

## **Datenschutz und Datensicherheit in der digitalisierten Medizin: zugleich ein Beitrag zum eHealth-Gesetz**

**Benedikt Buchner**

### **Angaben zur Veröffentlichung / Publication details:**

Buchner, Benedikt. 2016. "Datenschutz und Datensicherheit in der digitalisierten Medizin: zugleich ein Beitrag zum eHealth-Gesetz." *Medizinrecht* 34 (9): 660-64.  
<https://doi.org/10.1007/s00350-016-4379-x>.

### **Nutzungsbedingungen / Terms of use:**

**licgercopyright**

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under the following conditions:

**Deutsches Urheberrecht**

Weitere Informationen finden Sie unter: / For more information see:

<https://www.uni-augsburg.de/de/organisation/bibliothek/publizieren-zitieren-archivieren/publizieren>



# Datenschutz und Datensicherheit in der digitalisierten Medizin

Zugleich ein Beitrag zum eHealth-Gesetz\*

**Benedikt Buchner**

Am 29.12.2015 ist das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (eHealthG) in Kraft getreten<sup>1</sup>. Ausweislich der Begründung zum Gesetzentwurf der Bundesregierung soll das eHealth-Gesetz insbesondere „nutzbringende Anwendungen“ der elektronischen Gesundheitskarte (eGK) forcieren, die Telematik-Infrastruktur als zentrale Infrastruktur für eine „sichere Kommunikation im Gesundheitswesen“ etablieren und es sollen telemedizinische Leistungen gefördert werden<sup>2</sup>. Mit jeder dieser Zielsetzungen – nutzbringende Anwendungen der eGK, Kommunikation im Gesundheitswesen, telemedizinische Leistungen – wird auch wieder ein entsprechendes Mehr an Datenverarbeitung einhergehen, in erster Linie von personenbezogenen Gesundheitsdaten. Es ist daher nur konsequent, dass der Gesetzgeber auch beim eHealth-Gesetz dem Datenschutz wieder „höchste Priorität“ einräumt und er diesen „durch rechtliche und technische Maßnahmen“ sicherstellen will<sup>3</sup>.

## I. Recht und Technik

Mit der Sicherstellung des Datenschutzes „durch rechtliche und technische Maßnahmen“ ist auch schon die zentrale Herausforderung angesprochen, der sich der Gesetzgeber bei der Regulierung der digitalisierten Medizin gegenüber sieht: das Zusammenspiel von Recht und Technik. Recht und Technik müssen so aufeinander abgestimmt sein, dass weder das Recht der Technik noch die Technik dem Recht enteilt. Weder darf der Gesetzgeber technische Rahmenbedingungen voraussetzen bzw. einfordern, die so nach dem Stand der Technik noch gar nicht realisierbar sind, noch darf das Recht zu rückständig sein, indem es der Technik hinterherhinkt und es versäumt, den technischen

Fortschritt gerade im Bereich der digitalisierten Medizin zu steuern und neuen datenschutzrechtlichen Risiken zu begegnen. Damit einher geht die Frage, wie sie ganz im Zentrum der diesjährigen Tagung steht: Welche Rolle kommt dem Recht als Steuerungsmedium in einer digitalisierten Medizin überhaupt noch zu? Ist es hier noch das Recht oder ist es vielmehr in erster Linie die Technik, die – positiv wie negativ – den Takt vorgibt, ob und wie Datenschutz in Zeiten einer digitalisierten Medizin gewährleistet wird?

### 1. Code is Law?

Die Frage nach dem Verhältnis zwischen Recht und Technik greift eine Diskussion auf, wie sie für die Welt des Cyberspace schon seit langem geführt wird<sup>4</sup> – getrieben von der Erkenntnis, dass im Informationszeitalter das Recht keineswegs mehr die einzige und vor allem auch nicht unbedingt die effektivste Form einer Regulierung ist, wenn es darum geht, die Rahmenbedingungen für eine globale, digitalisierte Informationsverarbeitung festzuschreiben.

a) „Code and Other Laws of Cyberspace“

*Lawrence Lessig*, Law Professor aus Harvard und einer der Pioniere des Rechts der digitalisierten Welt, hat in seinem Buch „Code and Other Laws of Cyberspace“ vier mögliche Formen einer Regulierung des Cyberspace herausgearbeitet, die alle auf ihre Art und Weise im Cyberspace Regeln setzen können: nicht nur das Recht, sondern auch

\* Schriftliche Fassung des auf der 5. Tagung der Medizinrechtslehrerinnen und Medizinrechtslehrer am 6./7.5.2016 in Bremen gehaltenen Vortrags.

1) Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze v. 21.12.2015, BGBl. I S. 2408.

2) Zu diesen und weiteren Zielsetzungen s. BT-Dr. 18/5293, S. 1 f., 26.

3) BT-Dr. 18/5293, S. 1, 26.

4) S. bspw. *Hoeren*, NJW 1998, 2849, 2853 f.

die „Norms“ (verstanden als Sozialnormen), der Markt und schließlich die Technik (auch als „Architecture“ bezeichnet)<sup>5</sup>. Gerade diese Technik macht sich nach Überzeugung von Lessig mehr und mehr daran, zur bestimmenden Regulierungsform im Cyberspace zu werden:

„This regulator is code – the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned.“<sup>6</sup>

Lessig geht es dabei in seinen Ausführungen in erster Linie darum, zum einen auf diese Wachablösung durch die Technik aufmerksam zu machen und zum anderen dann auch vor der allzu kritiklosen Akzeptanz einer Regulierung durch Technik zu warnen – eben weil Technik im Guten wie im Schlechten eingesetzt werden kann, im Sinne von mehr ebenso wie im Sinne von weniger Datenschutz, im Sinne von weniger, aber auch im Sinne von mehr Überwachung. Eben deshalb ist Lessig auch der Überzeugung, dass man nicht einfach den „antigovernment button“ drücken und der Technik als Regulierer freien Lauf lassen darf<sup>7</sup>.

#### b) Gesundheitsdatenschutz: das Recht

Beim Blick auf die Regulierung des Gesundheitsdatenschutzes hierzulande dürfte Lessig daher zunächst einmal erleichtert sein. Wir Juristen haben das Feld der Regulierung hier bislang keineswegs geräumt, haben vielmehr fleißig Regeln gesetzt und setzen diese auch weiterhin. Die Frage ist beim Gesundheitsdatenschutz eher die, ob wir möglicherweise nicht schon zu viel an Regulierung haben. Bereits ein kurzer Blick auf die rechtlichen Rahmenbedingungen macht deutlich, welche Unmenge an rechtlichen Regelungen für die Datenverarbeitung im Gesundheitswesen einschlägig ist:

Der Gesundheitsdatenschutz beruht im Wesentlichen auf drei Eckpfeilern: dem klassischen Datenschutzrecht mit seinen allgemeinen und bereichsspezifischen Vorgaben, dem Sozialdatenschutzrecht und den Regelungen zur ärztlichen Schweigepflicht. Zum allgemeinen Datenschutzrecht zählen nicht nur das BDSG, sondern auch die 16 Landesdatenschutzgesetze (je nachdem, wer Träger der Gesundheitseinrichtung ist). Für Krankenhäuser in kirchlicher Trägerschaft sind darüber hinaus auch die Datenschutznormen der katholischen und evangelischen Kirche zu berücksichtigen. Bereichsspezifische Datenschutznormen finden sich daneben vor allem für den Krankenhausbereich. Letzterer Regelungsbereich ist durch ein völlig disparates Regelungskonzept gekennzeichnet, die unterschiedlichen landesrechtlichen Regelungsvorgaben lassen keinerlei Einheitlichkeit erkennen. Manche Landeskrankenhausesetze sehen überhaupt keine Regelungen zum Datenschutz vor, manche Gesetze mehr oder weniger umfangreiche Regelungen und mit Bremen und Nordrhein-Westfalen existieren darüber hinaus zwei Bundesländer, die sogar ein eigenes Gesetz für den Datenschutz im Krankenhaus bzw. in Gesundheitseinrichtungen erlassen haben<sup>8</sup>. Aus dem Sozialdatenschutzrecht sind neben den allgemeinen datenschutzrechtlichen Grundsätzen, wie sie in den §§ 67 ff. SGB X normiert sind, vor allem die §§ 284 ff. SGB V von Relevanz, die die bereichsspezifischen Datenschutzvorschriften für die gesetzliche Krankenversicherung enthalten. Für den Bereich eHealth ist dieser Abschnitt des SGB V mehrmals fortgeschrieben worden, zuletzt durch das eHealth-Gesetz vom Dezember 2015. Und last but not least sind für die Verarbeitung von patientenbezogenen Gesundheitsdaten stets die Regelungen der ärztlichen Schweigepflicht zu berücksichtigen, berufsrechtlich normiert<sup>9</sup> und strafrechtlich abgesichert in § 203 StGB.

#### c) Beispiel Outsourcing

Schon dieser kurze Überblick zeigt, dass der Datenschutz im Gesundheitswesen hierzulande jedenfalls nicht an einem Zuwenig an rechtlicher Regulierung scheitern wird. Scheitern wird er viel eher daran, dass diese Menge an Recht nicht auf die technischen Notwendigkeiten bzw. Möglichkeiten in der digitalen Welt abgestimmt ist, weil das Recht nicht adäquat darauf reagiert, was im digitalisierten Medizinalltag technisch möglich und notwendig ist. Ein Beispiel hierfür sind die rechtlichen Rahmenbedingungen für das Outsourcing von IT-Dienstleistungen, welches schon seit langem (medizinischer und technischer) Alltag ist.

In Zeiten der „papierlosen Praxis“, in der Patientendaten nicht mehr auf Karteikarten, sondern digital verarbeitet werden, ist für den Arzt ein Outsourcing bestimmter IT-Dienstleistungen in vielerlei Hinsicht unverzichtbar geworden<sup>10</sup>. Die datenschutzrechtliche Verpflichtung zur Datensicherheit in Form sogenannter technisch-organisatorischer Maßnahmen<sup>11</sup> und auch die berufsrechtliche Verpflichtung zu besonderen Sicherungs- und Schutzmaßnahmen beim Umgang mit Patientendaten<sup>12</sup> setzen ein spezifisches IT-Wissen voraus, das vom Arzt weder erwartet noch eingefordert werden kann. Es ist offensichtlich, dass der Arzt für Dienstleistungen wie die IT-Wartung, die Aktualisierung von Software oder die Datensicherung externe Anbieter einbinden muss; tatsächlich wird dies auch so praktiziert, IT-Outsourcing ist auch im ärztlichen Bereich Alltag. Gleichwohl hat das Recht bis heute auf diese Form der Digitalisierung der Medizin nicht reagiert, noch immer ist das IT-Outsourcing im medizinischen Bereich auf dem Papier in vielen Konstellationen nicht nur unzulässig, sondern sogar strafbar und schafft damit für die Medizin einen nicht hinnehmbaren Zustand der Rechtsunsicherheit.

Datenschutzrechtlich ließe sich das IT-Outsourcing noch rechtskonform gestalten, indem man das Outsourcing als eine sogenannte Auftragsdatenverarbeitung i. S. des § 11 BDSG einordnet und damit Arzt und externe Dienstleister als eine rechtliche Einheit behandelt<sup>13</sup>. Der externe IT-Dienstleister ist somit kein „Dritter“ im datenschutzrechtlichen Sinne und damit auch eine mögliche Preisgabe personenbezogener Daten gegenüber diesem IT-Dienstleister datenschutzrechtlich irrelevant. Voraussetzung hierfür ist, dass sich die ausgelagerte Dienstleistung auf Hilfs- oder Unterstützungstätigkeit bei der Datenverarbeitung beschränkt, nicht ein bestimmter Aufgabenbereich vollumfänglich übernommen wird und das Ganze als weisungsgebundene Tätigkeit des Auftragneh-

5) Lessig, Code and Other Laws of Cyberspace, 1999.

6) Lessig, Harvard Magazine online v. 1.1.2000, Code Is Law, abrufbar unter <http://harvardmagazine.com/2000/01/code-is-law.html> (letzter Abruf: 30. 6. 2016).

7) Ebd.

8) Bremisches Krankenhausdatenschutzgesetz (BremKHDSG) v. 25. 4. 1989 und Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz – GDSDG NW) v. 22. 2. 1994.

9) Vgl. § 9 Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997.

10) Kompetenzzentrum Trusted Cloud, Thesenpapier 7, S. 7, abrufbar unter <http://www.digitale-technologien.de> (letzter Abruf: 30. 6. 2016).

11) S. § 9 BDSG.

12) § 10 Abs. 5 MBO-Ä: „Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Ärztinnen und Ärzte haben hierbei die Empfehlungen der Ärztekammer zu beachten.“

13) Der Dienstleister als der „verlängerte Arm“ des Arztes; s. ausführlicher dazu Buchner, MedR 2013, 337; Jandt/Roßnagel/Wilke, NZS 2011, 641, 643.

mers eingeordnet werden kann<sup>14</sup>. Wenn zudem der Auftrag schriftlich erteilt wird und die gesetzlich vorgegebenen Vertragsbestandteile<sup>15</sup> in die schriftliche Auftragserteilung mit Aufnahme gefunden haben, ist ein solches IT-Outsourcing – datenschutzrechtlich – zulässig und in der Praxis umsetzbar.

Jedoch hilft diese – datenschutzrechtliche – Privilegierung nicht weiter, weil zusätzlich auch noch die Grundsätze der ärztlichen Schweigepflicht zu berücksichtigen sind und es das Recht bis dato versäumt hat, die Grundsätze der ärztlichen Schweigepflicht und die des allgemeinen Datenschutzrechts aufeinander abzustimmen. Nach allgemeiner Meinung stellt eine Auftragsdatenverarbeitung zwar eine datenschutzrechtlich privilegierte Verarbeitungsform dar, begründet jedoch keine Befugnis zur Offenbarung von Daten i. S. von § 203 StGB<sup>16</sup>. Auch sonst lässt sich aus dem Datenschutzrecht keine Befugnis zur Datenoffenbarung ableiten, weshalb als Befugnistatbestand für eine Offenbarung von Daten i. S. des § 203 StGB nur die Einwilligung der betroffenen Patienten bleibt<sup>17</sup> – eine Alternative, die aber in vielen Konstellationen kaum praktikabel und/oder mit erheblicher Rechtsunsicherheit behaftet ist<sup>18</sup>. Oftmals scheidet das Einholen einer Patienteneinwilligung schon an einem unvermeidbar hohen administrativen Aufwand. Problematisch ist bei der Einholung einer Einwilligung darüber hinaus grundsätzlich auch deren Freiwilligkeit, gerade wenn de facto gar nicht die (technische) Alternative besteht, im Falle der Verweigerung einer Einwilligung bei einzelnen Patienten auf ein IT-Outsourcing zu verzichten. Dienstleistungen wie die IT-Wartung, die Datensicherung u. Ä. sind nur dann praktikabel, wenn alle Patientendaten davon erfasst sind; es bleibt hier tatsächlich kein Raum für die Ausübung individueller Selbstbestimmung und die Berücksichtigung individueller Datenschutzpräferenzen des Einzelnen.

Im Ergebnis ist und bleibt damit ein IT-Outsourcing unzulässig, weil offensichtlich ein Wertungswiderspruch zwischen Datenschutzrecht und ärztlicher Schweigepflicht zu verzeichnen ist: Das an sich strenge Datenschutzrecht erlaubt ein IT-Outsourcing, die Grundsätze der ärztlichen Schweigepflicht hingegen nicht. Noch immer fehlt es an einer Fortschreibung des § 203 StGB, die dem IT-Alltag im Gesundheitsbereich adäquat Rechnung trägt. Die Digitalisierung der Medizin hat hier technische Fakten geschaffen, auf die das Recht bis heute nicht reagiert hat – mit der Konsequenz, dass immer noch die Strafbarkeit eines IT-Outsourcings im Raum steht, obwohl dieses tagtäglich praktiziert wird.

## II. Beispiel elektronische Gesundheitskarte: Recht ohne Technik

Ein Auseinanderklaffen zwischen Recht und Technik ist nicht nur dann zu verzeichnen, wenn das Recht wie im Falle des IT-Outsourcing der technischen Entwicklung hinterherhinkt, sondern auch dann, wenn das Recht umgekehrt der Technik enteilt, weil es technische Bedingungen voraussetzt, die so noch gar nicht realisierbar sind. Ein Beispiel hierfür sind die Regelungen zur elektronischen Gesundheitskarte, die mit dem GKV-Modernisierungsgesetz in Form des § 291a SGB V zum 1.1.2004 eingeführt wurden<sup>19</sup>. Die elektronische Gesundheitskarte ist ein Beispiel dafür, wie höchste datenschutzrechtliche Ansprüche verfolgt werden, diese gesetzgeberisch umgesetzt werden, letztlich dann aber daran scheitern, dass die Technik – in erster Linie unter dem Aspekt der Datensicherheit – diesen Ansprüchen nicht gerecht werden kann.

### 1. Die datenschutzrechtlichen Vorgaben

Die Zielsetzungen, die mit der elektronischen Gesundheitskarte verfolgt werden, bringen fast durchweg die Verarbeitung einer Vielzahl personenbezogener Daten mit sich – egal, ob es um die Aktualisierung der Versichertenstammdaten

geht, um das Bereithalten von Notfalldaten auf der Karte, um Medikationssicherheit durch den Medikationsplan oder auch um mehr Patientensouveränität dank elektronischer Patientenakte und Patientenfach. Und nicht nur die Menge der verarbeiteten Daten, sondern auch deren Art – regelmäßig handelt es sich um sog. besondere Kategorien personenbezogener Daten in Form von Gesundheitsdaten<sup>20</sup> – stellen an das Datenschutzrecht besonders hohe Anforderungen.

Jedoch ist allgemeine Meinung, dass der Gesetzgeber diesen hohen datenschutzrechtlichen Anforderungen durchaus gerecht geworden ist<sup>21</sup>. Und tatsächlich findet sich in den Regelungen des § 291a SGB V all das, was einen „guten Datenschutz“ nach allgemeiner Wahrnehmung ausmacht. Es war ganz offensichtlich allererste Zielsetzung des Gesetzgebers, mit der Regelung zur elektronischen Gesundheitskarte die (informationelle) Selbstbestimmung des Patienten umfänglich abzusichern und ins Zentrum zu stellen. Dies beginnt beim Informed Consent: Versicherte sind bereits bei Versendung der Karte durch die Krankenkassen „umfassend und in allgemein verständlicher Form über deren Funktionsweise, einschließlich der Art der auf ihr oder durch sie zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten zu informieren“<sup>22</sup>. Im Zentrum der Regelungen steht sodann die Einwilligung des Versicherten als genuiner Ausdruck informationeller Selbstbestimmung. Grundsätzlich dürfen Daten überhaupt erst dann verarbeitet werden, wenn der Versicherte seine Einwilligung erklärt hat; diese Einwilligung ist zu dokumentieren, sie ist jederzeit widerruflich und kann auf einzelne Anwendungen beschränkt werden (keine Pauschaleinwilligung)<sup>23</sup>. Die Patientenselbstbestimmung wird sogar doppelt abgesichert, indem nicht nur auf der ersten Stufe besagte Einwilligung in die Anwendung der Karte als solche erteilt werden muss, sondern auf einer zweiten Stufe darüber hinaus nochmals eine Autorisierung seitens des Versicherten bei jedem einzelnen Datenverarbeitungsvorgang erfolgen muss<sup>24</sup>. Und auch

14) Vgl. *Petri*, in: *Simitis* (Hrsg.), BDSG, 8. Aufl. 2014, § 11, Rdnr. 22; *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 5. Aufl. 2012, S. 60.

15) § 11 Abs. 2 BDSG.

16) Vgl. *Jandt/Roßnagel/Wilke*, NZS 2011, 641, 645; *Hoenike/Hülsdunk*, MMR 2004, 788, 789.

17) H. M. – s. *Jandt/Roßnagel/Wilke*, NZS 2011, 641, 645; *Hoenike/Hülsdunk*, MMR 2004, 788, 789. Letztere sind allerdings der Auffassung, dass die Weiterleitung von Informationen i. R. d. IT-Outsourcing keine „Offenbarung“ nach § 203 StGB darstelle und mithin straflos bleibe; zu den Möglichkeiten einer „datenschutzkonformen“ Auslegung des § 203 StGB s. auch *Buchner*, MedR 2013, 337, 338f.

18) Anders stellt sich die Situation im Krankenhausbereich dar: Hier stellen teils die Landeskrankengesetze einen gesetzlichen Erlaubnistatbestand für das IT-Sourcing zur Verfügung, wobei die Voraussetzungen von Bundesland zu Bundesland unterschiedlich ausgestaltet sind; s. bspw. § 7 Abs. 2 GDStG NW, § 10 Abs. 1 S. 2 BremKHDSG oder auch Art. 27 Abs. 4 S. 5 Bayerisches Krankenhausgesetz (BayKrG).

19) Gesetz zur Modernisierung der gesetzlichen Krankenversicherungen (GKV-Modernisierungsgesetz – GMG) v. 14.11.2003, BGBl. I S. 2190.

20) § 3 Abs. 9 BDSG und künftig Art. 9 DSGVO.

21) Selbst das durchaus strenge Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) bescheinigt den Regelungen zur elektronischen Gesundheitskarte, dass diese „aus Datenschutzsicht fast vorbildlich“ sind (vgl. ULD-Stellungnahme zum Referentenentwurf für ein „E-Health-Gesetz“ v. 11.2.2015); aus der Literatur s. etwa auch *Peters*, in: *KassKomm.*, § 291a SGB V, Rdnr. 4 (Stand: Juni 2016): „gut gemeint und von datenschutzrechtlichen Überlegungen getragen“.

22) § 291a Abs. 3 S. 3 SGB V.

23) § 291a Abs. 3 S. 5 SGB V.

24) § 291a Abs. 5 S. 1 SGB V; s. dazu *Schneider*, in: *Krauskopf*, Soziale Krankenversicherung, Pflegeversicherung, § 291a, Rdnr. 63 (Stand: März 2016)

die Betroffenenrechte haben Eingang gefunden in die gesetzlichen Regelungen. Mittels des sog. Patientenfachs soll der Versicherte jederzeit Einsicht in seine Patientendaten nehmen können<sup>25</sup>. Und er kann auch jederzeit verlangen, dass seine Daten – bis auf wenige Ausnahmen – wieder gelöscht werden<sup>26</sup>.

All die grundlegenden Regelungsprinzipien, wie sie aus dem sonstigen Datenschutzrecht bekannt sind, finden sich somit auch bei der elektronischen Gesundheitskarte. Sicherlich kann man, wie immer im Datenschutz, auch hier wieder die Frage aufwerfen, ob diese überhaupt tatsächlich umsetzbar sind oder nicht wieder die typischen Vollzugsdefizite drohen, wie sie auch sonst aus dem Datenschutz bekannt sind. Der Grundsatz der Informiertheit einer Einwilligung und die rechtliche Vorgabe, „umfassend und in allgemein verständlicher Form“ zu informieren, sind auch aus anderen Datenschutzgesetzen bekannt – und bekannt ist auch die Umsetzung im Alltag, die sich oftmals in einem bloßen Formalismus erschöpft. Was den Erlaubnistatbestand der Einwilligung angeht, wird seit jeher Kritik an der Einwilligung als bloßer „Fiktion“ geübt, weil diese tatsächlich weder freiwillig noch bewusst oder informiert ist<sup>27</sup>. All dies sind jedoch Aspekte, die die praktische Umsetzung des Datenschutzes ganz allgemein betreffen, für die das Datenschutzrecht ganz allgemein Lösungen entwickeln muss und die zunächst einmal nichts daran ändern, dass die Regelungen zur elektronischen Gesundheitskarte datenschutzrechtlich betrachtet lege artis sind.

## 2. Die technische Umsetzung

Das eigentliche Problem des § 291a SGB V sind nicht die gerade skizzierten, altbekannten und typischen Vollzugsdefizite, wie sie mit datenschutzrechtlichen Vorgaben einhergehen. Das Problem des § 291a SGB V ist vielmehr, dass die Regelungen zur elektronischen Gesundheitskarte technische Rahmenbedingungen voraussetzen, die bis heute nicht realisierbar sind. Der Gesetzgeber hatte hier einen Zeitplan zugrunde gelegt, der von vornherein unrealistisch war, weil die technische Komplexität des Projekts elektronische Gesundheitskarte schlicht unterschätzt wurde. Bis Ende 2015 war in § 291a SGB V die ursprünglich einmal gesetzte Zeitvorgabe nachzulesen, dass „bis spätestens zum 1. Januar 2006“ die Krankenversichertenkarte für all die anvisierten Zwecke – angefangen beim eRezept bis hin zum Patientenfach – zu einer elektronischen Gesundheitskarte erweitert werden sollte<sup>28</sup>. Zehn Jahre nach dieser Fristüberschreitung hat der Gesetzgeber zumindest insoweit reagiert, dass er das Datum „1. Januar 2006“ aus § 291a SGB V gestrichen hat.

Wann es zu der angekündigten Erweiterung der elektronischen Gesundheitskarte um all die Anwendungen mit Nutzen für die Versicherten kommen wird, ist noch immer nicht absehbar. Das elektronische Rezept, ursprünglich einmal als allererste Anwendung und als eines der Herzstücke des Projekts elektronische Gesundheitskarte eingeplant, ist auf unbestimmte Zeit verschoben – laut Auskunft der Bundesregierung „bis die notwendigen technischen und organisatorischen Basisstrukturen für die sichere Anwendung von Arztpraxen, Apotheken bereitstehen“<sup>29</sup>. Selbst der Online-Stammdatenabgleich, ein an sich überschaubarer Datenverarbeitungsprozess, der sich auf den Abgleich und gegebenenfalls die Online-Aktualisierung der Versichertenstammdaten auf der Karte beschränkt, scheitert immer wieder an technischen Problemen und scheint selbst nach den neuen zeitlichen Vorgaben des eHealth-Gesetzes wieder nicht fristgerecht umsetzbar zu sein<sup>30</sup>. Last but not least wird der Erfolg oder Misserfolg der meisten Anwendungen der elektronischen Gesundheitskarte von einer ganz zentralen technischen Frage abhängen, um die sich die Diskussion über die IT- und Datensicherheit der elektronischen Gesundheitskarte von Anbeginn an gedreht hat: Wo werden all diese personenbezogenen Daten gespeichert? Von Ärzteseite ist stets

vehement eine zentrale Speicherung abgelehnt worden und stattdessen eine Datenspeicherung auf der Karte selbst gefordert worden<sup>31</sup> – diskutiert wurden auch alternative dezentrale Speicherorte wie der eines USB-Sticks<sup>32</sup>. Eine weitere Möglichkeit ist die kombinierte Speicherung auf der Karte selbst sowie auf den Computern der Leistungserbringer und/oder eben die Datenspeicherung auf zentralen Servern. Für alle Speicheralternativen sind jeweils entsprechende Worst-case-Szenarien vorstellbar: vom Hacker-Angriff auf einen zentralen Server bis hin zum individuellen Datenverlust bei verlegter Karte oder gestohlenem Praxiscomputer. Solange aber für diese ganz zentrale technische Fragestellung, die gerade für die Datensicherheit von ausschlaggebender Bedeutung ist, nicht eine allgemein akzeptierte Lösung gefunden wird, ist es von vornherein unrealistisch, auf die Umsetzung all der schulmäßig normierten datenschutzrechtlichen Grundprinzipien in die Praxis zu hoffen. Das Recht – so „schön“ es auch sein mag – läuft leer, solange die Technik nicht leisten kann, was das Recht voraussetzt.

## III. eHealth-Gesetz: Technik durch Recht?

Bleibt abschließend die Frage, welche Rolle das Recht als Steuerungsmedium zukünftig spielen soll – gerade im Bereich eHealth –, wenn die bisherige Regulierung doch mehr oder weniger gescheitert ist. Aktuell stellt sich vor allem die Frage, ob sich die Geschichte der erfolglosen Regulierung der elektronischen Gesundheitskarte beim eHealth-Gesetz wiederholen wird.

### 1. Das Einfordern von Technik

Auch das eHealth-Gesetz basiert wieder auf ambitionierten technischen Zielvorgaben und fordert diese Technik mittels Fristen und Sanktionen offensiv ein. Mehr noch: Mit Zielsetzungen wie dem Aufbau einer Telematik-Infrastruktur und deren Ausbau sektorübergreifend zur zentralen Infrastruktur präsentieren sich die gesetzgeberischen Visionen nochmals anspruchsvoller als bei Einführung der elektronischen Gesundheitskarte.

Um diese technischen Visionen zu realisieren, dürfte es allerdings kaum ausreichen, die neue Technik mittels Sanktionen einfordern zu wollen, wie es das eHealth-Gesetz nunmehr an vielen Stellen vorsieht<sup>33</sup>. Verwiesen sei hier nochmals auf das Beispiel des Stammdatenabgleichs. Bereits jetzt, so kurz nach Inkrafttreten des eHealth-Gesetzes, ist schon wieder zweifelhaft, ob der neue, mit relativ engen Fristen versehenen Zeitplan, den das eHealth-Gesetz vorsieht<sup>34</sup>, gehalten werden kann oder ob – wieder einmal – die Technik schlicht nicht bereit ist und Datensicherheit noch immer

25) S. insbesondere § 291a Abs. 5 S. 8 u. 9 SGB V; ausführlich *Paland/Holland*, NZS 2016, 247, 253.

26) § 291a Abs. 6 S. 1 u. 2 SGB V; s. dazu *Peters*, in: *KassKomm.*, § 291a SGB V, Rdnr. 18 (Stand: Juni 2016).

27) S. bspw. *Härtling*, BB 2010, 839, 841; s. mit Blick auf die Vorgaben der DSGVO auch: *Schantz*, NJW 2016, 1841, 1844f.

28) § 291a Abs. 1 SGB V i. d. F. v. 14.11.2003 mit Wirkung v. 1.1.2014.

29) BT-Dr. 18/6990, S. 4; Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Kathrin Vogler* u. a. und der Fraktion DIE LINKE (Dr. 18/6788).

30) S. etwa *Bohsem*, Süddeutsche Zeitung online v. 28.10.2015, Verzettelt, abrufbar unter <http://www.sueddeutsche.de/wirtschaft/gesundheits-verzettelt-1.2711972>, sowie (darauf Bezug nehmend) KBV, E-Health-Gesetz: Sanktionen treffen die Falschen, abrufbar unter [http://www.kbv.de/html/418\\_18056.php](http://www.kbv.de/html/418_18056.php) (letzter Abruf jeweils 30.6.2016).

31) S. dazu bereits *DÄBl.* 2007, A–1452.

32) Vgl. die Stellungnahme von *Weinberg*, *DFZ* 2015, 24.

33) S. § 291 Abs. 2b S. 7 u. 14 SGB V sowie § 291b Abs. 1 S. 11.

34) S. § 291 Abs. 2b SGB V.

nicht sicher gewährleistet werden kann<sup>35</sup>. So aber verspielt das Recht über kurz oder lang seine Glaubwürdigkeit und kann als Steuerungsmedium nicht mehr ernstgenommen werden.

## 2. Das Setzen von Anreizen

Eher erfolgversprechend sind daher andere Regelungsmechanismen, die sich ebenfalls im eHealth-Gesetz finden lassen und die nicht unmittelbar an der Technik selbst ansetzen, sondern stattdessen an denjenigen Personen und Institutionen, die die neue Technik in der Praxis umsetzen müssen, also etwa Ärztinnen und Ärzte. Im diesem Sinne gehen die Regelungsansätze hier dahin, Anreize zur Nutzung neuer technischer Möglichkeiten zu setzen und auf diese Weise der neuen Technik Vorschub zu leisten. Wenn etwa die Übermittlung elektronischer Briefe von Arzt zu Arzt mit 55 Cent zusätzlich honoriert wird<sup>36</sup>, so bedeutet dies für Ärztinnen und Ärzte insbesondere auch einen Anreiz, sich den dafür notwendigen elektronischen Heilberufsausweis zuzulegen und damit eben eine der zentralen Schlüsselkomponenten für die Telematik-Infrastruktur, die dann künftig auch für zahlreiche andere Anwendungsmöglichkeiten der elektronischen Gesundheitskarte eingesetzt werden kann<sup>37</sup>. Ein solches Konzept des „Anreize-Setzens“ findet sich auch an vielen anderen Stellen im eHealth-Gesetz, etwa in § 87 Abs. 2a S. 24 SGB V, und es spricht einiges dafür, dass ein solches Konzept als Steuerungsmittel effektiver ist als die Kombination von Fristen und Sanktionen.

## 3. Das Forcieren von Entscheidungen

Vielversprechend ist darüber hinaus auch der Ansatz im eHealth-Gesetz, Entscheidungen zu forcieren, wenn Abstimmungs- und Einigungsschwierigkeiten zwischen den Institutionen den Auf- und Ausbau von eHealth bremsen. Viele Verzögerungen haben ihren Grund in einer Blockade zwischen den beiden „Bänken“ der Kostenträger der Leistungserbringer<sup>38</sup>, die teils nur schwer nachvollziehbar ist. Es spricht für sich, wenn selbst die Einigung auf eine Kostenpauschale für den elektronischen Brief im einheitlichen Bewertungsmaßstab (EBM) nicht zustande gebracht werden konnte – trotz jahrelanger Bemühungen und eines gesetzlichen Auftrags – und schließlich der Gesetzgeber eine Pauschale von 55 Cent festlegen musste<sup>39</sup>. Deutlich zum Ausdruck kommt die Unfähigkeit zu einer Entscheidungsfindung auch bei der Aufnahme von telemedizinischen Leistungen in den EBM. Seit 2012 besteht insoweit eine gesetzliche Vorgabe im SGB V<sup>40</sup> und doch hat es bis zum 1. 4. 2016 gedauert, dass

endlich eine erste telemedizinische Leistung in den EBM Aufnahme gefunden hat<sup>41</sup>. Da sich auch hier wieder die beiden Bänke der Kostenträger und der Leistungserbringer blockiert hatten, ist es insoweit dann durchaus sinnvoll, auch mittels Sanktionen die Entscheidungsbereitschaft zu forcieren, indem Kürzungen in den Haushalten verhängt werden, wenn der EBM nicht fristgerecht angepasst wird<sup>42</sup>.

## IV. Fazit

Obige Beispiele zeigen, dass das Recht durchaus auch in Zeiten von eHealth und Digitalisierung eine Rolle als Steuerungsinstrument einnehmen kann, und zwar auch, um den technischen Fortschritt zu fördern und zu fördern. Erfolgversprechend ist dies jedenfalls dann, wenn das Recht dort ansetzt, wo es auch tatsächlich steuernd eingreifen kann, also im Kontext von eHealth vor allem bei den Personen und Institutionen, deren Fähigkeit und Bereitschaft zum Nutzen der Technik und deren Bereitschaft zum Fördern der neuen Technik forciert werden sollen. So betrachtet, muss vom Gesetzgeber vor allem auch mehr Geduld eingefordert werden. Statt mittels enger Fristen und damit einhergehender Sanktionen neue Technik offensiv einzufordern, ist eher eine Strategie der kleinen Schritte angebracht, die Anreize setzt sowie Entscheidungsprozesse verbessert und beschleunigt – eben so, wie es im eHealth-Gesetz, zumindest auch, angelegt ist.

35) S. Ärzte Zeitung v. 22. 4. 2016, E-Card – Dieses Jahr keine Tests mehr?; abrufbar unter [http://www.aerztezeitung.de/praxis\\_wirtschaft/e-health/gesundheitskarte/article/909829/e-card-dieses-jahr-keine-tests.html](http://www.aerztezeitung.de/praxis_wirtschaft/e-health/gesundheitskarte/article/909829/e-card-dieses-jahr-keine-tests.html) (letzter Abruf: 30. 6. 2016).

36) § 291f Abs. 1 SGB V.

37) S. Paland/Holland, NZS 2016, 247, 249.

38) S. Paland/Holland, NZS 2016, 247, 248.

39) S. Paland/Holland, NZS 2016, 247, 249; zum Streit zwischen KBV und GKV: Dämon, WirtschaftsWoche online v. 6. 9. 2012, Warum sich Ärzte und Krankenkassen streiten; abrufbar unter <http://www.wiwo.de/politik/deutschland/honorarverhandlungen-warum-sich-aerzte-und-krankenkassen-streiten/7087474.html> (letzter Abruf: 30. 6. 2016).

40) § 87 Abs. 2a SGB V.

41) S. Beschluss des Erweiterten Bewertungsausschusses nach § 87 Abs. 4 SGB V in seiner 42. Sitzung am 15. 12. 2015 zur Änderung des Einheitlichen Bewertungsmaßstabes (EBM) mit Wirkung zum 1. 4. 2016, abrufbar unter [http://institut-ba.de/ba/babeschluesse/2015-12-15\\_eba42.pdf](http://institut-ba.de/ba/babeschluesse/2015-12-15_eba42.pdf) (letzter Abruf: 30. 6. 2016).

42) § 87 Abs. 2a S. 22 SGB V.