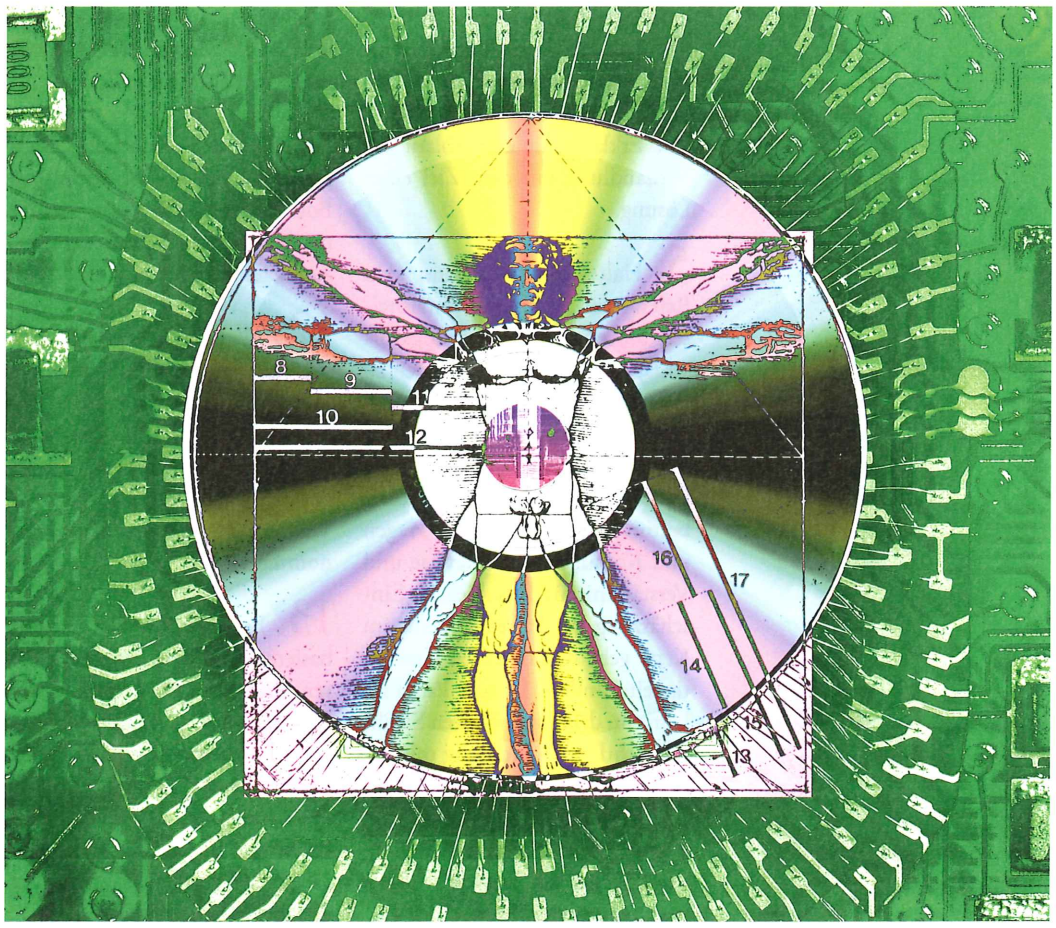
Digitaler Austausch gefährdet Rechtsgüter

Datensicherheit · Der Schutz von Rechtsgütern in der Informationstechnologie bereitet zunehmend Schwierigkeiten. Die Sicherheitsvorkehrungen sollten nicht alleine den Technikern überlassen werden.

Die neue Versichertenkarte verstösst gemäss der entsprechenden Verordnung des Bundes über die Versichertenkarte (VVK) gegen elementare Prinzipien der Sicherheit und gefährdet dadurch fundamentale Rechtsgüter. Beispielsweise besteht bei der neuen Versichertenkarte die Möglichkeit, einen Hinweis auf eine Patientenverfügung zu speichern.[1] Dieser Hinweis kann von allen Leistungserbringern, vom Logopäden über den Ernährungsberater bis hin zum Arzt, ohne Kenntnis des Patienten ergänzt, ersetzt oder gelöscht werden.[2] Doch der Patient selber kann die Richtigkeit des Eintrages nicht autonom – etwa von zu Hause aus – verifizieren.

National- und Ständerat debattierten letztes Jahr darüber, ob man vom Prinzip der aktiven Deklaration, Organe spenden zu wollen, zum Prinzip wechselt, aktiv bekunden zu müssen, dass man keine Organe spenden will.[3] Angedacht war dabei, dass der Arzt dem Hinweis auf der Versichertenkarte vertraut, wonach eine Patientenverfügung besteht. Wenn dieser Hinweis fehlte, stünde der Entnahme von Organen nichts mehr entgegen. Der Ständerat lehnte gegen die Intention des Nationalrats den Wechsel



KEYSTONE

Elektronische Übermittlung: Persönlichkeitsschutz nicht gewährleistet

zur aktiven Deklaration ab. Doch das Thema ist noch nicht vom Tisch. Laut *plädoyer* hat der Intermediär, welcher die elektronischen Rechtsschriften vom Absender an den Adressaten zustellt, die Möglichkeit, unbemerkt Einsicht in die auszutauschenden Rechtsschriften zu nehmen (*plädoyer* 3/13). Mit der Zustellung wird die Rechtsschrift folglich dem Intermediär offenbart oder zugänglich gemacht (zu «offenbaren» und «zugänglich machen» Stratenwerth / Wohlers[4] und Trechsel,[5] Kommentar zu Artikel 162, 273, 320, 321 StGB[6]). Es ist unverständlich, dass eine technische Bundesvorschrift ohne Legitimation des Gesetzgebers so verabschiedet wird, dass der Schutz eines im Strafgesetz verankerten Rechtsgutes unbemerkt umgangen werden kann.

Sicherheitsvorkehrungen häufig ungenügend

Die Ursachen für die Probleme bei der rechtskonformen Umsetzung können vielfältig sein. Dazu gehören zum Beispiel:

- fehlende Kommunikation zwischen den Fachspezialisten
- fehlendes Bewusstsein über die Eigenheiten in der IT
- Verwendung von Begriffen mit Ermessensspielraum und Fehlen quantitativer Bestimmungen
- mangelndes Bewusstsein in Bezug auf die Sachlage im Zusammenhang mit der Internationalität des Internets und mit den Schranken der Rechtsdurchsetzung
- Schwierigkeit, die entsprechenden Vorschriften zu befolgen, wenn sich diese auf den Stand des Wissens und der Technik abstützen
- grundsätzliches menschliches Verhalten im Umgang mit Gefahren
- fehlender Blick auf den vollständigen Prozess.

Fehlende Kommunikation und Auseinandersetzung mit dem Sachverhalt zwischen den Fachspezialisten führen dazu, dass Begriffe in der Kommunikation und den Vorschriften verwendet werden, welche irreführende Assoziationen wecken oder unpräzise sind. Beispielsweise wird in Artikel 2 ZertES[7] im Zusammenhang mit der elektronischen Signatur von «Identifizieren» und «Inhaber von Zertifikaten» gesprochen. Es ist aber nicht möglich, jemanden übers Datennetz mit elektronischen Signaturen und Zertifikaten zu identifizieren. Eine elektronische Signatur erlaubt lediglich, nachweislich festzustellen, wer für das Leisten der elektronischen Signatur verantwortlich ist. Nämlich ausschliesslich der Bezüger (nicht der Besitzer) des Zertifikats, mit dem die Signatur verifiziert wird.

Wenn das Bewusstsein über die Eigenheiten der IT fehlt, führt das angesichts der möglichen Gefahren zu ungenügenden Sicherheitsvorkehrungen. Welche Sorgfalt und folglich welche (Sicherheits-)Vorkehrungen beim Umgang mit Rechtsgütern anzuwenden sind, ist von zentraler Bedeutung. Im erwähnten *plädoyer*-Artikel wurden Sicherheitsvergleiche zwischen der realen Welt und der IT durchgeführt. Solche Vergleiche und Analogien sind mit Vorsicht vorzunehmen. Zutreffend sind sie dann, wenn festgestellt wird, dass ein Rechtsgut gefährdet ist oder verletzt wird, nicht aber zum Ausmass der Gefahr. Dazu eine Analogie: Sowohl in einem Bach als auch auf hoher See kann jemand ertrinken, doch die Gefahr für Leib und Leben könnte nicht unterschiedlicher sein. Anders als in der realen Welt birgt die virtuelle Welt unter anderem folgende zusätzlichen Gefahren:

- Der Datentransfer entzieht sich unseren Sinnen und ist im wahrsten Sinne des Wortes nicht (be)greifbar. Folglich versagen hier die dem Mensch angeborenen Kontrollmechanismen (Sehen, Riechen, Hören, Tasten, Schmecken).
- Die Dynamik und folglich die aus einem Ereignis resultierenden Schadensauswirkungen sind im Internet weit grösser als in der realen Welt. Zum Beispiel können auf einem USB-Stick unzählige illegal erworbene Kopien schnell und bequem gespeichert und ausser Haus gebracht werden.

Versichertenkarte: Leistungserbringer können gespeicherte Einträge abändern – ohne Wissen des Patienten

Dem Wandel der Technik Rechnung tragen

Das Erlassen von Vorschriften mit einem Ermessensspielraum kann aus Sicht der Technik zu Ungewissheit darüber führen, welche Sorgfalt in der IT anzuwenden ist. In Artikel 7 Absatz 1 DSG[8] und Artikel 8 Absatz 2 VDSG[9] wird etwa gefordert, dass Daten angemessen zu schützen sind. Aus Sicht der Technik stellt sich die Frage: «Was ist konkret zu unternehmen und welche Massnahmen sind umzusetzen?» Zur Illustration der Problematik folgendes Beispiel aus der realen Welt: Angenommen, eine Brücke ist über einen Fluss zu errichten. Aus Sicht eines Bauingenieurs stellt sich nun unter anderem die Frage, wie tragfähig und wie breit die Brücke mindestens sein muss. Wegen des Kostendrucks und des rapiden Anstiegs

der Kosten bei steigender Sicherheit wird erfahrungsgemäss eingehend darüber diskutiert, ob eine Massnahme wirklich umgesetzt werden muss. Für die Rechtssicherheit bedarf es nicht nur qualitativer, sondern auch quantitativer Vorschriften.

Ein möglicher Lösungsansatz dieser Problematik ist eine den Umständen kontinuierlich anzupassende Bundesvorschrift, welche anleitet, mit welchen technischen Mitteln entsprechend klassifizierte Güter (geheim, vertraulich) zu schützen sind.

Mit einem Anschluss ans Internet ist man mit der «ganzen» Welt verbunden, das Datennetz ist international. Bei der Verletzung von Rechtsgütern sind die praktischen Möglichkeiten beschränkt, Recht durchzusetzen, wie etwa Schadenersatz einzufordern oder strafrechtliche Sanktionen zu verhängen. Zudem ist bei politischen Delikten wie bei wirtschaftlichem Nachrichtendienst (Artikel 273 StGB) kein Rechtshilfegesuch ans Ausland möglich.[10] Also benötigt das dem Internet ausgesetzte Rechtsgut mehr Schutz, als allgemein vermutet wird.

Ausdrücke wie «Stand der Technik und des Wissens» in den Vorschriften führen zu Rechtsunsicherheit. Der Wandel der Technik, insbesondere in der IT, ist enorm. Um folglich diesem Wandel Rechnung zu tragen, greift der Erlassgeber bei der Festlegung der gebotenen Sorgfalt gerne zu Formulierungen wie «Stand der Technik und des Wissens».[11] Gemäss der Rechtsanwältin Eugénie Holliger-Hagmann krankt der «Stand des Wissens» jedoch an einer beträchtlichen Unbestimmtheit, weil er uferlos ist.[12]

Das menschliche Wesen verleitet dazu, im Umgang mit Gefahren unvorsichtig zu sein. Wie Nassim Taleb[13] darlegt, neigen Menschen dazu, aus der in der Vergangenheit gemachten Erfahrung, das heisst aus dem Ausbleiben schädlicher Ereignisse, zu schliessen, dass künftig weiterhin keine schädlichen Ereignisse eintreten werden. Im Umfeld einer Risikoabschätzung gibt bereits die Frage, ob bisher jemals so etwas passiert ist, dieser These recht. Weiter werden aussergewöhnliche Ereignisse in der Risikobetrachtung unbewusst ausgeblendet. Keinen Beweis für die Existenz eines Ereignisses zu finden, ist kein Beweis für dessen Nichtexistenz.

Fachgremien mit Juristen und Technikern nötig

Der fehlende Blick auf den ganzen Prozess führt dazu, den Erlass von Vorschriften zu vergessen. Hätte man alle Geschäftsfälle und den gesamten Prozess betreffend elektronische Signaturen betrachtet, so wäre mit grosser Wahrscheinlichkeit nicht unterlassen worden, zu definieren, wie elektronisch signierte Dokumente zu archivieren sind.

Um Missverständnisse in der Kommunikation zu beheben, bedarf es der entsprechenden Bildung auf Universitätsstufe, zum Beispiel das Angebot, ein den Bedürfnissen entsprechendes Nebenfach in Recht oder IT zu absolvieren. Dies würde das gegenseitige Verständnis für die unterschiedliche Herangehensweise bei der Problemlösung fördern und helfen, der Sache gerechte Vorschriften zu erlassen. Zudem sollten mehr interdisziplinäre Fachgremien geschaffen werden, in welchen Techniker und Juristen paritätisch vertreten sind. Dies ist bei dem vom Bund geförderten Verein eCH[14] nicht der Fall, weil die Juristen dort untervertreten sind. Die Rechtsgüter sind wie im Gesundheitswesen zu wichtig, als dass man die technische Realisierung und Standardisierung alleine den Technikern überlassen darf.

Daniel Muster

1 Art. 371 Abs. 2 ZGB und Art. 6 Abs. 1 Bst. i VVK.
2 Siehe Anhang VVK.
3 «Ständerat lehnt automatische Organspende ab»,«Tages-Anzeiger» vom 28.11.2013.
4 Stratenwerth/Wohlers, Schweizerisches Strafgesetzbuch, Handkommentar, Bern 2007.
5 Stefan Trechsel, Schweizerisches Strafgesetzbuch – Kurzkommentar, Zürich 1989.
6 Schweizerisches Strafgesetzbuch, in Kraft seit 1. Januar 1942.
7 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur.
8 Bundesgesetz über den Datenschutz.
9 Verordnung zum Bundesgesetz über den Datenschutz.
10 Bundesgesetz über internationale Rechtshilfe in Strafsachen, Art. 3 Abs. 1 IRSG in Kombination mit Art. 30 Abs. 1 IRSG.
11 Vgl. Art. 8 Abs. 2 VDSG und Art. 3 Abs. 2 Bundesgesetz über die Produktesicherheit (PrSG).
12 Eugénie Holliger-Hagmann, Produktesicherheitsgesetz PrSG, Zürich 2010, S. 125 ff., Kommentar zu Art. 3 Abs. 2 PrSG.
13 Nassim Nicholas Taleb, Der Schwarze Schwan, München 2007.
14 eCH (www.ech.ch) ein Verein zur Standardisierung des elektronischen Behördenverkehrs.