Deutscher Bundestag **Drucksache 19/18944**

19. Wahlperiode 05.05.2020

Antrag

der Abgeordneten Dr. Achim Kessler, Susanne Ferschl, Matthias W. Birkwald, Sylvia Gabelmann, Katja Kipping, Jutta Krellmann, Cornelia Möhring, Jessica Tatti, Harald Weinberg, Sabine Zimmermann (Zwickau), Pia Zimmermann und der Fraktion DIE LINKE.

Patienteninteresse voranstellen und gemeinwohlorientierten Gesundheitsdatenschutz einführen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Nach dem kostspieligen Stillstand des letzten Jahrzehnts um die Digitalisierung im Gesundheitssystem werden nun im Eilverfahren unfertige digitale Anwendungen eingeführt. Die Grundprinzipien der informationellen Selbstbestimmung werden schon in der Einführung verletzt. So sollen die Versicherten in der ersten Ausbaustufe nicht einmal entscheiden können, welche Ärztinnen und Ärzte welche Bereiche der sensiblen Daten einsehen können.

Die Digitalisierung im Gesundheitswesen kann nur dann als gelungen betrachtet werden, wenn ein konkreter Patientennutzen, eine Anwenderfreundlichkeit und die Gewährleistung von Selbstbestimmung und Datensicherheit miteinander verbunden werden. Insbesondere Menschen, die wegen ihres Alters, ihrer Erkrankung oder ihres Pflegebedarfs nur eingeschränkt neue technologische Hilfsmittel benutzen können, müssen bei der Konzeption der elektronischen Patientenakte (ePA) und der anderen Telematik-Anwendungen mitgedacht werden.

Der Nutzen für die Patientinnen und Patienten scheint in der Strategie der Bundesregierung zweitrangig zu sein, insbesondere im Vergleich zum Anliegen, der IT-Industrie schnellstmöglich Absatzchancen zu generieren. Mit dem Digitale-Versorgung-Gesetz wurde darauf verzichtet, neue digitale Anwendungen, insbesondere Apps, daraufhin zu überprüfen, ob die Patientinnen und Patienten tatsächlich gesundheitlich von der Benutzung profitieren. Statt mit der unabhängigen Bewertung von Therapieanwendungen wird mit dem undefinierten Rechtsbegriff der „positiven Versorgungseffekte“ gearbeitet. Das Bundesinstitut für Arzneimittel und Medizinprodukte soll dafür Kriterien definieren, während bislang nicht geplant ist, die Anwendungen selbst vor dem Zugang zur Versorgung zu überprüfen.

Das Herzstück der Angebote wird die elektronische Patientenakte sein, die ab 1. Januar 2021 allen gesetzlich Versicherten zur Verfügung stehen und über die Telematikinfrastruktur (TI) betrieben werden soll. Die Herstellung der Zugriffs-Apps zur ePA soll privaten Firmen überlassen werden. Es ist aber notwendig, die Interessen Dritter aktiv aus dem Geschehen herauszuhalten. Ein Wettbewerb privatrechtlicher Betreiber

droht sonst das eigentliche Angebot mit kommerziellen Zusatzgeschäften oder Marketing, auch der Krankenkassen, zu überlagern.

Ein Zugriff auf die ePA für Menschen ohne Smartphones soll später einmal mittels Terminals zum Beispiel in Arztpraxen und Filialen der Krankenkassen möglich sein. Für Menschen ohne Smartphone oder Tablet und guter Digitalkompetenz ist das Projekt augenscheinlich nicht konzipiert. Die elektronische Gesundheitskarte soll mit dem Smartphone oder Tablet auch dem Zugriff der Versicherten auf ihre Patientenakte dienen. Allerdings ist weder für die elektronische Gesundheitskarte noch für den Heilberufe-Ausweis sichergestellt, dass der Inhaber auch der Berechtigte ist. Ohne die sichere Identifizierung desjenigen, der die Karte erhält, kann die Karte datenschutzrechtlich auch nicht zur Online-Freigabe von Sozialdaten berechtigen. In der ersten Version der ePA wird es den Versicherten im ersten Jahr ausschließlich möglich sein, nach dem „Alles-oder-Nichts-Prinzip“ ihre Daten an die behandelnden Leistungserbringer freizugeben und ein „PDF-Sammelsurium“ zu verwalten. Der praktische Nutzen der ePA im medizinischen Behandlungsalltag ist deshalb in der Anfangsphase für die beteiligten Fachkräfte und Versicherten sehr gering.

Wird die TI selbst als geschlossene und verschlüsselte Daten-Infrastruktur vielfach aus sicherheitstechnischer Sicht positiv bewertet, so birgt ihre unsichere Umgebung zahlreiche Risiken für Datenverlust: Wie IT-Experten bei einer Tagung des Chaos Computer Clubs im Dezember 2019 gezeigt haben, ist es möglich, mit wenig Aufwand und krimineller Energie an einen Heilberufe-Ausweis, einen Konnektor oder eine elektronische Gesundheitskarte zu kommen (https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt#t=2285). Dieses Authentifizierungsproblem ist lange bekannt, in der Vergangenheit aber ignoriert worden und immer noch nicht behoben. Auch die Regelungen des Patientendatenschutzgesetzes (PDSG) beheben dieses Problem nicht, denn bei der Ausgabe der eGK besteht nach wie vor die Möglichkeit, dass eGKs ohne sichere Identifizierung und ohne sichere Übergabe von Karte und PIN ausgegeben werden. So wird weiterhin nicht verhindert, dass Menschen mit einfachen Mitteln an eGK und PIN gelangen. Da ein Zugriff auf Daten mit hohem Schutzbedarf, zu denen Gesundheitsdaten gehören, nur mit sicherer Identifizierung erfolgen darf, ist die datenschutzrechtliche Zulässigkeit der ePA ab 2021 fraglich.

Hundertausende Leistungserbringer und Millionen Versicherte sollen künftig einen Zugang zur Telematikinfrastruktur erhalten, wobei die großen Risiken für Datenverlust nicht in der TI selbst, sondern in ihrer unsicheren Umgebung liegen. Die IT-Systeme in Arztpraxen und vor allem auch in den Krankenhäusern sind in den letzten Jahren mehrfach wegen Hackerangriffen und entwendeten Daten in den Medien gewesen.

Digital vorliegende Daten sind niemals in Gänze sicher und große, zentral gespeicherte Datensätze bergen eine besondere Gefahr für Angriffe von außen. Gesundheitsdaten sind sensible personenbezogene Daten, die bei Missbrauch durch Dritte starke Diskriminierungen nach sich ziehen können. Der materielle, vor allem aber auch immaterielle Schaden für die Betroffenen kann immens sein. Jedoch werden die Geschädigten im Rahmen der geltenden Deliktshaftung und Beweislastverteilung die Beweiskette zwischen Datenverlust und Schaden etwa auf dem Arbeitsmarkt oder bei Versicherungsabschlüssen im Einzelfall kaum führen können. Die gesellschaftliche Verantwortung für die Wahrung der informationellen Selbstbestimmung aber darf nicht auf Einzelne abgewälzt werden, Die Einführung einer Gefährdungshaftung im Gesundheitsdatenschutz ist deshalb notwendig. Diese soll dazu führen, dass bereits der Datenverlust als Schaden für den einzelnen Versicherten anerkannt und entschädigt wird. Dies setzt auch die notwendigen Anreize, den Datenschutz beim Aufbau sinnvoller TI-Anwendungen ernst zu nehmen. Ein Verschulden einzelner Akteure am Datenverlust und Regressansprüche müssen dann im Innenverhältnis geklärt werden.

Die langfristigen finanziellen und vor allem gesellschaftlichen Kosten der Einführung einer ePA im „Hauruck-Verfahren“ sind aus den angeführten Gründen nicht tragbar. Eine produktive Einbindung digitaler Technologien ins Gesundheits- und Pflegesystem muss sich am tatsächlichen Patienteninteresse nach digitaler Selbstbestimmung und guter und bedarfsgerechter Versorgung orientieren. Sie muss einen medizinischen Nutzen im Behandlungsalltag nachweisen können und die Versorgung sozial gerechter machen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

einen Gesetzentwurf vorzulegen, der die Einführung der elektronischen Patientenakte bis auf Weiteres aussetzt und der

1. für alle Anwendungen der Telematikinfrastruktur (TI) und neuen digitalen Anwendungen in der Versorgung durch die gesetzliche Krankenversicherung (GKV) eine Gefährdungshaftung statt der bislang geltenden Deliktshaftung bei Datenverlust einführt. Ein Schadensersatzanspruch soll bereits dann bestehen, wenn zu schützende Daten nicht zugriffsberechtigten Dritten zugänglich gemacht wurden. Die Betroffenen sind über einen Datenverlust unverzüglich zu informieren. Der Anspruch besteht gegenüber einer zentralen Stelle, die ihrerseits ggf. ein Verschulden der an der TI-Beteiligten klärt und ihrerseits Regresse prüft. Die Hersteller von Apps sind voll haftbar zu machen, eine entsprechende Versicherung ist nachzuweisen;
2. für alle digitalen Anwendungen in der Gesundheitsversorgung, sowohl in der Telematikinfrastruktur als auch bei anderen Gesundheits-Apps, sicherstellt, dass keine Datenerhebung und -weitergabe erfolgt, die für die Anwendung nicht notwendig ist (privacy by design);
3. die Belange von Menschen mit besonderen Bedarfen wie hochaltrige Menschen oder Menschen mit Behinderungen besonders berücksichtigt, sodass auch diese Personengruppen an digitalen Angeboten selbstbestimmt partizipieren und datensicher mit den Anwendungen umgehen können;
4. die Entwicklung sämtlicher Apps auf mobilen Endgeräten für die Anwendungen der Telematikinfrastruktur in die Verantwortung der gematik legt, statt auf privaten Anbieterwettbewerb zu setzen:
   a) ein Zugriff auf die ePA oder anderer Anwendungen der TI mit unsicherer Soft- oder Hardware muss ausgeschlossen werden. Alle Anwendungen sollen mit offenem Quelltext (open-source) angeboten werden und mit dem Ziel, dass alle Anwendungen sowohl open source sind als auch regelmäßig geupdated werden;
   b) die gematik wird mit klarer Fristsetzung beauftragt, einen sicheren ePA-Zugang für heimische PC (mindestens für Windows, IOS und Linux) zu entwickeln;
   c) die Anwendungen der TI sind wissenschaftlich auf ihre Sicherheit und Benutzerfreundlichkeit (Usability), insbesondere auf in Bezug auf vulnerable Versichertengruppen (siehe Forderung 3), zu evaluieren;
   d) die Versicherten müssen neutral über Vorteile und Risiken der ePA und der anderen Anwendungen der TI und aufgeklärt werden;
   e) die Versicherten erhalten die Wahl, eine echte Ende-zu-Ende-Verschlüsselung bei der Datenübertragung von und zu ihrer ePA zu wählen. Sie werden darüber aufgeklärt, dass dies auch der Verzicht auf einen Zweitschlüssel für den Zugang zu ihrer ePA bedeutet und die Daten der ePA bei einem Verlust des Versicherten-Schlüssels nicht mehr zugänglich sind;

5. die bundeseinheitliche datenschutzrechtliche Aufsicht über alle Komponenten der TI beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit festlegt;
6. sicherstellt, dass die Versicherten und Mitglieder der Heilberufe bei der Übergabe der eGK bzw. der Heilberufe-Ausweise sicher identifiziert werden, sofern wie bislang geplant die beiden Karten zur Authentifizierung für die Weitergabe von Gesundheitsdaten im Rahmen der ePA oder anderer Online-Anwendungen der TI verwendet werden. Falls wie geplant ohne Einsatz der eGK ein ePA-Zugang über mobile Endgeräte geregelt wird, ist entsprechend eine sichere Identifizierung und spätere Authentifizierung der Nutzerin oder des Nutzers einzurichten. Für andere spezifische Komponenten für den TI-Zugang, etwa für die Konnektoren, ist eine Identifizierung der berechtigten Empfängerin bzw. des Empfängers sicherzustellen. Die gematik wird beauftragt, alle Identifizierungsprozesse in Abstimmung mit dem Bundesamt für Informationssicherheit und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu spezifizieren;
7. deutlich stärker als bisher die nichttechnische Umgebung der Telematikinfrastruktur zum Gegenstand von Vorgaben und Qualifizierung macht. Dies beinhaltet insbesondere die Stärkung der Aufgaben und Kompetenzen von Datenschutzbeauftragten von Leistungserbringern in Bezug auf die TI, die Schulung und Sensibilisierung von Beschäftigten sowie die verpflichtende Zertifizierung aller technisch an der TI Arbeitenden. Die Krankenkassen werden verpflichtet, den Versicherten zertifizierte und unabhängige Informationen und Schulungen aktiv anzubieten und auf einen kompetenten Umgang mit der ePA und anderen TI-Anwendungen sowie andere digitale Anwendungen in der GKV-Versorgung hinzuwirken.
8. digitale, mobile Gesundheitsanwendungen (Gesundheits-Apps) nur dann zum Teil der GKV-Versorgung macht, wenn
   a) ein patientenrelevanter Nutzen nachgewiesen wurde. Das Institut für Qualität und Wirtschaftlichkeit (IQWiG) wird beauftragt, dazu eine sachgerechte Bewertungsmethodik zu entwickeln, die mit vertretbarem Aufwand eine Beurteilung der Anwendungen auf die bewährten Nutzenparameter Mortalität, Morbidität und Lebensqualität erlaubt;
   b) das Nutzungsverhalten und soweit möglich die gesundheitlichen Effekte in der Versorgung anonymisiert evaluiert werden und die Versorgungsqualität so kontinuierlich weiterentwickelt wird;
   c) das Konzept von „Privacy by Design“ umgesetzt und durch Einsicht in die Quelltexte der Apps durch die gematik insbesondere sichergestellt wird, dass es keine Datenspeicherung oder -weitergabe gibt, die für die Funktionalität der Anwendung und der Evaluierung nicht notwendig ist;
   d) in den Apps kein Marketing, keine In-App-Käufe oder andere Zwecke als die in der Nutzenbewertung und der Evaluierung untersuchten vorgesehen sind;
   e) ein Erstattungspreis zwischen Anbieter und GKV-Spitzenverband verhandelt worden ist, der sowohl den Patientennutzen als auch die Entwicklungskosten für den Hersteller berücksichtigt. Der Erstattungspreis ist innerhalb von drei Monaten nach Zertifizierung der App zu vereinbaren;
   f) Versicherten und Behandelnden Schulungen angeboten werden, sofern sie notwendig sind, um mit der digitalen Anwendung sachgerecht und datensicher umzugehen;

   Alle Änderungen und Updates der digitalen Anwendungen, die Einfluss auf die Nutzenbewertung oder die datenschutzrechtliche Einschätzung haben, erfordern eine entsprechende unabhängige Überprüfung und ggf. eine Neubewertung.

Die Versicherten aller Krankenkassen erhalten Anspruch auf Versorgung mit allen zugelassenen digitalen Gesundheitsanwendungen. Die Krankenkassen müssen auch einen sicheren Zugang außerhalb kommerzieller App-Stores zu den Apps anbieten;

9. den Datenschutz institutionell und in der Anwendung in den Kliniken, Arztpraxen und anderen Leistungserbringern darüber gewährleistet, dass
   a) die Vorgaben der Sicherheitsrichtlinie/KRITIS vereinheitlicht und mit den neuen Gesundheitsdatenschutzvorgaben abgeglichen und bindend werden,
   b) Investitionen in Personal, Krankenhäuser und Arztpraxen beim Aufbau von datenschutzfreundlichen Strukturen unterstützt werden,
   c) Abläufe in Kliniken und in Praxen auf Sicherheitsrisiken geprüft werden.

Berlin, den 5. Mai 2020

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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