowohl der zu überarbeitenden als auch neuer Rechtsvorschriften gewährleistet wird und die zugleich das internationale Umfeld berücksichtigen;

1.3.4 die Entwicklung neuer Technologien im Zusammenhang mit dem IoT zu überwachen, um hohe Sicherheit, umfassende Transparenz und faire Zugangsbedingungen zu gewährleisten;

1.3.5 europäische und internationale Normungsinitiativen zu fördern, mit denen die Zuverlässigkeit, die Verfügbarkeit, die Belastbarkeit und die Instandhaltung von Produkten gewährleistet wird;

1.3.6 die Märkte zu überwachen und für gleiche Wettbewerbsbedingungen bei der Einführung des IoT zu sorgen, damit es nicht zu einer Konzentration transnationaler Wirtschaftsmacht in den Händen der auf dem Gebiet der neuen Technologie tätigen Akteure kommt;

1.3.7 sich im Bereich digitaler Kompetenzen zur Förderung von Sensibilisierungs- und Schulungsmaßnahmen in Verbindung mit Grundlagenforschung und Innovationen auf diesem Gebiet zu verpflichten;

1.3.8 die vollständige Umsetzung und wirksame Verwendung der Verfahren der alternativen Streitbeilegung und der Online-Streitbeilegung (ADR und ODR) zu gewährleisten;

1.3.9 sich für die Einführung, die Umsetzung und das reibungslose Funktionieren einer europäischen Regelung für Sammelklagen einzusetzen, die Unterlassungs- und Schadensersatzklagen ermöglicht, auch wenn durch die Nutzung des Internets der Dinge kollektive Schäden oder

Verluste entstehen. Dies sollte Gegenstand der Neugestaltung der Rahmenbedingungen für die Verbraucher („New Deal for Consumers“) sein.

1.4 Das Vertrauen der Verbraucher beruht auf der strikten Einhaltung der einschlägigen Rechtsvorschriften und der Verbreitung einer guten Unternehmenspraxis im Bereich Privatsphäre und Sicherheit. Es ist Aufgabe der Organe, diese in die Strategien für die soziale Verantwortung der Unternehmen und sozial verantwortliche Investitionen zu integrieren.

1.5 Das IoT wird sich zunehmend positiv auf Gesellschaft und Wirtschaft auswirken, sofern es angemessen mit der Entwicklung sozial- und umweltpolitischer Maßnahmen im Rahmen der kollaborativen Wirtschaft, der Kreislaufwirtschaft und der Functional Economy verknüpft wird.

## 2. Hintergrund und Kontext

2.1 Durch die rasante Entwicklung des Internets kam es in den letzten 15 Jahren in allen Bereichen des täglichen Lebens zu Veränderungen, die sich auch auf die verschiedenen Verbrauchergewohnheiten auswirken. Aller Voraussicht nach wird die IoT-Revolution in den nächsten zehn Jahren den Energie-, Agrar- und Verkehrssektor sowie traditionellere Wirtschafts- und Gesellschaftsbereiche erreichen, weshalb ganzheitliche Strategien für einen klugen Umgang mit diesen technologischen Umwälzungen notwendig sind.

2.2 Das IoT-Konzept entstand im Massachusetts Institute of Technology (MIT) und basiert im Kern auf einer Welt, in der Geräte vollständig miteinander vernetzt sind, sodass verschiedene interoperable Prozesse gemeinsam automatisiert werden können. Die Europäische Union bereitet sich seit längerem auf die Bewältigung der digitalen Konvergenz und der neuen IoT-Herausforderungen vor: angefangen mit dem Plan „i2010 – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“[1] bis hin zum jüngsten Aktionsplan zum Internet der Dinge (siehe das 2016 vorgelegte Arbeitsdokument der Kommissionsdienststellen *Advancing the Internet of Things in Europe* zur Mitteilung *Digitalisierung der europäischen Industrie. Die Chancen des digitalen Binnenmarkts in vollem Umfang nutzen*[2]).

2.3 Der EWSA hat sich wiederholt zur vierten industriellen Revolution geäußert, die sich durch die Konvergenz von digitalen, physikalischen und biologischen Technologien auszeichnet. Er verweist hierbei insbesondere auf seine Stellungnahme aus dem Jahr 2017[3]. Das Internet der Dinge ist nämlich das bevorzugte Anwendungsgebiet für die modernsten Formen der künstlichen Intelligenz, auf dem auch die vom EWSA definierten Grundsätze – insbesondere das Prinzip der „Kontrolle durch den Menschen“ („human in control“) – auf die Probe gestellt werden.

---

1 COM(2005) 229 final.

2 COM(2016) 180 final.

3 Künstliche Intelligenz – die Auswirkungen der künstlichen Intelligenz auf den (digitalen) Binnenmarkt sowie Produktion, Verbrauch, Beschäftigung und Gesellschaft – ABl. C 288 vom 31.8.2017, S. 1.

2.4 IoT-Geräte erfüllen oft nicht die zum Schutz der Nutzerdaten erforderlichen Authentifizierungsstandards. Dadurch können Probleme entstehen, weil die Geräte, Daten und Akteure in der Lieferkette Sicherheitslücken ausgesetzt sind.

2.5 Neue Technologien wie die Blockchain-Technologie können Sicherheitsproblemen und dem Verlust von Vertrauen entgegenwirken: Sie können eingesetzt werden, um Messungen von Sensordaten nachzuvollziehen, Kopien mit manipulierten Daten zu verhindern, aber auch um die Integrität und die Rückverfolgbarkeit von Modifikationen zu gewährleisten. Dank eines dezentralen Rechnungsbuchs können IoT-Geräte erkannt, Authentifizierungen durchgeführt und Daten sicher und ohne Ausfälle übertragen werden. IoT-Sensoren können dazu verwendet werden, Daten über eine Blockchain statt über einen Dritten zu übertragen. Die Verwendung von Smart Contracts (intelligenten Verträgen) ermöglicht die Autonomie von Geräten sowie eine einzigartige Identität und Datenintegrität. Die Einführungs- und Betriebskosten sind aufgrund des fehlenden Intermediärs vergleichsweise gering. Zu guter Letzt speichern die IoT-Geräte der Blockchain den Verlauf der vernetzten Geräte, wodurch mögliche Probleme leichter gelöst werden können[4].

2.6 Auf der anderen Seite werden derzeit Open-Source-Technologien entwickelt, die den Austausch von Informationen und Werten zwischen Maschinen im IoT ermöglichen. Sie erlauben kein Datamining, sondern nutzen eine Architektur auf Grundlage eines mathematischen Konzepts, das als gerichteter azyklischer Graph (engl. directed acyclic graph, kurz DAG) bekannt ist. Dabei fallen keine Transaktionskosten an, und die Kapazität des Netzwerks (Tangle) nimmt mit der Anzahl der Nutzer zu.

2.7 Wir stehen vor einem enormen wirtschaftlichen[5] und sozialen Potenzial, das große Chancen eröffnet, aber aufgrund seines multidisziplinären und bereichsübergreifenden Charakters auch erhebliche Herausforderungen und entsprechende Risiken mit sich bringt, die gleichermaßen Unternehmen, Verbraucher, Behörden und Bürger betreffen. Bei diesem Thema sollte daher ein gemeinsamer Ansatz verfolgt werden, allerdings sollten zugleich auch Besonderheiten bestimmter Fälle berücksichtigt werden. Die Vereinten Nationen gehen davon aus, dass im Jahr 2020 die Zahl der vernetzten Geräte bei 50 Milliarden liegen wird und u. a. Fernsehgeräte, Kühlschränke, Überwachungskameras und Fahrzeuge mit entsprechenden Verbraucheranwendungen ausgestattet sein werden.

2.8 IoT-Anwendungen bringen in einer globalisierten Welt bereits jetzt wirtschaftliche und soziale Vorteile mit sich. Hierzu gehören u. a. die Erweiterung des Angebots sozioökonomisch orientierter Dienste, kürzere Rückkopplungszyklen, Fernwartung, Unterstützung bei der Entscheidungsfindung, eine bessere Zuweisung von Ressourcen oder die Fernsteuerung von Diensten. Es gibt allerdings auch höchst sensible Faktoren – wie Privatsphäre und Sicherheit, Informationsasymmetrien und die Transparenz von Transaktionen, komplizierte Haftung,

---

4 Siehe Khwaja Shaik, *Why blockchain and IoT are best friends*, https://www.ibm.com; bzgl. Innovationen im europäischen Finanzsektor siehe ABl. C 246 vom 28.7.2017, S. 8.

5 Schätzungen von Digital McKinsey zufolge liegt das wirtschaftliche Potenzial des IoT für das Jahr 2025 bei einem Jahreswert zwischen 3,9 Milliarden und 11,1 Milliarden USD.

Produkt- und Systemsperren oder auch die Zunahme hybrider Produkte, die die Eigentums- und Besitzverhältnisse verändern und die Verbraucher dazu bewegen, Fernabsatzverträge mit eingeschränkten Garantien abzuschließen.

2.9 Die EU und ihre Mitgliedstaaten stehen vor enormen rechtlichen Herausforderungen, da viele Merkmale des IoT (hohe Komplexität und eine hohe gegenseitige Abhängigkeit, Autonomie, die Erzeugung und/oder Verarbeitung von Daten und die Offenheit) auch auf andere neue digitale Technologien wie Blockchain, 3D-Druck und Cloud-Computing zutreffen. Der EWSA ist der Ansicht, dass das Arbeitsdokument der Europäischen Kommission über die Haftung für neue digitale Technologien[6] ein weiterer Schritt in die richtige Richtung ist.

2.10 Um den Nutzen des IoT zu maximieren und die Risiken auf ein Minimum zu reduzieren, ist es erforderlich, zugängliche, eindeutige, prägnante und präzise Informationen bereitzustellen, insbesondere die Inklusion und digitale Anbindung der schutzbedürftigsten Verbraucher zu fördern und vollständig rückverfolgbare Produkte und Dienste anhand integrierter Standards hinsichtlich Vertrauen, Privatsphäre und Sicherheit zu gestalten.

## 3. Vertrauen der Verbraucher und Unternehmen in das IoT

3.1 Das IoT ist ein komplexes Ökosystem, das die Vernetzung von Geräten unterschiedlicher Hersteller, Händler und Softwareentwickler ermöglicht. Das kann die Klärung von Haftungsfragen erschweren, wenn es zu Verstößen gegen Vorschriften oder zu Sachschäden oder sonstigen Schäden für Dritte oder Systeme durch defekte Produkte oder durch über das Netz durch Dritte (mit Ausnahme der Endnutzer) zweckentfremdete Produkte kommt. Es ist sogar möglich, dass viele der Akteure in der globalen Wertschöpfungskette des Produkts nicht über ausreichende Kenntnisse und Erfahrung auf den Gebieten Sicherheit und Datenschutz bei Netzwerkgeräten verfügen.

3.2 Daher ist bei der Haftung ein neuer Ansatz erforderlich, wonach sowohl die Verbraucher als auch die Unternehmen, die IoT-Anwendungen nutzen, in einem Umfeld geschützt werden, in dem richtig konfigurierte Produkte infolge digitaler Sicherheitsvorfälle defekt oder unzulässig zweckentfremdet (z. B. durch Hacker) und unsicher werden können. In diesem Umfeld sollte es möglich sein, automatisierte Entscheidungen, die die allgemein anerkannten ethischen Grundsätze und Menschenrechte verletzen, vorherzusehen, zu verhindern und sich davor zu schützen.

3.3 Der EWSA begrüßt sowohl die Überarbeitung der Richtlinie aus dem Jahr 1985 über die Haftung für fehlerhafte Produkte[7] als auch die unlängst erfolgte Einrichtung einer Multistakeholder-Sachverständigengruppe für Haftung und neue Technologien, die ein Interessengleichgewicht zwischen Herstellern und Verbrauchern gewährleisten soll. Durch einen neuen Haftungsrahmen sollte sichergestellt werden, dass Haftung und Sicherheit entlang der Wertschöpfungskette sowie während der Lebensdauer des Produkts eindeutig nachvollzogen

6 SWD(2018) 137.

7 COM(2018) 246 final.

werden können. Dabei sollte Nachhaltigkeit als neuer Faktor berücksichtigt werden, der dazu verpflichtet, die Aktualisierung, Verbesserung, Portabilität, Kompatibilität, Wiederverwendung, Reparatur oder Anpassung von Produkten zu ermöglichen.

3.4 Im Zusammenhang mit dem IoT sollte insbesondere in Erwägung gezogen werden, für alle Akteure in der Produktlieferkette die Haftung zu bestimmen, damit keine Rechtslücken entstehen, wenn verschiedene Hersteller und Händler gleichzeitig beteiligt sind. Der EWSA hält es für unerlässlich, eindeutig festzulegen, welche Verfahren die Verbraucher in jedem Fall durchlaufen müssen, wobei alternative Streitbeilegungsverfahren zu fördern sind.

3.5 Der EWSA unterstreicht die Bedeutung vorvertraglicher Informationen, transparenter Vertragsbestimmungen und klarer Bedienungsanleitungen für Geräte. Etwaige Risiken und Schutzvorkehrungen sollten ausdrücklich hervorgehoben werden.

3.6 Die Interoperabilität und Kompatibilität von Geräten und der damit verbundenen Software muss gewährleistet werden, um Schwierigkeiten zu vermeiden und dem Verbraucher die Möglichkeit zu geben, die Anbieter miteinander zu vergleichen. Der EWSA betont, dass dieser Faktor auch für die Schaffung gleicher Wettbewerbsbedingungen zwischen großen Unternehmen und KMU von entscheidender Bedeutung ist.

3.7 Schließlich spricht sich der EWSA für die Achtung der Netzneutralität aus und fordert die Kommission auf, das Marktverhalten genau zu überwachen.

## 4. Privatsphäre der Verbraucher im IoT

4.1 Durch die neue Datenschutz-Grundverordnung (DS-GVO)[8] haben die Verbraucher nun mehr Kontrolle über ihre persönlichen Daten und Privatsphäre-Präferenzen. Der Nutzer eines Geräts sollte darüber entscheiden können, wie die von ihm generierten Daten genutzt werden und wer darauf zugreifen darf, denn durch die Datenvielfalt, -aggregation und -verknüpfung wird die Privatsphäre im IoT-Ökosystem ernsthaft gefährdet.

4.2 Ebenfalls zu berücksichtigen ist, wie sich die Vielzahl von Produkten, Diensten und Entitäten auf die Privatsphäre und den Datenschutz auswirkt, wenn Daten aufgrund von Interkonnektivität automatisch übertragen werden. Ebenso könnten durch die Verarbeitung oder Weiterverarbeitung von Informationen aus ursprünglich harmlosen Daten genaue Erkenntnisse über die Gewohnheiten, Aufenthaltsorte, Interessen und Vorlieben einzelner Personen gewonnen werden, sodass das Profil des Nutzers leichter zugänglich wird und nachverfolgt werden kann.

4.3 Rechtliche Garantien sollten gewährleisten, dass die Nutzer ihre Rechte auf Privatsphäre und den Schutz personenbezogener Daten uneingeschränkt wahrnehmen können. So können mögliche negative Auswirkungen wie diskriminierende Praktiken, aufdringliche Vermarktung, der Verlust der Privatsphäre oder Sicherheitsverstöße verhindert werden. Die Verbraucher

8 Am 25. Mai 2018 in Kraft getreten.

ihrerseits müssen über Informationen über den wirtschaftlichen Wert ihrer Daten verfügen und sich das Recht vorbehalten, diese zu teilen.

4.4 Wie in der DS-GVO vorgesehen, sollten Unternehmen und Regulierungsbehörden regelmäßig das Ausmaß der Erhebung personenbezogener Daten überprüfen und die Verhältnismäßigkeit und Notwendigkeit der verarbeiteten Daten für die Diensteerbringung bewerten. Die Aspekte und Auswirkungen der Privatsphäre sollten in jeder Phase der Planung, der Konzeption und der Entwicklung eines vernetzten Produkts und des Online-Ökosystems, in das es eingebunden ist, bewertet werden (Privatsphäre durch Technik). Deshalb sollten die Grundsätze „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ im Internet der Dinge konsequent umgesetzt werden.

4.5 Ebenso sollte jedes vernetzte Produkt standardmäßig so konfiguriert werden, dass die Privatsphäre bestmöglich geschützt wird (durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), damit das Verhalten und die Beschäftigung der Nutzer nicht unfreiwillig verfolgt werden.

4.6 In jedem Fall sollten die Verbraucher zweifelsfrei wissen, welche Daten erfasst werden, wer darauf Zugriff hat und wozu sie während der aktiven Verbindung mit dem Produkt oder dem Dienst verwendet werden sollen. Zudem sollten die Verbraucher die geltende Datenschutzerklärung kennen und darüber informiert sein, ob die verwendeten Algorithmen Einfluss auf die Qualität, den Preis oder den Zugang zu einem Dienst haben.

## 5. Sicherheit der Verbraucher und Unternehmen im IoT

5.1 Durch die Vernetzung von Geräten, die für das IoT-Ökosystem wesentlich ist, kann die Entwicklung illegaler oder unerwünschter technologischer Verfahrensweisen vorangetrieben werden, weshalb im IoT-Ökosystem leicht für virale Verbreitung nutzbare Schwachstellen entstehen können. Daher sollte in einem umfassenden Ansatz jede einzelne Systemkomponente sicher ausgelegt werden.

5.2 Die angebotenen Produkte und Updates im Zusammenhang mit Cybersicherheit müssen ihre Berechtigung haben und nicht bloß einzelne Geräte betreffen, sondern auch Sicherheitsrisiken abdecken, die aufgrund der Vernetzung mit anderen Geräten im IoT entstehen. Die Sicherheitsstandards dürfen dabei nicht aufgrund der Geräteanzahl sinken.

5.3 In diesem Zusammenhang sieht der Vorschlag für eine Verordnung über die EU-Cybersicherheitsagentur[9] einen Rahmen zur Zertifizierung von Informations- und Kommunikationstechnologien (IKT) vor, der eine freiwillige Sicherheitszertifizierung und Kennzeichnung für unterschiedliche Produkttypen, u. a. für IoT-Produkte, ermöglicht. Der EWSA begrüßt diese Maßnahme, bringt allerdings auch seine Bedenken darüber zum Ausdruck, dass sie nicht obligatorisch ist.

9 Siehe COM(2017) 477 final.

5.4 Die Cybersicherheitsmaßnahmen sollten sich gegen jegliche Arten von Schwachstellen richten, insbesondere gegen Hackerangriffe, unerlaubten Zugriff und Missbrauch sowie Schwachstellen im Zusammenhang mit Zahlungsmitteln und Finanzbetrug. In diesem Kontext befürwortet der EWSA die Befugnisse der Multistakeholder-Sachverständigengruppe für Haftung und neue Technologien.

5.5 Weiterhin sollten die Verbraucher vor Gefahren für die persönliche Sicherheit geschützt werden, die u. a. mit kontaktlosen Anwendungen, der Nutzung gemeinsamer Frequenzbänder, der Exposition gegenüber elektromagnetischen Feldern oder möglichen Interferenzen mit vernetzten medizinischen Geräten zur Aufrechterhaltung lebenswichtiger Funktionen einhergehen. Der EWSA spricht sich dafür aus, im Falle von Risiken für die Gesundheit, die Sicherheit sowie die persönlichen und wirtschaftlichen Interessen der Verbraucher Maßnahmen zur Überwachung und präventiven Marktrücknahme zu ergreifen.

5.6 Unternehmen sollten Standards für bewährte Verfahren – wie z. B. Sicherheit durch Technik und datenschutzfreundliche Voreinstellungen – befolgen und sich externen unabhängigen Bewertungen unterziehen. Unternehmen sollten verpflichtet sein, Sicherheitsvorfälle oder Datenschutzverletzungen zu melden und dabei auch über die Haftung für Schäden und Nichteinhaltung der Rechtsvorschriften zu informieren.

5.7 Unternehmen sollten den Verbrauchern einfache und zugängliche Informationen zur Verfügung stellen, damit die Verbraucher fundierte Entscheidungen treffen und Sicherheitsmaßnahmen ergreifen können, und sie sollten Sicherheitsupdates anbieten, die im Laufe des Produktlebenszyklus notwendig sind.

5.8 Der Mangel an kohärenten Rechtsvorschriften zu IoT-Netzen sollte behoben werden. Um die gegenwärtige Infrastruktur zu verbessern, müssen zukunftsfähige Breitbandtechnologien sowie andere Technologien der nächsten Generation entwickelt werden.

## 6. Vorschläge für politische Maßnahmen[10]

6.1 Öffentliche Verwaltungen sollten sich bei der Ausübung ihrer Befugnisse in den verschiedenen Gebieten der Europäischen Union aktiv an der Erarbeitung von Maßnahmen und IoT-Aktionsplänen beteiligen, um ein Gleichgewicht zwischen den Interessenträgern zu erreichen, Probleme frühzeitig zu erkennen und mögliche nachteilige Auswirkungen angemessen abzumildern. Der EWSA schlägt vor:

6.1.1 Testumgebungen (Sandbox), also physische Räume, Cluster usw., für Pilotprojekte und Machbarkeitsstudien (Proof of Concept) zu schaffen. Das Ziel sollte sein, neben Technologien auch Regulierungsmodelle[11] zu erproben;

---

10 Siehe den Bericht der Weltbankgruppe, *Internet of Things: The New Government-to-Business Platform* (Internet der Dinge: die neue Plattform zwischen Politik und Wirtschaft).

11 Siehe https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated.

6.1.2 die technologische Infrastruktur zu finanzieren, welche die Entwicklung innovativer IoT-Projekte im Rahmen des neuen Programms „Horizont Europa“ ermöglicht;

6.1.3 unabhängige Institute und Agenturen mit der Vermittlung und Aufsicht bei IoT-Projekten zu beauftragen. Der EWSA begrüßt die im Verordnungsvorschlag über Cybersicherheit aus dem Jahr 2017 vorgesehenen einschlägigen Maßnahmen und ruft die Kommission dazu auf, die Normungsprozesse in der digitalen Wirtschaft wirksam zu fördern und dazu die nötigen Haushaltsmittel zur Verfügung zu stellen[12];

6.1.4 öffentlich-private Partnerschaften und kollaborative Plattformen zu fördern und dabei die Wissenschaft, die Industrie und die Verbraucher miteinzubeziehen;

6.1.5 Investitionen in die Entwicklung lokaler Geschäftsmodelle zu fördern, welche die Vorteile des IoT nutzen und die Berücksichtigung komplexer Aspekte wie Datenschutz und -eigentum erleichtern;

6.1.6 Maßnahmen zum Kapazitätsaufbau in der Wirtschaft mit Blick auf die Mitverantwortung durchzuführen. Es sollte gewährleistet werden, dass im Einklang mit der sogenannten „Sorgfaltspflicht“, wie sie in der neuen Verordnung zur Cybersicherheit gefordert wird, alle IKT-Produkte und -Dienste der Sicherheit und dem Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen Rechnung tragen; in diesem Zusammenhang begrüßt der EWSA das Vorhaben, als Ergänzung zu dieser Verordnung **Verhaltenskodizes** zu erarbeiten;

6.1.7 Initiativen zur europäischen und internationalen Normung zu fördern, damit IoT-Systeme die grundlegenden Eigenschaften Zuverlässigkeit, Sicherheit, Verfügbarkeit, Belastbarkeit, Wartbarkeit sowie Einsatzfähigkeit aufweisen. Gerade die Normung ist für die schnelle Umstellung auf hoch digitalisierte industrielle Fertigungsprozesse von entscheidender Bedeutung;

6.1.8 dafür Sorge zu tragen, dass Nutzern des IoT, insbesondere den am stärksten benachteiligten oder in dünn besiedelten Gebieten lebenden Menschen, ein erschwinglicher und hochwertiger Zugang geboten wird;

6.1.9 Sensibilisierungskampagnen und Bildungsprogramme anzustoßen, um Unternehmen und Verbrauchern den Einstieg in das IoT zu erleichtern und ihnen die notwendigen Fähigkeiten und Kompetenzen zu vermitteln[13], wobei ein besonderes Augenmerk auf benachteiligte Gruppen und die Vielfalt zu richten ist;

6.1.10 Initiativen im Bereich der Bildung zur Sicherstellung einer angemessenen Prävention einzuleiten, da Kinder sich bereits ab einem frühen Alter in einer digitalen Umgebung bewegen;

12 ABl. C 197 vom 8.6.2018, S. 17.

13 ABl. C 434 vom 15.12.2017, S. 36.

6.1.11 diagnostische Analysen und Studien einzuleiten, um die Auswirkungen des IoT auf Bereiche wie neue nachhaltige Produktionsmodelle und Verbrauchsmuster zu untersuchen;

6.1.12 die vollständige Umsetzung und wirksame Verwendung der Verfahren der alternativen Streitbeilegung und der Online-Streitbeilegung (ADR und ODR) zu gewährleisten;

6.1.13 sich für die Einführung, die Umsetzung und das reibungslose Funktionieren einer europäischen Regelung für Sammelklagen einzusetzen, die Unterlassungs- und Schadensersatzklagen ermöglicht, auch wenn durch die Nutzung des Internets der Dinge kollektive Schäden oder Verluste entstehen. Dies sollte Gegenstand der Neugestaltung der Rahmenbedingungen für die Verbraucher („New Deal for Consumers“) sein.

6.2 Der EWSA fordert die Kommission auch dazu auf, die Vorschriften, die sich direkt oder indirekt auf das IoT beziehen, zu bewerten und nötigenfalls die geltenden Rechtsvorschriften zu verbessern. In diesem Zusammenhang sollte bei der ***Neugestaltung der Rahmenbedingungen für die Verbraucher*** die Aufmerksamkeit auch auf vernetzte Geräte, Netze, Netzsicherheit und die mit den Geräten verknüpften Daten gerichtet werden.

6.3 Schließlich weist der EWSA darauf hin, wie wichtig die Schaffung von Mechanismen für die Kooperation und die Koordination zwischen den Mitgliedstaaten ist – sowohl für eine effiziente und einheitliche Umsetzung der geplanten Vorschriften als auch für die über ihre Grenzen hinausreichenden Vereinbarungen, die die Europäische Union aufgrund der Standorte von Unternehmen und Lieferanten schließen muss, wobei der Schwerpunkt auf dem Austausch bewährter Verfahren liegt. Die internationale Politik zu grenzüberschreitenden Datenströmen sollte koordiniert werden, damit die beteiligten Länder gleich hohe Schutzstandards in ihr nationales Recht – sowohl in das materielle als auch das formelle Recht – aufnehmen können.

Brüssel, den 19. September 2018

Luca JAHIER
Präsident des Europäischen Wirtschafts- und Sozialausschusses