ZUM STAND DER VERNETZTEN DINGE: DIE PROBLEME MIT DER IT-SICHERHEIT BEI SMART TOYS

Stefan Hessel

Studentischer Mitarbeiter, juris-Stiftungsprofessur für Rechtsinformatik und CISPA
Universität des Saarlandes, Geschäftsführer der Defendo GbR – Möllers Hessel
66123 Saarbrücken, DE
stefan.hessel@uni-saarland.de

Schlagworte: ***Vernetzte Spielzeuge, Smart Toys, Internet der Dinge, IT-Sicherheit, Datenschutz, Sicherheitslücken***

Abstract: *In Deutschland ist der Missbrauch von Sendeanlagen nach § 90 des Telekommunikationsgesetzes (TKG) verboten. Anfang 2017 wurde die Norm auf die smarte Spielzeugpuppe «My friend Cayla» angewendet. Seither ist der Besitz der Puppe in Deutschland verboten. Die zuständige Bundesnetzagentur will das Gesetz jedoch nicht auf alle Spielzeuge mit einer ungesicherten Bluetooth-Verbindung anwenden. Der Beitrag erläutert und kritisiert diese Rechtsauffassung. Abschließend werden, ausgehend vom konkreten Fall, mögliche rechtliche Lösungen für Sicherheitsprobleme bei smarten Spielzeugen diskutiert.*

1. Einführung in die Problematik

Das allgemeine Persönlichkeitsrecht wird in der Bundesrepublik Deutschland nicht nur durch das Grundgesetz (Art. 2 Abs. 1 GG i.V.m Art. 1 Abs. 1 GG) garantiert, sondern auch durch ein umfassendes Regelungskonzept gewährleistet. Ein Teil der einfachgesetzlichen Regelungen zum Schutz des Persönlichkeitsrechts ist § 90 des Telekommunikationsgesetzes (TKG), der den Missbrauch von Sendeanlagen oder sonstigen Telekommunikationsanlagen verbietet. Inhalt der Regelung ist ein Verbot von Geräten, die durch ihre Tarnung als Alltagsgegenstand in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen. Erfüllt ein Gerät den Tatbestand des § 90 TKG, ist der Besitz, die Herstellung, der Vertrieb, aber auch die Einfuhr nach Deutschland verboten. Gemäß § 115 TKG wacht über die Einhaltung der Norm auf verwaltungsrechtlicher Ebene die Bundesnetzagentur. Zusätzlich existiert mit § 148 Abs. 1 Nr. 2 TKG auch ein Strafgesetz, das bei Verstößen eine Freiheitsstrafe bis zu zwei Jahren oder eine Geldstrafe vorsieht. In der Vergangenheit wurde § 90 TKG in erster Linie angewandt, um gegen sog. Minispione vorzugehen.[1] Dabei kann es sich z.B. um Spionagekameras, die als Kugelschreiber getarnt sind, handeln. Zu Beginn des Jahres 2017 wurde § 90 TKG von der Bundesnetzagentur allerdings auch auf die smarte Spielzeugpuppe «My friend Cayla» angewendet. Auslöser der behördlichen Entscheidung war ein Rechtsgutachten des Verfassers, das die unzureichend gesicherte Bluetooth-Verbindung der Puppe analysierte und einen Bezug zu § 90 TKG herstellte.[2] Diesem Rechtsgutachten hat sich die Bundesnetzagentur mit teilweise abweichender Begründung angeschlossen.[3] Die

[1] Bundesnetzagentur, Bundesnetzagentur sagt verbotenen Spionagekameras den Kampf an, https://www.bundesnetzagentur.de/cln_1411/shareddocs/pressemitteilungen/de/2016/160425_cam.html (alle Websiten zuletzt aufgerufen am 5. Januar 2018), 25. April 2016.

[2] Hessel, «My friend Cayla» – Eine nach § 90 TKG verbotene Sendeanlage?, JurPC Web-Dok. 13/2017, http://www.jurpc.de/jurpc/show?id=20170013.

[3] Bundesnetzagentur, Bundesnetzagentur zieht Kinderpuppe «Cayla» aus dem Verkehr, https://www.bundesnetzagentur.de/shareddocs/pressemitteilungen/de/2017/14012017_cayla.html, 17. Februar 2017.

Puppe gilt in Deutschland damit als verbotene Sendeanlage. In der wissenschaftlichen Diskussion um das Verbot stand zunächst die Frage im Mittelpunkt, ob die Puppe die erforderliche Bestimmtheit zum Abhören aufweist und welche Anforderungen an dieses Tatbestandsmerkmal im Allgemeinen zu stellen sind.[4] Die Antwort der Bundesregierung auf eine Kleine Anfrage u.a. der Fraktion Bündnis 90/Die Grünen im deutschen Bundestag vom August 2017 zeigt jedoch, dass auch eine andere Rechtsfrage bisher nicht abschließend geklärt ist.[5] So ergibt sich aus der Antwort der Bundesregierung, dass die Bundesnetzagentur bei ihrer rechtlichen Beurteilung den Fokus nicht auf die ungesicherte Bluetooth-Verbindung des Spielzeugs, sondern auf die Möglichkeit einer unbemerkten Übertragung des gesprochenen Wortes an den Hersteller legt.[6] Aus diesem Grund ist beispielsweise der smarte Teddybär «My friend Freddy Bär» – trotz ungesicherter Bluetooth-Verbindung – nach Ansicht der Bundesnetzagentur keine verbotene Sendeanlage.[7]

2. Technische Betrachtung

Bei dem Teddybären Freddy handelt es sich gewissermaßen um den «kleinen Bruder» der Puppe Cayla. Während die Puppe laut Hersteller für Mädchen ab vier Jahren geeignet ist,[8] sollen mit «My friend Freddy Bär» schon Zweijährige spielen können.[9] Wie bei der Puppe Cayla ist auch die Bluetooth-Verbindung des Teddybären ungesichert.[10] Dies bedeutet, dass sich ein Angreifer in einem Umkreis von etwa zehn Metern Zugriff auf das Mikrofon und den Lautsprecher der Spielzeuge verschaffen kann, sofern gerade kein anderes Gerät verbunden ist. Ein Angreifer kann das Spielzeug dann wie ein Bluetooth-Headset verwenden und nicht nur in Dialog mit dem Kind treten und Anweisungen (z.B. «Öffne mir bitte die Haustür») erteilen, sondern auch hören, was im Raum gesprochen wird. Im Gegensatz zur Puppe Cayla, die wenigstens über eine LED anzeigen soll, dass das Mikrofon eingeschaltet ist, existiert ein solcher Hinweis bei «My friend Freddy Bär» nicht.[11] Das Missbrauchsrisiko dürfte daher im Fall des Teddybären sogar als etwas höher zu bewerten sein. Im Übrigen weist die Hardware der Spielzeuge jedoch keine signifikanten Unterschiede auf. Unterschiede existieren jedoch bei der Software, die der Hersteller zur Verwendung der Spielzeuge zur Verfügung stellt und die zur Nutzung der Spielfunktionen auf einem Smartphone installiert werden muss. Während im Fall von «My friend Cayla» das gesprochene Wort zur Sprachanalyse auf einen Server in die USA übertragen wird, arbeitet die Software des Teddybären Freddy rein lokal und überträgt keine Daten ins Internet. Aus technischer Perspektive ist bei einem Angriff über die ungesicherte Bluetooth-Schnittstelle die Frage, ob Daten zum Hersteller übertragen werden, jedoch ohne Bedeutung.

---

4 Hessel, JurPC, Abs. 28; Schwenke, § 90 TKG – Anwendbarkeit des Verbotes von «Minispionen» im Zeitalter smarter Geräte, Kommunikation & Recht 2017, S. 297 (S. 298 f.); Vogelgesang/Hessel, Spionagegeräte im Kinderzimmer? Die Problematik des § 90 TKG bei Smart Toys, Zeitschrift für den Datenschutz (ZD) 2017, S. 269 (S. 721).

5 Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/13401, Besserer Verbraucherschutz im Telekommunikationsbereich, http://dipbt.bundestag.de/dip21/btd/18/134/1813401.pdf, 24. August 2017, S. 11.

6 Ebenda.

7 Ebenda.

8 Bundesverband des Spielwaren-Einzelhandels e.V., TOP 10 Spielzeug 2014, My friend Cayla, http://www.top10spielzeug.de/My-friend-Cayla.

9 Bundesverband des Spielwaren-Einzelhandels e.V., TOP 10 Spielzeug 2015, Freddy Bär, http://www.top10spielzeug.de/Top10-Spielzeug-Nominierte/Nominierte-2015/Freddy-Bär.

10 Vogelgesang/Hessel, ZD 2017, S. 270.

11 Ebenda.

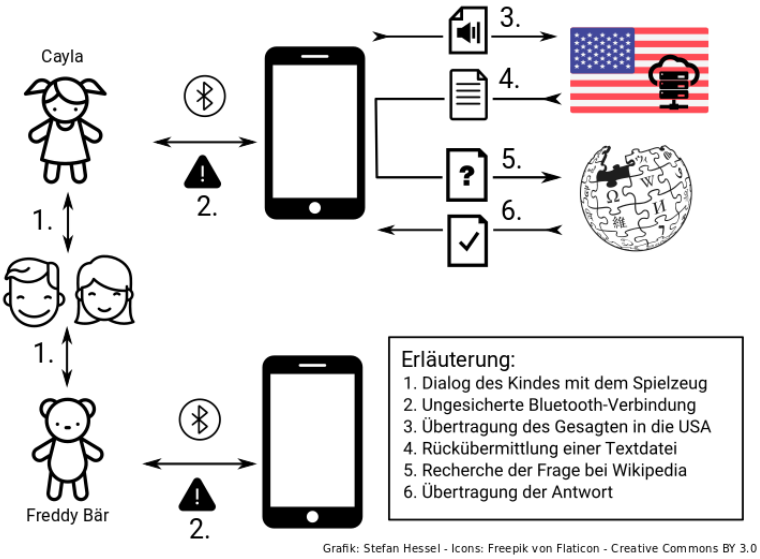

Abbildung 1: Übersicht zur Funktionsweise der Spielzeuge

3. Rechtliche Analyse

Obwohl beide Geräte über dieselbe Schwachstelle verwundbar sind, nimmt die Bundesnetzagentur eine unterschiedliche Einordnung im Hinblick auf § 90 TKG vor. Während die Puppe Cayla eine verbotene Sendeanlage ist, soll der Teddybär Freddy wegen der fehlenden Datenübertragung an den Hersteller nicht verboten sein. Fraglich ist jedoch, ob sich diese Auffassung mit § 90 TKG in Einklang bringen lässt. Dabei kommt es entscheidend darauf an, ob eine Datenübertragung an den Hersteller eine Voraussetzung von § 90 TKG ist.

3.1. Wortlaut des § 90 TKG

Das Erfordernis einer Übertragung an den Hersteller könnte sich zunächst aus dem Tatbestandsmerkmal der Sendeanlage ergeben. Voraussetzung einer solchen ist jedoch nur eine Informationsübertragung ohne die Verwendung von Verbindungsleitungen.[12] Eine Übertragung mittels Bluetooth erfüllt diese Voraussetzung bereits.[13] Allerdings könnte es im Fall des Teddybären an einer Eignung zum unbemerkten Abhören fehlen. Eine Eignung zum unbemerkten Abhören liegt vor, wenn das nicht öffentlich gesprochene Wort über den natürlichen Klangbereich hinaus wahrnehmbar gemacht wird.[14] Im Fall des Teddybären Freddy könnte man annehmen, dass es an einer solchen Eignung fehlt, da – im Gegensatz zur Puppe Cayla – keine Übertragung ins Internet stattfindet. Diese Betrachtung greift allerdings zu kurz, denn die Bluetooth-Verbindung des Teddybären ist z.B. in der Lage Wände und Decken zu durchdringen. Dadurch kann das nicht öffentlich gesprochene Wort auch dort hörbar gemacht werden, wo das menschliche Gehör versagt. Insofern ist eine Übertragung des gesprochenen Wortes über eine lokale Bluetooth-Verbindung für eine Eignung zum unbemerkten Abhören ausreichend. Fraglich ist jedoch, inwieweit ein Abhören über die lokale Bluetooth-Verbindung dem Hersteller

[12] Möllers/Vogelgesang/Hessel/Leffer, Mit Schirm, Charme und Kamera – Verbotene Sendeanlagen i.S.d. § 90 TKG, Trends und Communities der Rechtsinformatik: Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017, 2017, S. 687 (S. 689).

[13] Hessel, JurPC, Abs. 24.

[14] Graulich, Kommentierung zu § 90. In: Arndt / Fetzer / Scherer / Graulich (Hrsg.), Telekommunikationsgesetz Kommentar, 2.Auflage, Schmidt Verlag, Berlin 2015, § 90, Rn. 12.

zugerechnet werden kann, oder ob ein (widerrechtlicher) Eingriff eines Dritten vorliegt. Dafür kommt es darauf an, ob die Möglichkeit des Abhörens über die Bluetooth-Verbindung ein Bestandteil des Nutzungskonzepts des Herstellers ist. In diesem Zusammenhang ist zunächst zu berücksichtigen, dass der Hersteller bewusst auf eine Absicherung der Bluetooth-Schnittstelle verzichtet hat und das Spielzeug in technischer Hinsicht wie ein Headset mit dem Smartphone interagieren lässt. Für ein Abhören mittels Bluetooth muss ein Angreifer lediglich eine andere als die Anwendung des Herstellers, beispielsweise eine Diktiersoftware, auf seinem Smartphone starten. Darin jedoch einen widerrechtlichen Eingriff in das Nutzungskonzept des Herstellers zu sehen, der eine Zurechnung unmöglich macht, erscheint überzogen. Schließlich hat der Hersteller sogar erkannt, dass ein Zugriff auf das Mikrofon nicht nur für seine Anwendung, sondern auch für andere Anwendungen möglich ist und empfiehlt daher die «Nicht stören»-Funktion des Smartphones einzuschalten, um ungestört mit dem Spielzeug spielen zu können.[15] Insofern ist die Möglichkeit eines ungesicherten und unbemerkten Zugriffs auf den Lautsprecher und insbesondere das Mikrofon sowohl im Fall von «My friend Cayla», als auch im Fall «My friend Freddy Bär» dem Hersteller zuzurechnen. Eine Übertragung an den Hersteller ist nicht notwendig, um eine Eignung der Spielzeuge zum unbemerkten Abhören anzunehmen. Aus dem Wortlaut des § 90 TKG lässt sich das Erfordernis einer Übertragung an den Hersteller daher nicht ableiten.

3.2. Entstehungsgeschichte des § 90 TKG

Historisch hat sich das Verbot von Abhöranlagen aus dem ehemaligen Fernmeldeanlagengesetz entwickelt.[16] Dort wurde mit dem Gesetz zur Verhinderung des Missbrauchs von Sendeanlagen vom 27. Juni 1986 eine Regelung aufgenommen, die bis heute in wesentlichen Zügen unverändert geblieben ist.[17] Eine größere Änderung des Gesetzes war die Einführung der sog. sonstigen Telekommunikationsanlagen im Jahr 2012, mit dem Ziel, die Norm möglichst technikoffen zu gestalten.[18] Die historische Genese des § 90 TKG enthält jedoch keine Anhaltspunkte dafür, dass eine unbemerkte Übertragung an den Hersteller Voraussetzung für ein Verbot der Sendeanlage sein soll. Der Gesetzgeber hatte vielmehr im Jahr 1984 gerade sog. Minispione vor Augen,[19] bei denen die Reichweite ebenfalls nur wenige Meter betragen kann.[20]

3.3. Telos der Norm

Während eine Auslegung nach der Systematik im Falle von § 90 TKG nicht zur Klärung der Frage beitragen kann,[21] könnte der Sinn und Zweck der gesetzlichen Regelung möglicherweise Anlass zu einer Einschränkung des Anwendungsbereichs im Sinne der Bundesnetzagentur geben. § 90 TKG soll die Privatsphäre des Einzelnen schützen.[22] Mit der Norm schützt der Gesetzgeber das nicht öffentlich gesprochene Wort und gewährleistet damit das allgemeine Persönlichkeitsrecht und das Fernmeldegeheimnis.[23] Im Gegensatz zu den strafrechtlichen Regelungen in den §§ 201, 201a StGB, die eine konkrete Verletzung des höchst persönlichen Lebensbereichs verlangen, ist eine solche bei § 90 TKG gerade nicht erforderlich. Vielmehr soll er die strukturelle Gefahr, die von der Verbreitung solcher Geräte ausgeht, eindämmen.[24] Allerdings könnte man überlegen, ob sich aus dem Gesamtkonzept der gesetzlichen Regelung ergibt, dass ein Verstoß gegen § 90 TKG nur für denjenigen möglich ist, der auch Täter des § 201 StGB sein kann. Aus dieser Überlegung heraus

15 Vivid Deutschland GmbH, My friend Freddy Bär: Hilfe & Info, http://freddybaer.de/hilfe.
16 Möllers/Vogelgesang/Hessel/Leffer, IRIS 2017, S. 688.
17 Ebenda.
18 Ebenda.
19 Deutscher Bundestag, 10. Wahlperiode, Drucksache 10/1618, Entwurf eines Gesetzes zur Verhinderung des Mißbrauchs von Sendeanlagen,http://dipbt.bundestag.de/doc/btd/10/016/1001618.pdf, S. 1.
20 Wahl, Minispione: Technik und Abwehr des Lauschangriffs, 3. Auflage, Franzis, Poing 2003, S. 32 ff.
21 Hessel, JurPC, Abs. 28.
22 Vogelgesang/Hessel, ZD 2017, S. 272.
23 Ebenda.
24 Ebenda, S. 273.

ließe sich die Auffassung der Bundesnetzagentur, dass bei den smarten Spielzeugen eine Audioübertragung an den Hersteller vorliegen muss, erklären. Fraglich ist jedoch, ob diese Annahme tatsächlich mit dem Zweck der Regelung vereinbar ist. Zunächst ist dabei festzuhalten, dass sich die Sicherheitslücke bei den Spielzeugen durch jedermann ausnutzen lässt. Insofern könnte im Fall des Teddybären Freddy auch der Hersteller – einen Vorsatz vorausgesetzt – Täter des § 201 StGB sein. Damit ist schon fraglich, ob die Voraussetzungen für diese Einschränkung im Sinne des Gesamtkonzepts überhaupt vorliegen. Grundsätzlich würde es dafür einer Lücke bedürfen, die sich nicht trivial ausnutzen lässt, sondern eine weitergehende Manipulation zum Abhören erfordert. Ein solches Szenario wäre dem Hersteller dann nicht zurechenbar. Allerdings würde sich der Angreifer aus einem eigentlich ungefährlichen Gegenstand eine verbotene Sendeanlage herstellen und auf diese Weise gegen § 90 TKG verstoßen. Schließlich ist für eine teleologische Reduktion im Sinne der Bundesnetzagentur in Anbetracht des datenschutz- und verfassungsrechtlichen Hintergrunds des § 90 TKG kein Raum.[25] Dies gilt bei Kindern, die einem besonderen gesetzlichen Schutz unterliegen, umso mehr.[26] Im Ergebnis widerspricht das Erfordernis einer Datenübertragung an den Hersteller daher sogar dem Sinn und Zweck des Gesetzes.

4. Zwischenergebnis

Aus der dargestellten rechtlichen Analyse ergibt sich, dass § 90 TKG für die Eignung einer verbotenen Sendeanlage keine Übertragung des gesprochenen Wortes an den Hersteller erfordert. Es ist jedoch erforderlich, dass die Abhörmöglichkeit dem Hersteller zugerechnet werden kann. Im Fall der Puppe Cayla und des Teddybären Freddy kann durch diese Auslegung gewährleistet werden, dass die in technischer Hinsicht vergleichbaren Missbrauchsgefahren auch in rechtlicher Hinsicht ausreichend berücksichtigt werden. Daraus folgt, dass nach der aktuellen Rechtslage in Deutschland nicht nur die Puppe Cayla nach § 90 TKG verboten sein dürfte, sondern auch der Teddybär Freddy.

5. Bestehender Rechtsrahmen

Die IT-Sicherheit von Kinderspielzeug ist jedoch kein Problem, das auf einige wenige Geräte beschränkt ist. Vielmehr gab es in der Vergangenheit immer wieder Sicherheitslücken und erfolgreiche Angriffe auf Spielzeuge.[27] Die Vielzahl der Vorfälle macht dabei deutlich, dass die IT-Sicherheit bei vernetzten Spielzeugen, wie die IT-Sicherheit bei anderen IoT-Geräten, ein erhebliches Problem ist. Dabei ist § 90 TKG aufgrund seines engen Anwendungsbereiches nur eingeschränkt geeignet, diese Aufgabe zu bewältigen. Dies lässt sich darauf zurückführen, dass nur wenige Sicherheitslücken gleichzeitig eine Einordnung als verbotene Sendeanlage zulassen. Führt man sich die gesetzgeberische Intention bei der Schaffung von § 90 TKG – den Schutz vor Minispionen – vor Augen, erscheint dieses Ergebnis auch folgerichtig. Fraglich ist jedoch, ob neben § 90 TKG weitere gesetzliche Regelungen existieren, die geeignet sind die IT-Sicherheit von Spielzeugen zu gewährleisten. Zunächst ist festzuhalten, dass die bestehenden spezialgesetzlichen Regelungen für die Sicherheit von Spielzeugen, insbesondere die EU-Richtlinie 2009/48/EG über die Sicherheit von Spielzeug,[28] bisher keine Anforderungen an die IT-Sicherheit stellen. In Betracht kommt jedoch eine Anwendung des allgemeinen Datenschutzrechts, dessen Anwendbarkeit im Folgenden anhand der Datenschutzgrundverordnung (DSGVO) geprüft werden soll. Die DSGVO ist nach Art. 2 Abs. 1 DSVGO nur anwendbar, soweit im Rahmen der Verwendung des Spielzeuges personenbezogene Daten verarbeitet werden. Bei einem Großteil der vernetzten Spielzeuge, insbesondere solchen, die eine Datenübertragung an den Hersteller aufbauen, ist diese Voraussetzung unproblematisch. Allerdings fallen Spielzeuge, die keine personenbezogenen Daten verarbeiten, aber möglicherweise dennoch Sicherheitslücken aufweisen, nicht in den Anwendungsbereich. Ein Beispiel dafür

25 Ebenda, S. 272.
26 Ebenda.
27 Ebenda, S. 271.
28 Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug, ABl. L 170/1.

könnte z.B. ein Bluetooth-Lautsprecher für Kinder sein, dessen Bluetooth-Verbindung, wie bei den bereits vorgestellten Geräten, nicht ausreichend abgesichert ist. In diesem Fall werden keine personenbezogenen Daten verarbeitet, ein Angreifer könnte aber dennoch über den Lautsprecher Anweisungen erteilen. Schließlich ist die DSGVO nach Art. 2 Abs. 2 lit. c bei der Ausübung persönlicher oder familiärer Tätigkeiten nicht anwendbar. Sofern das Spielzeug lediglich Daten mit einem Gerät der Eltern austauscht, scheidet eine Anwendung der DSGVO aus. Ein Beispiel dafür ist beispielsweise der Teddybär Freddy. Dieser kommuniziert ausschließlich mit der Anwendung auf dem Smartphone der Eltern und überträgt, nach bisherigem Kenntnisstand, keine Daten an den Hersteller. Folglich ist in einem solchen Fall die DSGVO nicht anwendbar. Sofern das Spielzeug jedoch Daten an den Hersteller überträgt, ist dieser jedoch als verantwortliche Stelle nach Art. 4 Nr. 7 DSGVO zu qualifizieren. Daraus resultiert eine Bindung des Herstellers an die Grundsätze der Datenverarbeitung aus Art. 5 DSGVO. Er hat insbesondere technische und organisatorische Maßnahmen zu treffen, um die Integrität und Vertraulichkeit der Daten zu gewährleisten (Art. 5 Abs. 1 lit. f DSGVO). Verstößt der Hersteller gegen diesen Grundsatz, kann die zuständige Aufsichtsbehörde nicht nur die gefürchteten Geldbußen nach Art. 83 DSGVO verhängen, sondern auch ihre Befugnisse nach Art. 58 Abs. 2 ausüben. Eine Verpflichtung zunächst die mildeste Maßnahme, eine Warnung nach Art. 58 Abs. 2 lit. a DSGVO, auszuüben, besteht dabei für die Aufsichtsbehörde nicht.[29] Im Falle von gravierenden Sicherheitslücken könnten sogar Verkaufsverbote auf die DSGVO gestützt werden. Dass eine Anwendung von datenschutzrechtlichen Vorschriften auf Spielzeuge nicht nur in der Theorie möglich ist, zeigt beispielhaft die förmliche Aufforderung der französischen Datenschutzaufsichtsbehörde CNIL im Fall der Puppe Cayla und des ebenfalls unsicheren Roboterspielzeugs I-Que.[30] Die CNIL monierte in ihrer Aufforderung neben einer fehlerhaften Datenschutzerklärung insbesondere die fehlende Absicherung der Bluetooth-Verbindung.[31] Im Ergebnis zeigt sich, dass das allgemeine Datenschutzrecht zumindest teilweise geeignet ist, die IT-Sicherheit von vernetzten Spielzeugen zu gewährleisten. Dies gilt jedoch nicht schrankenlos, sondern erfordert stets eine Verarbeitung von personenbezogenen Daten durch den Hersteller.

6. Fazit und Ausblick

Die IT-Sicherheit bei vernetzten Spielzeugen ist Teil eines größeren Problems, dass für viele andere IoT-Geräten ebenfalls besteht. Angesichts zahlreicher Sicherheitslücken in der Vergangenheit ist auch in der Zukunft damit zu rechnen, dass vernetzte Spielzeuge Schwachstellen bei der IT-Sicherheit haben und daraus für Kinder und Eltern negative Konsequenzen drohen werden. Dem wird durch die bestehende Rechtslage, obwohl es sich bei Kindern um eine rechtliche besonders schützenswerte Gruppe handelt, bisher nur unzureichend Rechnung getragen. Der Gesetzgeber sollte daher die bestehenden Spezialgesetze zur Sicherheit von Spielzeugen um Vorschriften zur IT-Sicherheit ergänzen. Die Anforderungen an die Hersteller sollten dabei hoch sein und, neben einer Pflicht zum «Security by Design», auch die Verpflichtung zu fortlaufenden Sicherheitsupdates umfassen. Eine solche spezialgesetzliche Regelung würde sich ebenfalls in das bestehende Regelungskonzept einer gesonderten Normierung von Sicherheitsanforderungen an Spielzeuge einfügen. Insoweit sollte die Frage, welche Anforderungen an die IT-Sicherheit von vernetzten Spielzeugen gestellt werden und wer diese überwacht, von der Frage einer allgemeinen Regelung für die IT-Sicherheit von IoT-Geräten getrennt werden.

---

[29] Eichler, DS-GVO Artikel 58 Befugnisse. In: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 22. Edition, Stand: 1. Januar November 2017, Art. 58 DSGVO, Rn. 18.

[30] Commission nationale de l'informatique et des libertés, Connected toys: CNIL publicly serves formal notice to cease serious breach of privacy because of a lack of security, https://www.cnil.fr/en/connected-toys-cnil-publicly-serves-formal-notice-cease-serious-breach-privacy-because-lack-security.

[31] Ebenda.