Deutscher Bundestag **Drucksache 18/8015**

18. Wahlperiode 24.03.2016

Kleine Anfrage

der Abgeordneten Renate Künast, Dr. Konstantin von Notz, Nicole Maisch, Dr. Franziska Brantner, Luise Amtsberg, Volker Beck (Köln), Katja Dörner, Katja Keul, Monika Lazar, Irene Mihalic, Özcan Mutlu, Tabea Rößner, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Abhörpuppen – Datenschutz im Kinderzimmer

Im Jahr 2015 wurden allein auf dem deutschen Spielwarenmarkt 3 Milliarden Euro umgesetzt (Eurotoys, Statista 2016). Kinder und ihre Wünsche haben einen enormen Einfluss auf das Konsumverhalten ihrer Eltern. Sie bestimmen heute maßgeblich mit, wie das frei verfügbare Familieneinkommen ausgegeben wird, und sie haben selbst immer größere finanzielle Mittel zu ihrer freien Verfügung. Das Taschengeld von Kindern beträgt derzeit im Mittel 26,35 Euro im Monat. Darüber hinaus erhalten viele Kinder zu Weihnachten und zum Geburtstag noch Geldgeschenke in Höhe von durchschnittlich 170 Euro pro Jahr (Kids Verbraucher Analyse, Statista 2016). Für Spielwarenhersteller und andere Unternehmen stellen Kinder daher eine außerordentlich kaufkräftige und damit besonders interessante Zielgruppe dar.

Dabei macht auch die fortschreitende Digitalisierung unserer Lebensverhältnisse – mit allen Chancen und Risiken – vor den Kinderzimmertüren nicht halt. Mehr als jedes dritte Kind hat ein „Lieblingsspielzeug“, das aus dem Mobil-, Computer- oder Konsolenbereich kommt (iconkids & youth, Statista 2016), und neuartiges, vernetztes Spielzeug erobert den Markt. Diese Neuerungen werfen jedoch auch Datenschutzfragen auf.

Die Unternehmen Vivid Deutschland GmbH und Matell GmbH vertreiben seit neuestem z. B. sprechende und hörende Puppen mit harmlos klingenden Namen wie „Hello Barbie“ oder „My friend Cayla“. Während „Hello Barbie“ bislang nur in den USA vermarktet wird, ist die Puppe „My friend Cayla“ seit letztem Jahr in Deutschland erhältlich. Sie richtet sich an Kinder im Alter zwischen 4 und 10 Jahren. Mittels Mikrofon und drahtloser Internetverbindung nimmt Cayla alle Gespräche in ihrer Umgebung auf und überträgt die Daten dann an die Server des Drittunternehmens ToyQuest Limited mit Sitz in Hong Kong, China. Dort werden die Daten verarbeitet und – wenn Cayla angesprochen wurde – eine „passende“ Antwort entworfen. Die Puppe wird als Gesprächspartner für Kinder beworben.

Die nur im Internet abrufbaren Datenschutzbestimmungen zu Cayla erlauben es dem Unternehmen ToyQuest Limited, die „Audiodateien von den Stimmen der Nutzer, entsprechende Transkriptionen und/oder in Zusammenhang mit der Nutzung der App entstandene Log Files“ (http://myfriendcayla.de/datenschutz) an Drittunternehmen weiterzuleiten. Eines dieser Drittunternehmen ist dabei das zum Amazon-Konzern gehörende Unternehmen IVONA Software. Dieses behält sich wiederum vor, „to evaluate and profile customers, including customer preferences and purchasing trends, which we may use for marketing purposes and in

respect of operations and development“ (www.ivona.com/us/privacy-policy/#head2). Es ist daher zu befürchten, dass die aus den vermeintlich privaten „Kinderzimmergesprächen“ gewonnenen Daten bereits jetzt oder künftig zu Werbe- und Marktforschungszwecken genutzt werden. Die Konzerne können die so gewonnenen Verhaltensdaten nutzen und verkaufen. Die Kinder werden dadurch vom Verbraucher zum Produkt degradiert.

Auch bei Spielzeug, das per App gesteuert wird, können Daten von Unternehmen gesammelt und weitergegeben werden. So hat die Stiftung Warentest für den Spielzeug-Roboter Sphero BB-8 festgestellt, dass die Software, die eigentlich nur das Spielzeug fernsteuern soll, unnötige Daten erfragt und diese an Dritte weitergibt. So werden neben detaillierten Angaben zu dem Mobilgerät, auf dem die App läuft, auch die E-Mail-Adresse und das Alter des Nutzers an Dritte gesendet (www.test.de/Spielzeug-Roboter-Sphero-BB-8-Niedlich-aber-zu-neugierig-4971623-0/).

Wie attraktiv für Dritte und wie schwer gegen ungewollten Zugriff zu schützen die Daten von „vernetztem Spielzeug“ sind, zeigt auch ein Hackerangriff auf das Unternehmen VTech Electronics Europe GmbH (www.spiegel.de/netzwelt/gadgets/vtech-spielzeug-daten-von-eltern-und-kinder-erbeutet-a-1065182.html). Der Hersteller von Kindertablets und Lernsoftware aus China musste im November 2015 eingestehen, dass Hacker die bei VTech Electronics Europe GmbH gespeicherten Daten von mehr als 200 000 Kindern erbeutet hatten. Als Konsequenz hieraus änderte VTech Electronics Europe GmbH jüngst seine englischen Datenschutzbestimmungen. Darin heißt es jetzt sinngemäß, dass es sein könne, dass Dritte an die Daten gelangen (www.spiegel.de/netzwelt/gadgets/vtech-aerger-ueber-neue-agb-des-spielzeugherstellers-a-1076806.html). Dies ist kein angemessenes Datenschutzniveau für sensible „Kinderzimmerdaten“.

Wir fragen die Bundesregierung:

1. Teilt die Bundesregierung die Auffassung, dass Kinder besonders verletzliche und außerordentlich schutzwürdige Verbraucher sind, für die der Staat eine besondere Verantwortung trägt?
2. Welche Maßnahmen hat die Bundesregierung bisher unternommen, um Eltern für die Risiken, die mit zuvor beschriebenen Spielzeug verbunden sind, zu sensibilisieren?
3. Was tut die Bundesregierung konkret, um auf das neuartige, vernetzte Spielzeug zu reagieren?
4. Was tut die Bundesregierung, um die Privat- und Intimsphäre von Kindern, die vernetztes Spielzeug benutzen, vor Ausforschungen durch Unternehmen zu Marktforschungszwecken zu schützen?
5. Wie kontrolliert sie den Erfolg dieser Bemühungen?
6. Welche Erkenntnisse hat die Bundesregierung über den Markt mit vernetztem Spielzeug in Deutschland?

   Welche Produkte werden bereits in Deutschland verkauft, wie sind die Verkaufszahlen?
7. a) Hält die Bundesregierung die Einverständniserklärung von Eltern zur Aufnahme, Verarbeitung und Speicherung der „Gespräche“ ihres Kindes mit einer vernetzten Puppe durch Drittunternehmen für wirksam?

   b) Falls ja, ist dies nach Auffassung der Bundesregierung auch mittels Allgemeiner Geschäftsbedingungen möglich, so wie bei der Puppe „My friend Cayla“?

8. Wie stellt sich die Rechtslage nach Auffassung der Bundesregierung dar, wenn die Spielzeuge auch die Daten von unbeteiligten Dritten erfassen, verarbeiten und speichern, die nicht wissen, dass ein entsprechendes Spielzeug eingeschaltet und im Raum ist und die keine Einverständniserklärung gegeben haben?
9. Welche datenschutzrechtlichen Bestimmungen (Bundesdatenschutzgesetz – BDSG, Telemediengesetz – TMG, Telekommunikationsgesetz – TKG usw.) kommen nach Auffassung der Bundesregierung für Puppen zum Tragen, die ganze Gespräche mitschneiden können?
10. Wer sind die datenschutzrechtlich verantwortlichen Stellen für den Einsatz solcher Puppen, und in welchem Verhältnis stehen mehrere gleichzeitig Verantwortliche zueinander?
11. Wie können nach Auffassung der Bundesregierung Eltern für die in der Regel nicht einwilligungsfähigen Kinder anstelle der Kinder einwilligen, wenn diese zugleich verantwortliche datenverarbeitende Stelle im Sinne der Datenschutzbestimmungen sind?
12. Wie stellt sich die Rechtslage nach Auffassung der Bundesregierung dar, wenn das Spielzeug die Gespräche mit Kindern erfasst, verarbeitet und speichert, deren Eltern nicht in die Nutzung eingewilligt haben?
13. Wie stellt sich die Rechtslage nach Auffassung der Bundesregierung hinsichtlich der Datenschutz-Grundverordnung dar?

    Sieht die Bundesregierung hier mögliche Umsetzungsspielräume bei der Umsetzung in nationales Recht, und wird sie diese wahrnehmen?
14. Hält die Bundesregierung vor dem Hintergrund einer Umfrage der Gesellschaft Public Relations Agenturen e. V., der zufolge das Vertrauen von 90 Prozent der Eltern in Spielzeug davon abhängt, ob dies „ungefährlich“ ist, vernetztes Spielzeug, das im Betriebsmodus ständig Daten über sein Umfeld an Dritte sendet, für „ungefährlich“?
15. Welche Erkenntnisse hat die Bundesregierung über den Hackerangriff auf das Unternehmen VTech Electronics Europe GmbH und über die Auswirkungen für deutsche Verbraucherinnen und Verbraucher?
16. Hat es im Zusammenhang mit diesem Angriff eine Information der zuständigen Behörden und/oder bundesdeutscher Nutzerinnen und Nutzer gemäß § 42a BDSG gegeben, und wenn nein, weshalb nicht?
17. Hat die Bundesregierung Erkenntnisse über die Urheber der Attacke und wozu diese die Daten verwenden wollen?
18. Welche Stelle in der Bundesregierung hat sich mit dem Vorfall beschäftigt?
19. Hat die Bundesregierung das Unternehmen kontaktiert, um sich über das Ausmaß zu informieren, und falls nein, wieso nicht, und falls ja, mit welchem Ergebnis?
20. Zieht die Bundesregierung hieraus Schlüsse für ihre Cyber-Sicherheitsstrategie, und wenn ja, welche?

Berlin, den 24. März 2016

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333