

Dennis-Kenji Kipker

Unbestimmte Rechtsbegriffe

Durch das IT-Sicherheitsgesetz wird mit dem § 8a BSIG als wesentliche Verpflichtung für den Betreiber einer Kritischen Infrastruktur festgelegt, dass angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der genutzten informationstechnischen Systeme zu treffen sind, um die Funktionsfähigkeit der Kritischen Infrastruktur aufrechtzuerhalten. Bei der Umsetzung dieser Anforderung soll der „Stand der Technik“ eingehalten werden. Was aber hierunter zu verstehen ist, wird durch das Gesetz selbst nicht bestimmt. In der Gesetzesbegründung heißt es dazu im Wesentlichen nur, dass der Stand der Technik der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen ist, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen gesichert erscheinen lässt. Zur näheren Bestimmung wird auf internationale, europäische und nationale Normen und Standards verwiesen.

Bei solchen bewusst offen formulierten gesetzlichen Angaben handelt es sich um sogenannte „unbestimmte Rechtsbegriffe“, die im IT-Sicherheits- und Datenschutzrecht an verschiedenen Stellen Verwendung finden. So zum Beispiel für die Einwilligungserteilung nach § 4a BDSG für den Begriff der „freien Entscheidung“ des Betroffenen, ebenso für die Ausnahme vom Schriftformerfordernis bei Vorliegen „besonderer Umstände“. Der Bezug zu Datenschutz und Datensicherheit ergibt sich aber auch nicht immer unmittelbar aus dem Gesetz, so beispielsweise für die §§ 91 Abs. 2, 93 Abs. 1 AktG. Hier heißt es lediglich, dass der Vorstand geeignete Maßnahmen zu treffen hat, damit „den Fortbestand der Gesellschaft gefährdende Entwicklungen“ früh erkannt werden. Daneben haben die Vorstandsmitglieder bei ihrer Geschäftsführung „die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ anzuwenden. Allgemein anerkannt ist, dass unter ebenjene Beobachtungs- und Sorgfaltspflichten auch Maßnahmen der IT-Sicherheit zu fassen sind.

Unbestimmte Rechtsbegriffe kommen grundsätzlich immer dann zur Anwendung, wenn es unpraktikabel scheint oder unmöglich ist, einen Lebenssachverhalt vollumfänglich durch eine gesetzliche Vorschrift zu regeln. Gerade auch, weil sich Datenschutz und Datensicherheit aus einem engen Zusammenspiel von Recht und Technik ergeben, besteht hier das Bedürfnis, den unbestimmten Rechtsbegriff als eine Schnittstelle zwischen den beiden letztgenannten Disziplinen zu verwenden. Ein weiterer Grund für die Nutzung der unbestimmten Rechtsbegriffe liegt in der damit verbundenen Technikoffenheit und der hieraus folgenden Anpassungsfähigkeit des Rechts an die zukünftige und nicht selten rasche Entwicklung im Bereich der Informationssysteme. Denn im

Zweifelsfall lässt sich das allgemeine Verständnis einer Rechtsvorschrift flexibler und schneller anpassen als die Schaffung eines neuen Gesetzes möglich ist, sollten sich die technologischen Rahmenbedingungen wieder einmal geändert haben.

Obwohl die Verwendung von unbestimmten Rechtsbegriffen unter rechtsstaatlichen Gesichtspunkten somit grundsätzlich zulässig und sogar erwünscht ist, kann sie in der Anwendungspraxis mit erheblichen Schwierigkeiten verbunden sein. Nicht nur, dass unbestimmte Rechtsbegriffe auch gesetzliche Pflichten regeln können, die bei Verstoß zu einem Schadensersatzanspruch führen oder bußgeldbewehrt sind – wie zum Beispiel im Falle der durch das BSIG nach § 8a zu treffenden technischen und organisatorischen Vorkehrungen. Auch die zur Konkretisierung erforderliche – und damit zur Verwendung der entsprechenden Gesetze zwingend notwendige – Auslegung der unbestimmten Rechtsbegriffe kann vor allem unter zwei Gesichtspunkten Probleme bereiten: Erstens dann, wenn durch sie auf Sachverhalte Bezug genommen wird, die außerhalb des Rechts liegen. Zweitens in dem Falle, wenn die Konkretisierung der unbestimmten Rechtsbegriffe nicht oder noch nicht in abschließender Weise erfolgt ist. Das ist primär bei neu geschaffenen Gesetzen der Fall. Um auch für diese Fälle Rechtssicherheit zu schaffen, ist unter Zuhilfenahme der zumeist in der Gesetzesbegründung aufgeführten Konkretisierungsquellen möglichst rasch die Ausfüllung der entsprechenden unbestimmten Rechtsbegriffe vorzunehmen.

Speziell für das neue IT-Sicherheitsrecht stellt sich diese Problematik in beiderlei Hinsicht, denn die Regelungen beispielsweise im BSIG stellen nicht nur eine Querschnittsmaterie mit deutlichem Technikbezug dar, sondern sind auch gesetzgeberisches Neuland, sodass hier im Wesentlichen nicht auf eine bereits bestehende Auslegungserfahrung zurückgegriffen werden kann. Gleichwohl ist der durch die neuen Vorschriften Verpflichtete nicht völlig auf sich allein gestellt. Jüngst hat beispielsweise der Bundesverband IT-Sicherheit „TeleTrusT“ eine aus der Gremienarbeit hervorgegangene Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes publiziert,¹ daneben werden in der Literatur Konzepte zur Maßstabsbestimmung vorgeschlagen². Ebenso lassen sich bereits bestehende technische Normen und Standards unter Umständen direkt mit (neuen) unbestimmten Rechtsbegriffen verknüpfen – entsprechende Forschungsarbeit wird schon jetzt geleistet.

¹ Abrufbar unter https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf (Stand: 13.07.2016).

² Siehe *Michaelis*, DuD 2016, 458 ff.