www.betriebs-berater.de

Betriebs Berater

BB

47 | 2024

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

18.11.2024 | 79. Jg.
Seiten 2689–2752

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dr. Axel-Michael Wagner, RA, und Stefan Groß, StB, CISA

Zu den neuen Vorgaben des BSI bei der Kassendatenfiskalisierung, oder: Die Grenzen administrativer Rechtssetzung im Rechtsstaat – Teil II

Im ersten Teil des Beitrags wurde die historische Entwicklung der BSI-Vorgaben im Kontext von § 146a AO und der Kassensicherungsverordnung, fokussiert auf die Vorgaben im Bereich Umgebungsschutz und PKI, nachgezeichnet. Darauf aufbauend untersucht der zweite Teil die technische Notwendigkeit und die verfassungsrechtliche Rechtfertigung dieser umfangreichen Vorgaben und schließt mit einem Blick über den Tellerrand auf die Herausforderungen der Technikgesetzgebung insgesamt.

VII. Fehlende Herleitung und Begründung der sachlichen Notwendigkeit

Bevor die neuen Vorgaben neben den beschriebenen formalen Einwänden auch aus materiellrechtlicher Sicht hinterfragt werden, soll kurz allgemein darauf eingegangen werden, ob Sachnotwendigkeiten insbesondere aufgrund relevanter Risikoszenarien und einer plausiblen Risikobewertung erkennbar sind, die zu diesen Vorgaben Anlass gegeben haben. Die entsprechenden Erkenntnisse haben rechtlich Bedeutung für die Erforderlichkeit im Rahmen der Verhältnismäßigkeitsprüfung, doch dazu später mehr.

Was die Anforderungen an den Umgebungsschutz anbelangt, die großen Einfluss auf grundlegende Entscheidungen sowohl des Steuerpflichtigen als auch von TSE-Herstellern haben, enthält das „unterstützende Dokument" des BSI keine Begründung bzw. Herleitung des geforderten Niveaus des Umgebungsschutzes anhand von plausibel hergeleiteten Risikoszenarien (einschließlich Eintrittswahrscheinlichkeit und möglichem Schaden). In der Literatur wurde zwar 2020 befürchtet, es sei nur eine Frage der Zeit, bis im Hinblick auf die damals neuen Vorgaben „die ersten Computerfreaks wieder neue Möglichkeiten für ‚Schummler' geschaffen haben";[109] Indizien, dass dies tatsächlich der Fall ist und die Anforderungen an den Umgebungsschutz deshalb schon wieder nachjustiert werden müssen, sind aber nicht ersichtlich. Das BSI geht vielmehr unspezifisch von theoretischen (technischen) Angriffsszenarien aus, die – unausgesprochen – „um jeden Preis" verhindert werden sollen, ohne zu untersuchen, wie aufwendig und wahrscheinlich diese Szenarien in der Praxis sind und in welcher Relation das Risiko zu den vom BSI vorgegebenen Härtungs- bzw. Abhilfemaßnahmen steht. Dies ist auch deshalb relevant, weil im Vorfeld der Veröffentlichung des „unterstützenden Dokuments" von Verbänden durchaus derartige Risikobeurteilungen angestellt und alternative Absicherungs- und Architekturkonzepte vorgestellt wurden. So kam eine Risikoanalyse der Arbeitsgruppe „Fiskalisierung" des Bundesverbands IT-Sicherheit e. V. 2021[110] zu dem Schluss, dass – wie schon eingangs erwähnt – das gewichtigste Manipulationsszenario mit dem mit großem Abstand höchsten Schadenspotenzial die Nichteingabe von Umsätzen in die Kasse ist. Dieses Risiko werde mit der gesetzlichen Belegausgabepflicht[111] zwar abgemildert, aber nicht verhindert. Dieses Szenario selbst und dessen fehlende Verhinderbarkeit durch technische Maßnahmen erkannte übrigens auch bereits das BSI im ursprünglichen SMAERS-Schutzprofil von 2020.[112] Sämtliche anderen aktuell vorhandenen Manipulationsrisiken würden, so die genannte Risikoanalyse von 2021, schon durch die bisherigen Maßnahmen (TSE-Einsatz, Belegausgabepflicht, Einzelaufzeichnungspflicht, Meldeverfahren, Kassen-Nachschauen) weitgehend verhindert, sofern eine Cloud-TSE (im Sinne einer Cloud-CSP-Komponente) eingesetzt wird. Im Gegensatz zu Hardware-TSEs seien Abschalteinrichtungen bei Cloud-TSEs aufgrund der permanenten Verbindung bzw. der Protokollierung von Verbindungsproblemen im Übrigen schwieriger zu realisieren. Manipulationen an einer (auch ohne hinreichenden Umgebungsschutz) lokal betriebenen SMAERS-Komponente selbst würden hingegen viel Spezialwissen erfordern, seien schwierig umzusetzen und im Prüfkonzept der Finanzverwaltung leicht zu erkennen. Derartige Risiken seien demnach auch ohne (weiter risikominimierendes) Umgebungsschutzkonzept verhältnismäßig klein und akzeptabel. Zusätzlich zur detaillierten Risikoanalyse wurden auch alternative technische Konzepte für eine zusätzliche Absicherung der SMAERS-Komponente vorgeschlagen, etwa eine Virtualisierung (Betrieb einer virtuellen Maschine auf dem Kassensystem) ohne lokalen Hardware-Sicherheitsanker[113] oder ein Kassensystem-Backend, das gemeinsam mit einer SMAERS-Komponente vom Frontend getrennt (und ggf. in der Cloud betrieben) wird.[114]

Unabhängig davon, ob man diese Risikoanalyse in ihren Einzelbewertungen teilt, erscheint zumindest fraglich, ob die vom BSI im „unterstützenden Dokument" zugrunde gelegten Standard-Angriffsvektoren aus dem Baukasten der IT-Sicherheit („Hackerangriffe" etc.) und die implizite Risikobewertung des BSI, die sich aus den nunmehr vorgegebenen (Umgebungsschutz-)Maßnahmen erschließen lässt, auch bei einer auf den Einsatzzweck (Fiskalisierung von Kassendaten) fokussierten Risikoanalyse angemessen wären. Als Beispiel soll hier die konkrete Vorgabe des Einsatzes eines TPM-2.0-Moduls dienen. Nur

109 Vgl. *Teutemacher*, AO-StB 2020, 123, 125.

110 Zwischenbericht der TeleTrusT-AG „Fikalisierung" vom 18.2.2021 (nicht veröffentlicht), versandt u. a. an das BMF und das BSI.

111 § 146a Abs. 2 S. 1 AO.

112 Vgl. SMAERS-Schutzprofil, Kap. 3.2: „The TOE [d. h. die SMAERS-Komponente] does not protect against threats that result from temporarily or permanently not using an ERS as required by law."

113 Ein Schutz vor Cloning würde dann durch besondere Kommunikation zwischen der auf der virtuellen Maschine laufenden SMAERS-Komponente mit der fernverbundenen CSP-Komponente sichergestellt.

114 Dieser letzte Architekturvorschlag entspricht konzeptionell den schon seit 2020 tatsächlich betriebenen Cloud-TSE-Angeboten, die eine einzelne Komponente des Kassensystems „in die Cloud ziehen", um die SMAERS-Komponente dann dort „daneben" zu betreiben.

bei „erhöhtem Schutzbedarf" wird in dem vom BSI erstellten, allgemein auf die Sicherheit von IT-Systemen bezogenen „IT-Grundschutz-Kompendium" mittlerweile (2023) – als Regel mit Ausnahmemöglichkeit – ein TPM-2.0-Modul und weitere Mechanismen zum Schlüsselschutz gefordert.[115] Das Ziel ist dort, Datenträger eines Servers „mit einem als sicher geltenden Produkt oder Verfahren" zu verschlüsseln, wobei nicht nur das TPM alleine als Schlüsselschutz dienen sollte. Das – ohnehin rechtlich unverbindliche – Grundschutz-Kompendium sieht zwar im Regelfall den Einsatz eines TPM-2.0-Moduls nicht vor, aber inhaltlich korrespondiert die vom Grundschutz-Kompendium im Fall eines „erhöhten Schutzbedarfs" für notwendig gehaltene sichere (insbesondere TPM-2.0-gestützte) Datenträgerverschlüsselung mit den BSI-Anforderungen an die TSE im Bereich der Ausführungsumgebung für die SMAERS-Komponente („sicherer Speicher für sensible Objekte").[116] Die Frage ist also, ob auch bei der Kassenfiskalisierung von einem (derart) „erhöhten Schutzbedarf" auszugehen ist, zumal dieser Begriff aus dem Bereich der IT-Sicherheit[117] für die Ausfüllung von § 146a AO zweckentfremdet wurde und die sonstigen Vorkehrungen bzw. Prozesse des einzelnen Steuerpflichtigen bei dieser pauschalen Annahme keine Rolle spielen. Eine Analyse der spezifischen Risiken im Rahmen möglicher Manipulation von Kassendaten kann – wie oben aufgezeigt – durchaus zu dem Schluss führen, dass Manipulationsszenarien hinsichtlich SMAERS-Objekten, die ausschließlich durch ein TPM-2.0-Modul verhindert werden können, nicht wahrscheinlich genug sind, um diese konkrete technische Forderung zu rechtfertigen. Nach alledem erscheint schon unabhängig von einer (verfassungs-)rechtlichen Betrachtung höchst zweifelhaft, ob die generelle Forderung nach einer „räumlichen Nähe" von Kassensystem und SMAERS-Komponente – zumindest im Zusammenspiel mit neuen Anforderungen im Bereich des Umgebungsschutzes an eine (in Erfüllung der Forderung der „räumlichen Nähe") lokal betriebene SMAERS-Komponente wie beispielsweise dem Einsatz eines TPM-2.0-Moduls – eine so wesentliche (weitere) Risikoverminderung bedeutet, dass dies noch im Verhältnis zum Aufwand der dafür notwendigen Maßnahmen steht.

Nur am Rande soll darauf hingewiesen werden, dass auch die Anforderungen an den Umgebungsschutz in iOS- und Android-Umgebungen in der Praxis nicht mit vernünftigem Aufwand umsetzbar sind.[118] Die Frage der dahinterstehenden, implizit vom BSI getroffenen Risikoabwägung stellt sich hier in gleicher Weise.

Was unabhängig davon die hier exemplarisch untersuchten neuen PKI-Vorgaben des BSI anbelangt, so ist schon die generelle Notwendigkeit einer PKI-Lösung im Zusammenhang mit TSEs zu hinterfragen. Die Zuordnung einer TSE zu einem Steuerpflichtigen geschieht nicht über ein übliches PKI-Zertifikat zur (unauflösbaren) Zuordnung eines Schlüssels zu einer identifizierten Person, sondern – ohne dass die gesetzliche Grundlage das vorsehen würde[119] – über die Seriennummer der TSE im Rahmen der Meldung nach § 146a Abs. 4 S. 1 Nr. 3 AO. Diese Zuordnung lässt sich durch eine erneute, anderweitige Meldung auch wieder lösen, sodass eine PKI im klassischen Sinn gar nicht notwendig ist. Dennoch basieren die neuen PKI-Vorgaben des BSI – ähnlich wie der Umgebungsschutz – auf der Grundannahme, dass höchste Sicherheitsstandards gelten müssen,[120] mithin auf einer impliziten Risikoabwägung, dass die bisherigen, oben skizzierten PKI-Vorgaben nicht ausreichen und nicht einmal die gesetzlichen Vorgaben zu Vertrauensdiensten ausreichend sind. Die zugrunde liegenden Motive und Szenarien sind unklar. Wenn es darum geht, dass die Finanzverwaltung „ermächtigt" werden soll, Zertifikate zu sperren[121] – was weder in der KassenSichV noch in den AEAO zu § 146a erwähnt geschweige denn hinsichtlich der Voraussetzungen definiert wäre –, so ist darauf hinzuweisen, dass auch die gesetzlichen Grundlagen im Rahmen der eIDAS-Infrastruktur den zuständigen Behörden diese Möglichkeit einräumen.[122] Der Hauptfall der Sperrung – und damit das zentrale Risikoszenario – dürfte gegeben sein, wenn der private Schlüssel aus der CSP-Komponente ausgelesen und missbräuchlich verwendet wird oder eine Hardware-TSE abhandenkommt.[123] Bei einer in der Cloud von einem TSE-Hersteller gehosteten CSP-Komponente ist dieser Fall ohnehin nicht relevant, weil ein Angriff des TSE-Herstellers auf seine eigenen TSEs nicht zu den plausiblen Angriffsvektoren zählt. Selbst wenn aber im Falle einer Hardware-TSE eine solche Form des Verlusts des privaten Schlüssels vorliegt, gibt es keinen Grund zu der Annahme, dass der Mechanismus im Rahmen der eIDAS-Vorgaben nicht ausreichend wäre. Damit bleibt von den hier exemplarisch untersuchten neuen PKI-Vorgaben nur noch die (in den eIDAS-Vorgaben nicht enthaltene) Anforderung relevant, bei Auslaufen oder Widerruf des TSE-Zertifikats – etwas, das der Steuerpflichtige nicht beeinflussen kann und möglicherweise gar nicht erfährt und das ggf. nur auf einem Verdacht beruht – umgehend die mit diesem Zertifikat assoziierte TSE durch „Fernlöschung" ihres privaten Schlüssels endgültig unbrauchbar zu machen. Das ist aber kein „Risikoszenario" im technischen Sinn, sondern die Folge einer inhaltlichen, im Grunde rechtspolitisch hoch brisanten Entscheidung,[124] TSEs nun mittelbar auch „physisch" an das zugrundeliegende Zertifikat zu koppeln und im Falle eines Wegfalls des Zertifikats „ferngesteuert zu zerstören". Für diese vom TSE-Hersteller umzusetzenden Vorgaben des BSI bieten weder § 146a AO noch die in § 11 Abs. 1 S. 1 KassenSichV genannten § 9 BSI-Gesetz und BSI-ZertV eine hinreichende Rechtsgrundlage.

VIII. Eingriff in die Berufsausübungsfreiheit und Vorgaben für das eingreifende Gesetz

Vorstehend wurde dargelegt, dass im Fokusbereich der vorliegenden Ausführungen einerseits das neue „unterstützende Dokument" des BSI nicht näher hergeleitete oder begründete Anforderungen an den Umgebungsschutz für bestehende IT-Infrastrukturen des Steuerpflichtigen und andererseits die überarbeitete TR-03153 nicht näher hergeleitete oder begründete Anforderungen an eine TSE-spezifische PKI stellen. Neben der formalen gesetzlichen (Ermächtigungs-) Grundlage ist die inhaltlich-technische Notwendigkeit dieser Vor-

115 Vgl. IT-Grundschutzkompendium des BSI, Ed. 2023, Kap. SYS.1.1.A34.
116 S. o.
117 Vgl. Definition der Schutzbedarfskategorien des BSI, anwendbar seit 1.11.2019.
118 So muss in Bezug auf Android der PlayStore von Google zum Einsatz kommen, während andere Store-Alternativen wie PAXStore für POS-Systeme ausgeschlossen werden.
119 § 146a Abs. 4 S. 1 Nr. 3 AO spricht nur von der Art der TSE, was begrifflich nicht deren individuelle Seriennummer einschließt. Erst AEAO zu § 146a, Abschnitt 1.16.2.2 fasst darunter – nicht rechtlich verbindlich – auch die Seriennummer.
120 Vgl. TR-03145-5, Kap. 1.
121 Vgl. TR-03145-5, Anlage B, zu den möglichen Werten der Felder „RevokingPartys" und „RevocationReason".
122 Dabei ist insbesondere darauf hinzuweisen, dass § 14 Abs. 3 VDG auch die Anordnung des Widerrufs eines Zertifikats durch die „Aufsichtsstelle", nämlich die Bundesnetzagentur (vgl. § 2 VDG), vorsieht.
123 Vgl. auch die Sperrungsgründe als mögliche Werte des Felds „RevocationReason" in Anlage B der TR-03145-5. Der dort angegebene „Defekt" der TSE führt ohnehin dazu, dass diese nicht mehr einsatzfähig ist, also auch keinen „Schaden" anrichten kann.
124 Hier steht ein Eingriff in das Eigentumsrecht des Steuerpflichtigen an seiner Hardware-TSE zur Diskussion.

gaben im Sinne einer sich aus plausiblen Risikoszenarien ergebenden angemessenen Risikobewertung und Risikosteuerung zweifelhaft. In der Folge stellt sich die Frage nach den rechtlichen Maßstäben, an denen die rechtlichen Vorgaben – beginnend mit § 146a AO selbst – inhaltlich zu messen sind.

Aus verfassungsrechtlicher Perspektive ist insbesondere die in Art. 12 Abs. 1 GG[125] verbürgte Berufsausübungsfreiheit relevant. Art. 12 Abs. 1 GG schützt vor Beeinträchtigungen, die gerade auf die berufliche Betätigung bezogen sind, indem sie eine Berufstätigkeit unmittelbar unterbinden oder beschränken.[126] Durch § 146a AO, die KassenSichV, die Technischen Richtlinien, das SMAERS-Schutzprofil und das „unterstützende Dokument" des BSI wird das privatwirtschaftliche Handeln von Steuerpflichtigen in (Bar-)Geldgeschäften verschiedener Wirtschaftszweige (wie Einzelhandel und Gastronomie) aus Gründen der Sicherung des Steueraufkommens durch unmittelbare und – über die von diesen Regelungen erzwungene Vorgaben des TSE-Herstellers gegenüber dem Steuerpflichtigen – mittelbare Verhaltenspflichten reguliert. Es steht außer Frage, dass hierdurch die „Bewegungsfreiheit bei der beruflichen Betätigung" der Steuerpflichtigen, auch durch Zwang zur Tätigung wesentlicher Investitionen (Beschaffung von TSE-Infrastruktur), die sie sonst aus originärem beruflichem Eigeninteresse nicht tätigen würden, eingeschränkt wird. Bei den TSE-bezogenen Verpflichtungen des Steuerpflichtigen handelt es sich gerade nicht um die Auferlegung von Steuern und Abgaben als solcher, für die Art. 12 GG nicht einschlägig ist,[127] sondern um einen Eingriff in die unternehmerische Gestaltungs- und Entscheidungsfreiheit. Steuerpflichtige müssen durch die erweiterten Vorgaben zum Umgebungsschutz, wenn sie ein entsprechendes Cloud-TSE-Produkt (weiterhin) nutzen wollen, spätestens aufgrund der neuen Anforderungen[128] und in noch intensiverem Maße als bisher schon Teile ihrer IT-Infrastruktur der Administration eines fremden Dritten unterwerfen, Hardware anschaffen und ggf. vorher in einem System integrierte Funktionalitäten auftrennen.

TSE-Hersteller hingegen haben für das Erlangen der notwendigen BSI-Zertifizierung die BSI-Vorgaben unmittelbar einzuhalten (§ 9 BSI-Gesetz). Die Ausrichtung an den BSI-Vorgaben ist somit Grundvoraussetzung für die unternehmerische Betätigung der TSE-Hersteller im TSE-Markt. Zwar gewährleistet die Berufsausübungsfreiheit keinen Anspruch auf die „erfolgreiche Marktteilnahme oder künftige Erwerbsmöglichkeiten", der Schutzbereich des Art. 12 Abs. 1 GG ist jedoch dann berührt, wenn Normen einen unmittelbaren Berufsbezug aufweisen oder zumindest die Rahmenbedingungen der Berufsausübung so verändern, sodass diese in einem „engen Zusammenhang mit der Ausübung eines Berufs stehen" und „objektiv eine berufsregelnde Tendenz" haben.[129] Die BSI-Vorgaben wirken sich unmittelbar auf die berufliche Betätigung der TSE-Hersteller in ihrer Entscheidung, wie sie ihre TSE ausgestalten zu haben, aus. Aus der Perspektive der TSE-Hersteller betreffen die BSI-Vorgaben nicht nur die Rahmenbedingungen der unternehmerischen Tätigkeit (wie beispielsweise Meldepflichten), sondern beschränken die Berufstätigkeit unmittelbar.[130]

Daraus ergibt sich ohne Weiteres, dass auch die hier im Fokus stehenden Umgebungsschutzanforderungen des BSI (als Teil der TSE-bezogenen BSI-Vorgaben) an der Berufsausübungsfreiheit zu messen sind, und zwar sowohl im Hinblick auf den TSE-Hersteller als auch, aufgrund der erzwungenen Weitergabe der Zertifizierungsvorgaben an den Steuerpflichtigen im Wege des Umgebungsschutzkonzepts, im Hinblick auf die Steuerpflichtigen. Schon die im SMAERS-Schutzprofil von 2020 enthaltene Anforderung, dass die SMAERS-Komponente in derselben „operationalen Umgebung" wie das elektronische Aufzeichnungssystem (also das Kassensystem) betrieben werden muss, schränkte den Steuerpflichtigen spürbar ein.[131] Es war danach nicht zulässig, das elektronische Aufzeichnungssystem mit der SMAERS-Komponente „fernzuverbinden" – im Gegensatz zu der vom BSI ausdrücklich erlaubten sog. „client server"-Architektur, d. h. einer Fernverbindung innerhalb des Sicherheitsmoduls selbst (lokale SMAERS-Komponente und über einen sicheren Übertragungsweg fernverbundene CSP-Komponente).[132] Damit wurden – trotz der grundsätzlich gewollten Technologieoffenheit[133] – bestimmte Architekturen erlaubt, andere verboten. Es kann durchaus argumentiert werden, dass bereits in diesem Verbot die Einschränkung der Berufsausübungsfreiheit liegt bzw. lag. Vorliegend steht jedoch die wesentliche Verschärfung der bisherigen Anforderungen in beiden (exemplarischen) Themenkomplexen Umgebungsschutz und PKI im Fokus, die jeweils dazu führen, dass bestehende Architekturen und Produkte mit hohem Aufwand spätestens im Rahmen der nächsten Re-Zertifizierung verändert und erweitert werden müssen. Die Änderungen bzw. Erweiterungen der Vorgaben des BSI 2023 zum Umgebungsschutz stellen der grundsätzlichen architektonischen Forderung von 2020 konkrete, in der Praxis letztlich kaum erfüllbare Forderungen zur Beschaffenheit der zugrunde liegenden IT-Umgebung zur Seite und sind geeignet, bestehende und an die neuen Vorgaben anzupassende Produkte aufgrund ebenjener neuer Vorgaben aus dem Markt zu drängen. Hinzu kommen die PKI-Vorgaben an die TSE-Hersteller, die diesen die – ihnen nach den bisherigen Vorgaben belassene – Freiheit bei der Ausgestaltung entsprechender Infrastrukturen nehmen. Insgesamt handelt es sich um eine massive Einschränkung der Gestaltungsfreiheit der TSE-Hersteller beim Design ihrer Produkte.

Alle hier relevanten Vorgaben betreffen damit im Ergebnis das Verfahren und die Mittel der Berufstätigkeit[134] – Entgegennahme von Bargeld als Gegenleistung (Steuerpflichtige) bzw. Inverkehrbringen von TSEs (TSE-Hersteller) – und stehen „in so engem Zusammenhang mit der Ausübung ihres Berufes, dass sie objektiv eine berufsregelnde Tendenz haben".[135]

Eingriffe in die Berufsausübungsfreiheit sind nur dann gerechtfertigt, wenn sie „durch oder aufgrund eines Gesetzes" (Art. 12 Abs. 1 S. 2 GG) erfolgen und darüber hinaus verhältnismäßig sind. Schon das Vorhandensein einer ausreichenden parlamentarischen Gesetzesgrundlage ist, wie oben bereits im Kontext zu Art. 80 GG erläutert,

125 Für inländische juristische Personen i. V. m. Art. 19 Abs. 3 GG, vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 59 ff.
126 BVerfG, 30.6.2020 – 1 BvR 1679/17, 1 BvR 2190/17, BVerfGE 155, 238, 277, Rn. 95 m. w. N., st. Rspr.
127 Die Auferlegung von Steuern und Abgaben selbst eröffnet regelmäßig nicht den Schutzbereich des Art. 12 Abs. 1 GG, sondern den des Art. 2 Abs. 1 GG, es sei denn, die Regelung hat „objektiv berufsregelnde Tendenz", vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 127.
128 Wenn sie diese Vorgaben der Umgebungsschutzkonzepte bislang, aus welchen Gründen auch immer, nicht eingehalten haben.
129 BVerfG, 30.6.2020 – 1 BvR 1679/17, 1 BvR 2190/17, BVerfGE 155, 238, 277, Rn. 96; BVerfG, 20.4.2004 – 1 BvR 905/00, 1 BvR 1748/99, BVerfGE 110, 274, 288 f., Rn. 41.
130 Vgl. BVerfG, 30.6.2020 – 1 BvR 1679/17, 1 BvR 2190/17, BVerfGE 155, 238, 277, Rn. 98.
131 Vgl. SMAERS-Schutzprofil, Kap. 3.4: „The ERS [d. h. elektronisches Aufzeichnungssystem] and the TOE [d. h. SMAERS-Komponente] must be contained in the same physical operational environment that must protect the integrity of communication data between the TOE and the electronic record-keeping system".
132 Vgl. SMAERS-Schutzprofil, Kap. 3.4, illustriert auf S. 17 unter c).
133 Vgl. BT-Drs. 18/9535, 14 unten und 17 („technologieneutral").
134 Vgl. *Burgi*, in: Kahl/Waldhoff/Walter, Bonner Kommentar zum GG, Stand: Juni 2024, Art. 12 Abs. 1, Rn. 122.
135 Vgl. BVerfG, 13.7.2004 – 1 BvR 1298/94 u. a., BVerfGE 111, 191, 213, Rn. 143.

zweifelhaft. Denn § 146a AO ist als das ermächtigende Gesetz zu abstrakt und schafft – auch zusammen mit der auf dieser Basis erlassenen KassenSichV – keine „ausreichend dichte parlamentsgesetzliche Vorordnung“[136]. Das BSI hat vielmehr die einzelnen Teile der TSE nach Belieben definieren und darüber hinausgehende Pflichten (wie den Betrieb einer PKI oder die Erfüllung von Umgebungsschutzanforderungen) nach Belieben ausgestalten können, weil es insoweit in § 146a AO an entsprechenden, konkretisierenden Vorgaben durch den Gesetzgeber fehlt. Gerade die wesentlichen Richtungsentscheidungen sind jedoch dem Parlamentsgesetzgeber vorbehalten, wobei das zu ermächtigende Gesetz eine der Wesentlichkeit der Materie entsprechende Regelungsdichte aufweisen muss.[137] Je intensiver die Beeinträchtigung der Berufsfreiheit, desto strengere Anforderungen sind an die (parlamentsgesetzliche) Regelungsdichte zu stellen.[138] Zumindest die neuen, konkretisierten Vorgaben zum Umgebungsschutz und zur PKI machen eine entsprechende gesetzgeberische Entscheidung im Rahmen von § 146a AO erforderlich.[139] Schon in formaler Hinsicht ist damit den Anforderungen des Art. 12 GG nicht Genüge getan.

IX. Verfassungsrechtliches Übermaßverbot

Lässt man das formale Problem der unzureichenden gesetzlichen Grundlage einmal beiseite, ist auf inhaltlicher Ebene beim Eingriff in die Berufsausübungsfreiheit das verfassungsrechtliche Übermaßverbot einzuhalten. Sowohl die gesetzliche Grundlage für einen Eingriff in die Berufsausübungsfreiheit – hier § 146a AO – als auch eine untergesetzliche Grundlage müssen nach vernünftigen Erwägungen des Allgemeinwohls zweckmäßig erscheinen[140], d. h. verhältnismäßig sein.[141] Dabei führt die mangelnde Dichte der parlamentsgesetzlichen Vorordnung (s. o.) übrigens dazu, dass das BSI bei der Festlegung seiner hier in Rede stehenden Vorgaben keine Einschätzungsprärogative für sich in Anspruch nehmen, d. h. die Verhältnismäßigkeit seiner Vorgaben nicht selbst anhand von Prognoseentscheidungen bewerten konnte.[142]

Schon die obigen Ausführungen zur sachlichen Notwendigkeit des Umgebungsschutzes, insbesondere zu einer bislang fehlenden dokumentierten Herleitung der entsprechenden Vorgaben sowie am Zweck orientierten Bewertung von Risiken und Alternativen durch das BSI, lassen bezweifeln, dass die neuen Vorgaben des BSI erforderlich sind. Erforderlich wären die neuen Vorgaben zum Umgebungsschutz, wenn für die Erreichung des Zwecks des Schutzes von Kassendaten gegen nachträgliche Manipulationen kein anderes Mittel zur Verfügung steht, das – in der Formulierung des Bundesverfassungsgerichts – „den Grundrechtsträger weniger und Dritte und die Allgemeinheit nicht stärker belastet“.[143] Darüber hinaus müssen sämtliche technischen Forderungen im Verhältnis zum verfolgten Zweck und dem verfolgten Risiko stehen und für die Betroffenen zumutbar sein.[144] Es genügt rechtlich beispielsweise nicht, einen Angriff des Steuerpflichtigen auf einzelne Elemente der SMAERS-Komponente (nur) zu postulieren. Entscheidend ist, ob die Dringlichkeit des Zwecks, nachträgliche Manipulationen zu verhindern, in einem angemessenen Verhältnis mit den die Schwere der Beeinträchtigungen der vorgegebenen Maßnahmen steht.[145] Keinesfalls kann eine Verschärfung der Anforderungen alleine durch das Argument rechtfertigt werden, dass in einer hypothetischen Statistik einzelne Manipulationsfälle entfallen würden, sondern die Anforderungen müssen insgesamt im Verhältnis zum verfolgten Zweck stehen. Was den Umgebungsschutz anbelangt, erscheint schon die ursprüngliche Forderung des BSI, wonach das Kassensystem und die SMAERS-Komponente in derselben „operationalen Umgebung“ betrieben werden muss, ausdrücklich auch zulässigerweise vermittelt durch ein LAN-Kabel in denselben Räumlichkeiten, nicht erforderlich. Eine räumliche Nähe von IT-Komponenten hat in der heutigen IT-Welt keinerlei eigenständigen Wert im Hinblick auf den Zugriff Unbefugter, auch wenn das BSI dies unter Rückgriff auf das (rechtliche!) Argument desselben „Verantwortlichen“ behauptet.[146] Ein milderes, gleich geeignetes Mittel für den Umgebungsschutz ist zumindest die Vorgabe einer gesicherten Fernverbindung zwischen Kassensystem und SMAERS-Komponente, um den Umgebungsschutz innerhalb der Cloud-Umgebung des TSE-Herstellers – und nicht in lokalen Systemen des Steuerpflichtigen – abbilden zu können. Auf dieses Argument wird noch im Zusammenhang mit der Gleichbehandlung verschiedener TSE-Hersteller bzw. -Architekturen zurückzukommen sein: Gleichartige Gefahrenpotenziale (Manipulation) an verschiedenen Stellen innerhalb derselben Kausal- bzw. (Daten-)Verarbeitungskette werden ohne sachlichen Grund – und ohne ersichtliche Reflektion seitens des Normgebers – unterschiedlich bewertet und gesteuert. Die strikteren Vorgaben an einer der beiden Stellen können rechtlich dann nicht „erforderlich“ sein, wenn sie an der anderen Stelle nicht für erforderlich gehalten wurden.

Was das Thema PKI anbelangt, erscheinen schon die bisherigen Vorgaben des BSI als milderes, gleich geeignetes Mittel zur Regelung der PKI-Ausgestaltung. Selbst wenn man dies – warum auch immer – anders sähe, wäre jedenfalls der bestehende gesetzliche Regelungsrahmen für PKIs (im Wesentlichen die eIDAS-VO) ein milderes, gleich

136 Vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 188 m. w. N.

137 Vgl. *Grzeszick*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 20 Abs. 1, Rn. 106.

138 Vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 188 m. w. N.

139 Dabei besteht das Problem nicht – wie häufig in derartigen Fällen – darin, dass das BSI in untergesetzlichen Vorgaben den Bewertungs- und Einschätzungsspielraum des Gesetzgeber unterlaufen hat (vgl. *Grzeszick*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 20 Abs. 1, Rn. 120), sondern darin, dass der Gesetzgeber diesen Spielraum überhaupt nicht genutzt hat, was im Rahmen von Art. 12 GG seine Pflicht gewesen wäre.

140 Die vom BVerfG im sog. „Apothekenurteil“ entwickelte Stufenlehre besagt zwar, dass Eingriffe in die Berufsausübungsfreiheit gerechtfertigt sind, „soweit vernünftige Erwägungen des Gemeinwohls es zweckmäßig erscheinen lassen“ (BVerfG, 11.6.1958 – 1 BvR 596/56, BVerfGE 7, 377, 404 ff.). Die Prüfung der Verhältnismäßigkeit nach dem Übermaßverbot (legitimer Zweck, Geeignetheit, Erforderlichkeit, Angemessenheit/Zumutbarkeit) hat die Stufenlehre in der nachfolgenden Rechtsprechung zu Art. 12 Abs. 1 GG jedoch nicht ersetzt. Die Kriterien der Stufenprüfung werden vielmehr in der Verhältnismäßigkeitsprüfung mit herangezogen, vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 156 ff.

141 Vgl. nur *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 155, 157.

142 Vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 171 f. Der behördliche Gestaltungsspielraum für eine Prognoseentscheidung ist vielmehr gerade aus der gesetzlichen Grundlage heraus zu entwickeln, vgl. *Schmidt-Aßmann*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 19 Abs. 4, Rn. 197a.

143 Vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 175 m. w. N.

144 Vgl. *Grzeszick*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 20 Abs. 1, Rn. 119.

145 Die Prüfung der Angemessenheit/ Zumutbarkeit eines Eingriffes fordert eine Gesamtabwägung zwischen „der Schwere der […] Grundrechtsbeeinträchtigung“ mit dem „Gewicht und der Dringlichkeit der sie rechtfertigenden Gründe“, BVerfG, 23.3.2022 – 1 BvR 1187/17, BVerfGE 161, 63, 122, st. Rspr.; auf die vom BVerfG entwickelte „Stufenlehre“ (s. o.) wird hier im Rahmen der Zumutbarkeit einzugehen sein, vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 165.

146 Vgl. Supporting Document for Common Criteria Protection Profile SMAERS, Kap. 8, Evaluation Activity EA8.6: „Regarding the security requirements, the physical operational environment of the ERS extends to the entire contiguous area in which the ERS is located and for which the operator of the ERS is directly responsible. Therefore, e.g. operation of the SMAERS component located in a different room of the branch in whose salesroom the ERS is located is compliant (i. e. different room on the same premises).“

geeignetes Mittel zur Regelung der PKI-Ausgestaltung auch für TSEs. Es ist in keinem Fall ersichtlich, weshalb die wesentlich strikteren Vorgaben des BSI erforderlich im Sinne des Übermaßverbots sind.

Unabhängig davon erscheinen die strengeren Vorgaben auch nicht zumutbar, da vorliegend kein „angemessener Ausgleich zwischen dem Eingriffsgewicht" der BSI-Vorgaben und dem „verfolgten gesetzgeberischen Ziel", mithin „zwischen Individual- und Allgemeininteresse", erreicht wurde.[147] Die Eingriffe in die Berufsausübungsfreiheit wiegen schwer, denn die BSI-Vorgaben betreffen Steuerpflichtige wie TSE-Hersteller in ihrer unternehmerischen Freiheit, die Bedingungen ihrer Berufsausübung selbst zu bestimmen, und stellen zusätzlich eine wesentliche finanzielle Belastung dar, die insbesondere für die Steuerpflichtigen weit unterschätzt wurde. Die Einschränkungen durch die Vorgaben an den Umgebungsschutz und die PKI sind zudem von Dauer, da die Zertifizierung durch das BSI „fortlaufend aufrechtzuerhalten ist", § 146a Abs. 3 S. 2 AO.[148] Nach dem Gedanken der Stufenlehre sind die Eingriffe auch nicht nach „vernünftige[n] Erwägungen des Gemeinwohls"[149] zweckmäßig. Es ist insbesondere in Bezug auf die hier exemplarisch diskutierten Umgebungsschutz- und PKI-Vorgaben kein Grund ersichtlich, dass die bisherigen Vorgaben in diesen Bereichen unzulänglich waren und zu nennenswerten Manipulationsfällen geführt hätten, deren Ursache es zu beseitigen gilt. Wie oben dargelegt, gibt es schon keine systematische Untersuchung (des Normgebers) zu der Frage, welche Manipulationsrisiken sich mit welcher Wahrscheinlichkeit realisieren (bzw. welchen Aufwands seitens des Angreifers bedürfen), geschweige denn dazu, welche Schutzmaßnahmen welchen Aufwand (seitens des Normadressaten) notwendig machen, sodass diese beiden Größen auch nicht miteinander verglichen werden konnten. Stattdessen wurden letztlich pauschal „maximale" Schutzmaßnahmen vorgegeben, bei denen keine praktikablen, auf Verhältnismäßigkeitserwägungen im einzelnen konkreten Fall beruhenden Ausnahmen[150] vorgesehen sind. Im Kontext solcher „maximaler" Vorgaben, deren Einhaltung besondere Ressourcen erforderlich macht, ist auch zu berücksichtigen, dass erhebliche Manipulationsrisiken an anderen Stellen durch eben diese Vorgaben gerade nicht minimiert werden können,[151] d. h. während bestimmte Manipulationsszenarien – ohne Nachweis, dass diese tatsächlich drohen – durch horrenden Aufwand vermieden werden sollen, bleiben andere Manipulationsszenarien, da schwieriger oder gar nicht kontrollierbar, unangetastet. Weiter ist unter dem Stichwort „Bestandsschutz" zu berücksichtigen, dass durch die Änderung der BSI-Vorgaben, die im Rahmen der nächsten Rezertifizierung zu beachten sind,[152] langfristige Investitionsplanungen auf den Kopf gestellt werden; es wird also auch aufgrund des zeitlichen Moments in bestehende Verhältnisse in einer Intensität eingegriffen, die der damaligen Einführung des § 146a AO ähnlich ist – für die ein Vorlauf von vier (tatsächlich über fünf) Jahren zur Anwendung kam –, ohne dass ein überwiegender Grund dafür ersichtlich ist. Damit führen die neuen Vorgaben ohne nachvollziehbaren wesentlichen Nutzen dazu, dass die bisherigen Produkte nicht mehr verwendet werden können und auf alternative Produkte ausgewichen werden muss (Sicht des Steuerpflichtigen) bzw. neue Produkte mit erheblichem Aufwand geschaffen werden müssen (Sicht des TSE-Herstellers). Das ist für beide Gruppen von Normadressaten unzumutbar, zumal Hardware-TSEs als Alternative insbesondere für Filialisten aufgrund der Anzahl der zu verwaltenden und jeweils ein gekapseltes Einzelsystem darstellenden Hardware-TSEs nicht praktikabel sind.[153] Ein angemessener Interessensausgleich wurde so nicht erzielt; die neuen BSI-Vorgaben schränken Steuerpflichtige und TSE-Hersteller unzumutbar in ihrer Berufsausübungsfreiheit ein.

X. Ungleichbehandlungen und mögliche Auflösungen

In Verbindung mit der oben dargestellten Thematik des Eingriffs in die Berufsausübungsfreiheit liegt zudem nahe, dass sowohl im Kontext von § 146a AO an sich als auch im Kontext der BSI-Vorgaben zur SMAERS-Komponente ohne Vorliegen eines sachlichen Grundes vergleichbare Sachverhalte unterschiedlichen Vorgaben unterworfen werden. Dies führt dazu, dass Steuerpflichtige bzw. TSE-Hersteller, die eine bestimmte Architektur verwenden, anders behandelt werden als Steuerpflichtige bzw. TSE-Hersteller, die ein andere Architektur verwenden, ohne dass ein (technischer) Grund für die Ungleichbehandlung besteht. Verfassungsrechtlich steht ein Verstoß gegen das Gleichbehandlungsgebot (Art. 3 Abs. 1 GG ggf. i. V. m. Art. 19 Abs. 3 GG) in Rede.[154]

Einerseits werden das elektronische Aufzeichnungssystem und die TSE ungleich behandelt, die beide – bis zur Signatur in der CSP-Komponente der TSE – „ungesicherte" fiskalisierungspflichtige Daten verarbeiten. Vorgaben für die Ausgestaltung des elektronischen Aufzeichnungssystems (bzw. Kassensystems als Untermenge) enthält ausschließlich § 146a Abs. 1 S. 1 AO in abstrakter Form und ohne delegierte Konkretisierungsmöglichkeit.[155] Dem Hersteller eines elektronischen Aufzeichnungssystems bleibt es somit selbst überlassen, wie und in welcher Intensität er das System selbst gegen unbefugte Eingriffe „härtet" oder seinem Kunden, dem Steuerpflichtigen, entsprechende Vorgaben macht.[156] Auch das BSI weist in seinen Regularien zum Umgebungsschutz darauf hin, dass es (natürlich) keine Vorgaben für das elektronische Aufzeichnungssystem selbst macht.[157] Der Implementationsaufwand der Hersteller von Kassensystemen im Zuge der Einführung von § 146a AO bestand dementsprechend „lediglich" darin, die intern im Kassensystems anfallenden Daten inhaltlich in

147 BVerfG, 23.3.2022 – 1 BvR 1187/17, BVerfGE 161, 63, 122, m. w. N., st. Rspr.

148 Für Unternehmen steht der mit der Berufsausübung verbundene Gelderwerb – und damit mittelbar auch Kostenerhöhungen – bei der Bewertung der Schwere der Beeinträchtigung im Vordergrund. Wenn neben dem reinen Gelderwerb Eingriffe in die unternehmerische Entscheidungsfreiheit erfolgen, wie hier durch die Umgebungsschutzanforderungen, tritt dies erschwerend hinzu. Auch das Ausmaß der finanziellen Einbußen und die Dauer der Beeinträchtigungen sind entsprechend zu berücksichtigen, vgl. *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 103. EL Jan. 2024, Art. 12 Abs. 1, Rn. 178.

149 BVerfG, 11.6.1958 – 1 BvR 596/56, BVerfGE 7, 377, 405.

150 Vgl. etwa Tz. 170 der GoBD (Selbstbindung der Verwaltung) im Kontext des Datenzugriffs der Finanzverwaltung: „Die Finanzbehörde hat bei Anwendung der Regelungen zum Datenzugriff den Grundsatz der Verhältnismäßigkeit zu beachten."

151 Vgl. *Teutemacher*, AO-StB 2020, 123, 125.

152 Nach Kap. 2.1.1 und 2.1.2 des Anhangs A zur TR-03153 darf der Abschluss der Zertifizierung nach der vormaligen TR-03153 nicht nach dem 30.4.2025 liegen, ansonsten ist nach der Version 1.1.1 der TR-03153 zu verfahren. Das BSI, das bekanntlich das Zertifizierungsverfahren in der Zeit abschließt, die vom BSI benötigt wird, „kann" dann ausnahmsweise Verlängerungen zulassen.

153 So können in diesem Fall etwa die abgesicherten TSE-Daten sämtlicher TSEs des Steuerpflichtigen nicht im Rahmen zentraler Archivsysteme zusammengeführt werden, was die BSI-Vorgaben an das Speichermedium ausdrücklich zulassen.

154 *Dreier*, GG, Bd. I, 4. Aufl. 2023, Art. 3 Abs. 1, Rn. 31.

155 Insbesondere aufgrund der Verordnungsermächtigung in § 146a Abs. 3 S. 1 Nr. 1 AO darf vom Verordnungsgeber nur definiert werden, welche Untermenge aller elektronischen Aufzeichnungssysteme mit einer TSE abzusichern sind.

156 Vgl. auch Gesetzesbegründung in BT-Drs. 18/9535, 11, zum Zustand „außerhalb" der neuen TSE-Regelungen: „Bislang bestehen keine gesetzlichen Vorgaben zur Gewährleistung der Integrität, Authentizität und Vollständigkeit von digitalen Grundaufzeichnungen." Dieser Zustand besteht für das elektronische Aufzeichnungssystem auch nach Einführung der TSE-Vorgaben des § 146a AO fort.

157 Vgl. „unterstützendes Dokument" zum SMEARS-Schutzprofil, Kap. 7.1: „This supporting document does not further define nor specify the ERS component."

das maßgebliche Datenformat der „einheitlichen digitalen Schnittstelle" (DSFinV-K) zu überführen und über die sog. Einbindungsschnittstelle im Sinne der TR-03153[158] zur „Absicherung" (Zähler, Zeitstempel, Signatur) durch die TSE zur Verfügung zu stellen. Die SMAERS-Komponente der TSE erhält diese Output-Datensätze des Kassensystems in Echtzeit. Auch wenn das Inverkehrbringen von elektronischen Aufzeichnungssystemen, welche die abstrakten Vorgaben des § 146a Abs. 1 S. 1 AO nicht einhalten, formal nach § 146a Abs. 1 S. 1 AO verboten ist, muss dennoch im Streitfall nur die Einhaltung der genannten Vorgaben – anhand eines sich aus dem Gesetz nicht ergebenden Granularitäts- bzw. Sicherheitsmaßstabs – nachgewiesen werden, nicht aber die Einhaltung von BSI-Richtlinien und -Schutzprofilen.

Im Unterschied dazu werden für eine nachgelagerte Komponente innerhalb desselben Datenverarbeitungsstrangs, d.h. für die TSE (und die Ausführungsumgebung der SMAERS-Komponente), die oben ausschnittsweise aufgezeigten „Hochsicherheitsvorgaben" gemacht, obwohl die Vorfallsdaten in der Sphäre des elektronischen Aufzeichnungssystems vor ihrer Fiskalisierung (d.h. signierenden Absicherung in der CSP-Komponente) ebenso „vulnerabel" sind wie innerhalb der SMAERS-Komponente der TSE. Diese ungerechtfertigte Ungleichbehandlung muss dem Gesetzgeber selbst angelastet werden, der die Datenherkunft ohne formale Kontrolle (§ 146a Abs. 1 S. 1), die „Fiskalisierung" aber mit hohem formalem Kontrollaufwand (TSE, § 146a Abs. 1 S. 2 bis 4, Abs. 3 AO) ausgestaltet hat. Nach dem Prinzip „garbage in, garbage out" bringt eine hochsichere Fiskalisierung von bereits im elektronischen Aufzeichnungssystem aufgrund mangelnder Sicherheitsvorgaben manipulierter Ausgangsdaten nichts.[159] Der berüchtigte „Überbrückungsknopf" an der Kasse (um jegliche Aufzeichnungen temporär zu unterbinden) ist nach wie vor möglich, wenn auch der dann unterdrückte Einsatz der TSE im Ausdruck des entsprechenden Bons – sofern dann noch einer erstellt wird – identifizierbar ist. Flächendeckend (etwa durch Testkäufe seitens der Finanzverwaltung) können derartige Auffälligkeiten ohnehin nicht geprüft werden.

Im Ergebnis werden hier die Hersteller von (datenproduzierenden) elektronischen Aufzeichnungssystemen und von (datensignierenden) TSE-Systemen ungleich behandelt, nämlich völlig unterschiedlichen Dichten belastender Regelungen unterworfen, obwohl sie dieselben Datensätze in unterschiedlichen Verarbeitungsphasen – aber mit gleicher Manipulationsanfälligkeit – verarbeiten.

Andererseits führt die Unzulässigkeit einer Fernverbindung von Kassensystem und SMAERS-Komponente im Gegensatz zur Möglichkeit einer Fernverbindung von SMAERS- und CSP-Komponente im Rahmen der BSI-Regularien dazu, dass Austauschmechanismen (Datenschnittstellen) zwischen Verarbeitungs-Teilschritten unterschiedlich behandelt werden. Es handelt sich um ein strukturell ähnliches Gleichbehandlungsproblem wie oben im ersten Fall, wenn auch im Kontext der TSE selbst und auf Ebene der untergesetzlichen (BSI-) Vorgaben. Das Kassensystem stellt Datensätze zur Verfügung, die von der SMAERS-Komponente der TSE übernommen und von dort an die CSP-Komponente und zurück (über die SMAERS-Komponente) in das – zulässigerweise auch außerhalb der TSE selbst liegende[160] – Speichermedium übermittelt werden. Während das BSI den Transport der noch ungesicherten (ungestempelten und unsignierten) Daten zwischen SMAERS-Komponente und CSP-Komponente toleriert, wenn dies über eine gesicherte Fernverbindung („Trusted Channel") erfolgt, soll die SMAERS-Komponente hingegen in unmittelbarer räumlicher Nähe (d.h. in derselben physikalischen operationalen Umgebung) des elektronischen Aufzeichnungssystems betrieben werden. Dabei ist die zugrunde liegende (Sicherheits-)Anforderung – die Wahrung der „Integrität der Kommunikation" – in beiden Fällen identisch.[161] Für die Wahrung der Kommunikationsintegrität ist die Art der Anbindung insbesondere im Missbrauchsfall jedoch gar nicht bedeutsam, oder andersherum ausgedrückt: Jede Fernverbindung kann abgeschaltet werden, jede Hardware-TSE und damit die Verbindung von Kassensystem und TSE (inkl. SMAERS-Komponente) kann willkürlich getrennt werden[162] – was in beiden Fällen sowohl vom Sender als auch vom Empfänger registriert werden kann.[163] Es gibt deshalb auch aus dem Gesichtspunkt von Missbrauchsszenarien keinen Grund, unterschiedliche Arten der Anbindung vorzugeben, zumal gerade bei unterschiedlichen Missbrauchsrisiken der verschiedenen Anbindungsformen einer (nämlich der „missbrauchsärmeren") Form einheitlich für beide Sachverhalte der Vorzug gegeben werden müsste.

Im Ergebnis werden hier die Hersteller von TSE-Systemen, welche innerhalb der TSE die SMAERS- und die CSP-Komponente fernverbinden wollen, und die Hersteller von TSE-Systemen, welche das Kassensystem und die TSE fernverbinden wollen, ungleich behandelt, ob-

158 Vgl. TR-03153, Kap. 3.5 und 5.1.

159 Es kann – mangels Begründung seitens des BSI – nur vermutet werden, dass es auch ein Ziel des Umgebungsschutzes war, mittelbar das elektronische Aufzeichnungssystem selbst mit zu „härten". Auch wenn sich nach den BSI-Vorgaben das elektronische Aufzeichnungssystem und die SMAERS-Komponente der TSE nicht auf demselben physischen System, sondern nur in physischer Nähe zueinander, befinden müssen, werden beide doch in der Praxis aufgrund von Ressourcenerwägungen meist auf demselben System ablaufen. Da auf der Laufzeitumgebung der SMAERS-Komponente daneben nur Applikationskomponenten des elektronischen Aufzeichnungssystems als „Nutzlast" erlaubt sein sollen (s.o.), würde in diesem Fall der Umgebungsschutz der SMAERS-Komponente auch dem elektronischen Aufzeichnungssystem „zugute" kommen. Da aber weder das Gesetz noch die KassenSichV noch – folgerichtig – die BSI-Regularien Vorgaben für den Umgebungsschutz des elektronischen Aufzeichnungssystems selbst vorsehen, ist es ohne weiteres möglich, das elektronische Aufzeichnungssystem in einer anderen – unsicheren – Umgebung als die SMAERS-Komponente ablaufen zu lassen. Die BSI-Regularien für die TSE können auch nicht in die gesetzliche Vorgabe des § 146a Abs. 1 S. 1 AO für elektronische Aufzeichnungssysteme „hineininterpretiert" werden, wie sich aus der im Text aufgezeigten, im Gesetz bewusst angelegten Ungleichbehandlung ergibt.

160 Vgl. TR-03153, Ziff. 6: externes Aufbewahrungssystem „und somit außerhalb der Sicherheitseinrichtung".

161 Vgl. Schutzprofil SMAERS, Kap. 3.4: „The integrity of the communication data between TOE [d.h. SMAERS-Komponente] and CSP in the client-server architecture is protected via a trusted channel" bei Trennung von SMAERS- und CSP-Komponente und „protect the integrity of communication data between the TOE [d.h. SMAERS-Komponente] and the electronic record-keeping system" für die Kommunikation zwischen Kassensystem und SMAERS-Komponente.

162 Insoweit ist die Aussage von *Bron/Schroeder*, BB 2022, 279, 282, dass Systeme „mit nutzerseitig vollständig abtrennbarer Technischer Sicherheitseinrichtung" einen Verstoß gegen §§ 146a Abs. 1 S. 1, S. 5 AO darstellen würden, in dieser Pauschalität nicht richtig, weil die TSE nach dem Gesetz gerade kein integraler Bestand des elektronischen Aufzeichnungssystems ist, sondern „nur" eine an dieses (technisch) „angebundene" (so das BSI) Einrichtung.

163 Die Diskussionen in Fachkreisen 2021/2022 fokussierten sich u.a. auf ein „Denken vom Notfallmodus her", d.h. inwieweit bestimmte (Verbindungs-)Konstellationen von Kassensystem und TSE durch „vorsätzliches Außerkraftsetzen" der Übermittlungswege (Internet-Zugang etc.) letztlich zu einem – vom Gesetzgeber nicht gewollten – nicht TSE-abgesicherten Kassensystem (mit einer „untätigen TSE in der Cloud") führen würden. Eine Fortsetzung solcher Szenarien ist die lokale Zwischenspeicherung von Vorfallsdaten ohne TSE (aufgrund eines Verbindungsabbruchs), deren lokale Löschung und anschließende Neuverbindung, sodass Vorfallsdaten verlorengehen und die TSE nie erreichen (dieses „Manipulationsszenario", d.h. eine Divergenz zwischen tatsächlichen und von der TSE aufgezeichneten Vorfällen, ist allerdings auch mit anderen Mitteln umsetzbar). Ein manipulatives Ausnutzen eines Notfallmodus' des Kassensystems ist bei entsprechender (in der TSE-Produktlandschaft auch verwendeter) Architektur durchaus serverseitig erkennbar (und damit auch im Rahmen einer Kassennachschau oder Betriebsprüfung feststellbar). Diese Diskussionen können überhaupt bei der Frage der räumlichen Nähe zwischen Kassensystem und SMAERS-Komponente keine Rolle spielen, weil auch bei der – nach den BSI-Regularien zulässigen – Nahverbindung über ein LAN-Kabel in denselben Räumlichkeiten dieses vorsätzlich unterbrochen („ausgesteckt") und das Kassensystem mit entsprechendem Datenverlust neu gestartet werden kann.

wohl dieselben (noch unsignierten) Datensätze über die jeweilige Fernverbindung übermittelt werden bzw. würden. Diese nicht rechtfertigbare Ungleichbehandlung wirkt im Rahmen der Argumentation zu Art. 12 GG auch auf die Erforderlichkeit der BSI-Vorgaben zurück: Das BSI hält bei diesen zwei aufeinanderfolgenden, gleich strukturierten Übermittlungsvorgängen mit Daten derselben „verwundbaren" Qualität – Datenübermittlung zwischen elektronischem Aufzeichnungssystem und SMAERS-Komponente der TSE einerseits und Datenübermittlung zwischen SMAERS-Komponente und CSP-Komponente innerhalb der TSE andererseits – im ersten Fall eine physische Nähebeziehung im Rahmen des Übermaßverbots (s. o.) für erforderlich, im zweiten Fall aber nicht. Von zwei unterschiedlichen Vorgaben für strukturell gleich gelagerte und deshalb gleich zu behandelnde Sachverhalte kann aber nicht die eine erforderlich, die andere aber nicht erforderlich sein.

Dies wiederum führt zu der Frage, wie eine Gleichbehandlung der beiden dargestellten, jeweils ungleich behandelten Themen herbeigeführt werden kann. Hinsichtlich der Ungleichbehandlung von elektronischem Aufzeichnungssystem und TSE könnte der Gesetzgeber entweder derart weitreichende, mehrstufige und technisch ausgefeilte Schutzkonzepte wie für die TSE auch für elektronische Aufzeichnungssysteme selbst installieren,[164] oder er schafft die zusätzlichen technischen Vorgaben für die TSE ab und überlässt es den TSE-Anbietern wie den Steuerpflichtigen, wie sie im Einzelfall – wie beim elektronischen Aufzeichnungssystem selbst – nachweisen, auf welche (technische) Weise die generellen Voraussetzungen des Gesetzes (§ 146a Abs. 1 S. 1 AO) eingehalten wurden. Hinsichtlich der Ungleichbehandlung der Datenschnittstellen könnte das BSI entweder auch eine Fernverbindung zwischen elektronischem Aufzeichnungssystem und SMAERS-Komponente über einen „Trusted Channel" – ebenso wie zwischen SMAERS- und CSP-Komponente – zulassen oder alternativ vorgeben, dass auch die CSP-Komponente in unmittelbarer räumlicher Nähe der SMAERS-Komponente liegen muss. Wohlgemerkt: Damit würden nur die Ungleichbehandlungen formal beseitigt; welche dieser Lösungen nach (verfassungs-)rechtlichen Kriterien materiell (insbesondere am Maßstab des Art. 12 GG) zulässig wäre, ist damit noch nicht gesagt.

Unabhängig von der Frage der (verfassungs-)rechtlichen Zulässigkeit solcher alternativer Konstellationen aber mag man sich vorstellen, welcher Aufschrei und Investitionsbedarf droht, wenn BSI-Vorgaben in der jetzt für TSEs anwendbaren Regelungsdichte bzw. Detailtiefe auf jegliche steuerrelevanten elektronischen Aufzeichnungssysteme – nicht nur Kassensysteme als Untermenge – ausgeweitet würden, um die Vorgabe in § 146a Abs. 1 S. 1 AO für elektronische Aufzeichnungssysteme „technisch zu konkretisieren". Dabei ginge es entsprechend der Reichweite des (im Gesetz nicht definierten) Begriffs des elektronischen Aufzeichnungssystems exemplarisch neben Kassensystemen auch um ERP-Systeme, Dokumentenmanagement-Systeme, E-Mail-Clients und -Server oder Zugangssysteme für Mitarbeiter (z. B. zur Messung von Arbeitszeiten und vergütungspflichtigen Überstunden), hinsichtlich derer das BSI dann minutiös vorgeben würde, wie diese technisch sicherzustellen haben, dass jeder Vorgang und Vorfall „einzeln, vollständig, richtig, zeitgerecht und geordnet" aufgezeichnet wird. In diesen Bereichen darf bislang jeder Hersteller weitgehend selbst entscheiden, ob und welchen nichtgesetzlichen Regelwerken bzw. Normen er seine Produkte unterwirft, um die abstrakten Anforderungen des § 146a Abs. 1 S. 1 AO umzusetzen. Darauf aufbauend ist dann bislang allein der Steuerpflichtige am Zug – dokumentiert durch eine entsprechende, GoBD-konforme Verfahrensdokumentation –, die unter Einsatz dieser Systeme implementierten, steuerrelevanten Unternehmensprozesse zu definieren und damit[165] auch die Einhaltung der Vorgaben des § 146a Abs. 1 S. 1 AO bzw. der spiegelbildlichen GoBD-Vorgaben[166] sicherzustellen. Dies zeigt, dass die punktuell hohe Regelungsdichte im Kontext der TSE-Vorgaben – basierend auf einer punktuellen Delegation durch den Gesetzgeber – kaum sinnvoll bzw. praktisch auf weitere, ebenso relevante Verarbeitungsvorgänge erstreckt werden kann, selbst wenn das möglicherweise sogar aus profiskalischer Sicht wünschenswert wäre.

Ein Beispiel mag illustrieren, dass es durchaus auf Basis der unterschiedlichen Regelungsdichten für elektronische Aufzeichnungssysteme und TSEs Gestaltungsmöglichkeiten gibt, welche dazu führen, dass die Umgebungsschutzvorgaben des BSI – etwa die Verwendung eines TPM-2.0-Moduls – nicht vor Ort beim Steuerpflichtigen erfüllt werden müssen. Wird formal eine „kleine Komponente" eines über verschiedene Software-Module und Hardware-Plattformen verteilten Kassensystems[167] in der Cloud-Umgebung des TSE-Anbieters direkt „neben" der SMAERS-Komponente ausgeführt, so gelten für die Kommunikation zwischen den verschiedenen Modulen des Kassensystems untereinander die Anforderungen des BSI für die TSE (natürlich) nicht. Letztlich macht sich diese Gestaltung die Ungleichbehandlung von elektronischem Aufzeichnungssystem und TSE zunutze, um den Nachteil der Ungleichbehandlung der Daten-Schnittstellen auszugleichen. Derartige Konzepte führten in den Jahren 2021 und 2022 zu der Diskussion, wo genau der „Ort" des elektronischen Aufzeichnungssystems ist und ob jeder noch so kleine Teil eines Kassensystems zu einem (weiteren) „Ort" führt, an dem dann zulässigerweise auch die SMAERS-Komponente betrieben werden kann. Das BMF erwog, im Anwendungserlass zu § 146a AO festzuschreiben,[168] dass der Ort „derjenige Teil des elektronischen Aufzeichnungssystems [ist], an dem die abzusichernden Geschäftsvorfälle inhaltlich, unabhängig von ihrer Formatierung oder Codierung, erstmals vollständig vorliegen". Unabhängig von den sprachlichen Ungenauigkeiten[169] ist aber der Begriff eines „erstmaligen vollständigen Vorliegens" an einem physischen Ort bei verteilten Software-Anwendungen nicht nur interpretationsbedürftig, sondern auch willkürlich gestaltbar. Die Regelung wurde nicht übernommen und auch in den überarbeiteten BSI-Regularien findet sich kein Hinweis darauf, an welchem Ort verteilte Kassensysteme „liegen".[170] Die Lösung über einen „Wurmfortsatz" des Kassensystems in der Cloud des TSE-Anbieters, der in derselben (Cloud-)Umgebung ausgeführt wird wie dessen SMAERS-Komponente, bleibt also formal möglich, und bei einem Filialisten ist dann weder erforderlich, dass die lokal betriebenen Teile des Kassensystems über einen TPM-2.0-Schutz verfügen, noch, dass in jeder Filiale ein verschlossener Raum mit Zutrittsberechtigung nur für konzernfremde

164 Möglicherweise – wegen unterschiedlicher Risikogeneigtheit – auch nur für Kassensysteme als Untermenge der elektronischen Aufzeichnungssysteme.
165 D. h. nicht nur durch die Software allein.
166 Dabei enthalten die GoBD selbst auch keine konkreten technischen, sondern ausschließlich abstrakte, technologieunabhängige Vorgaben.
167 Im Extremfall nur eine „Empfangseinrichtung" außerhalb der TSE für die von anderen Komponenten des elektronischen Aufzeichnungssystems gesendeten Vorgangsdaten.
168 Zur „Bindungswirkung" von Anwendungserlassen s. o.
169 Insbesondere geht es nicht darum, dass die Geschäftsvorfälle selbst an einem bestimmten Ort „vorliegen", sondern die Daten darüber, und auch nicht irgendwelche Daten über die Geschäftsvorfälle, sondern gerade die durch die TSE abzusichernden.
170 Vgl. SMAERS-Schutzprofil, Kap. 8, zu EA8.6: „the physical operational environment of the ERS extends to the entire contiguous area in which the ERS is located".

Dritte eingerichtet wird, in dem sich ein PC mit der SMAERS-Komponente befindet.

XI. Die Drohkulisse Schätzung

In der Praxis der Steuerpflichtigen, die Kassensysteme mit verschiedenen Cloud-TSE-Architekturen einsetzen, wird immer wieder die Frage bedeutsam, welche (möglichen) Verstöße gegen formale Vorgaben des BSI bzw. (auf den Vorgaben des BSI beruhend) der TSE-Hersteller zu einer Schätzungsbefugnis des § 162 Abs. 2 S. 2 AO führen. Im Gegensatz zum Bußgeldrahmen bei einer Steuergefährdung durch „nicht richtiges Schützen" des Kassensystems mittels einer TSE (§ 379 Abs. 1 S. 1 Nr. 5 AO),[171] der bei 25 000 Euro liegt (§ 379 Abs. 6 AO), kann eine Steuerschätzung bei großen Unternehmen leicht zu ganz anderen „Schadensdimensionen" führen.[172] Dabei stellt sich zunächst die Frage der Beweislast, also wer in einem entsprechenden (finanzgerichtlichen) Verfahren nachweisen muss, dass die Buchführung bzw. die Aufzeichnungen – mit der Folge der Schätzungsbefugnis – „verworfen" werden konnten. Grundsätzlich wird zugunsten des Steuerpflichtigen vermutet, dass die Aufzeichnungen den Vorgaben entsprechen; diese Vermutung ist (erst) widerlegt, wenn die Buchführung und die Aufzeichnungen mit an Sicherheit grenzender Wahrscheinlichkeit materiell ganz oder teilweise nicht ordnungsgemäß sind. Die Finanzbehörde muss also nicht die Unrichtigkeit selbst und den genauen Umfang und das Ausmaß der Unrichtigkeit der Buchungen und Aufzeichnungen beweisen.[173] Zivilrechtlich würde man von einer widerleglichen Vermutung mit Beweiserleichterungen beim Gegenbeweis sprechen.

Die vorgenannte Beweiserleichterung bezieht sich allerdings auf die materielle Unrichtigkeit. Dementsprechend ist nach ständiger Rechtsprechung des BFH bei Buchführungsfehlern allgemein nicht auf die formale Bedeutung des Buchführungsmangels, sondern auf dessen sachliches Gewicht abzustellen,[174] und auch die Vorgaben der §§ 145, 146 AO (ebenso wie die „Vorgaben" der Finanzverwaltung etwa in den GoBD) geben mangels vergleichbarer Verhältnisse bei den einzelnen Steuerpflichtigen grundsätzlich nicht vor, wie die dortigen Pflichten im Einzelnen (technisch) zu erfüllen sind. In einer Entscheidung vom 28.11.2023 hat der BFH für Alt-Kassensysteme herausgearbeitet, dass zwar die Verwendung eines objektiv manipulierbaren Kassensystems grundsätzlich einen formellen Mangel von hohem Gewicht darstellt, sich in Anwendung des Verhältnismäßigkeitsgrundsatzes aber das Gewicht dieses Mangels im Einzelfall reduzieren kann, „wenn das Kassensystem zur Zeit seiner Nutzung verbreitet und allgemein akzeptiert war und eine tatsächliche Manipulation unwahrscheinlich ist".[175] Die Rechtsprechung folgt also der von § 158 Abs. 2 AO vorgegebenen Betrachtung „nach den Umständen des Einzelfalls", und eine objektive Manipulierbarkeit[176] heißt noch nicht, dass diese, vielleicht dem konkreten Steuerpflichtigen nicht einmal bekannte, Möglichkeit auch ausgenutzt wurde.

§ 158 Abs. 2 AO wurde zwischenzeitlich dahingehend ergänzt, dass die Buchführung des Steuerpflichtigen auch dann verworfen werden darf, wenn „die elektronischen Daten nicht nach der Vorgabe der einheitlichen digitalen Schnittstelle […] des § 146a […] zur Verfügung gestellt werden".[177] Die Finanzverwaltung interpretiert dies technisch, d. h. ob die Daten „in dem geforderten Datenformat vorgelegt werden".[178] Ist dies nicht der Fall, wird, so die Gesetzesbegründung, die Prüfung erschwert.[179] Die Frage aber, ob die Daten, wenn sie im richtigen Datenformat produziert wurden, auch unter korrekter Anwendung der BSI-Vorgaben für den Umgebungsschutz oder für die PKI eines TSE-Herstellers erstellt wurden, hat damit nichts zu tun. Mit anderen Worten: Auch bei Nichteinhaltung der Umgebungsschutzvorgaben durch den Steuerpflichtigen oder einer nicht den BSI-Vorgaben entsprechenden PKI durch den TSE-Hersteller genügen die „Output-Daten" der TSE als solche den formalen Formatvorgaben der DSFinV-K, d. h. sie sind les- und verarbeitbar.[180]

Durch Verstöße gegen einzelne (Umgebungsschutz-)Auflagen der TSE-Hersteller, die auf den BSI-Vorgaben basieren, erhöht sich mithin das Schätzungsrisiko im Zusammenhang mit § 158 Abs. 2 AO nicht. Selbst wenn durch derartige Unzulänglichkeiten – etwa wenn aus individuellen Gründen kein TPM-2.0-Modul eingesetzt wurde – im Rahmen einer Betriebsprüfung eine faktisch nachteilige Wirkung zum Nachteil des Steuerpflichtigen eintreten würde, kann das zumindest dadurch kompensiert werden, dass der Steuerpflichtige aufzeigt, die steuerrelevanten Daten in einem GoBD-konformen und entsprechend dokumentierten Prozess verarbeitet zu haben.

XII. Technikgesetzgebung am Beispiel von § 146a AO: Ein Fazit

Ob man aus alledem folgern muss, dass die *politische* Entscheidung für die TSE und deren Zertifizierung durch das BSI „Fehlgriffe" waren,[181] sei hier dahingestellt. Die vorstehenden Ausführungen anhand von Einzelthemen innerhalb der neuen BSI-Vorgaben zeigen aber jedenfalls, dass die neuen Vorgaben des BSI mit großer Wahrscheinlichkeit als „übergriffig" und *rechtlich* unwirksam zu qualifizieren sind. Das liegt einerseits am schon immer „wackeligen" Delegationskonzept des Gesetzgebers in Form der ungenügenden inhaltlichen Vorzeichnung der weiteren Gesetzesausfüllung durch untergesetzliche Normen. Gesetz- und Verordnungsgeber dürfen sich nicht damit begnügen, technische Leerbegriffe zu verwenden, deren inhaltliche Bedeutung vollständig nachgelagert von der Verwaltung mit Leben gefüllt wird.[182] Dies führt zu der Versuchung – sowohl ebenjener Ver-

171 Der Tatbestand lautet „wer ein in § 146a Abs. 1 S. 2 AO genanntes System nicht richtig schützt", was genaugenommen nicht richtig ist, denn § 146a Abs. 1 S. 2 AO verwendet uneingeschränkt den Begriff „elektronisches Aufzeichnungssystem", während erst die KassenSichV nach § 146a Abs. 3 S. 1 Nr. 1 AO die „die elektronischen Aufzeichnungssysteme, die über eine zertifizierte technische Sicherheitseinrichtung verfügen müssen" (als Teilmenge), definiert, auf die sich der Tatbestand des § 379 Abs. 1 S. 1 Nr. 5 AO beziehen soll.

172 Wobei unklar ist, ob sich beim Betrieb mehrerer Systeme gleicher Art, die (vermeintlich) gegen § 379 Abs. 1 S. 1 Nr. 4 oder 5 AO verstoßen, das Bußgeld multiplizieren. Die Frage der Tateinheit (§ 19 OWiG, vgl. dazu *Sackreuther*, in: BeckOK OWiG, 42. Ed., Stand: 1.1.2024, § 19, Rn. 10–14) musste insoweit noch nicht von Gerichten beantwortet werden.

173 Vgl. *Gercke*, in: Koenig, AO, 5. Aufl. 2024, § 158, Rn. 12 m. w. N.

174 Vgl. nur BFH, 14.12.2011 – XI R 5/10, BFH/NV 2012, 1921 (st. Rspr.).

175 Vgl. BFH, 28.11.2023 – X R 3/22, BB 2024, 1051.

176 Die täglichen Meldungen über neue Hintertüren in Systemen („zero-day exploits", vgl. Wikipedia, Exploit, abrufbar unter https://de.wikipedia.org/wiki/Exploit, Abruf: 25.9.2024) zeigen, dass kein einigermaßen komplexes System keine Manipulationsmöglichkeiten enthält.

177 Vgl. § 158 Abs. 2 Nr. 2 AO.

178 Vgl. AEAO zu § 158, Tz. 5.

179 Vgl. BT-Drs. 20/3436, 87, 88.

180 Unabhängig von den einzelnen „Vorfallsdatensätzen" enthalten die Stammdaten der genutzten TSE, die Teil des DSFinV-K-Formats sind, zwar die Seriennummer der TSE (als Hashwert des im Zertifikat enthaltenen öffentlichen Schlüssels), nicht aber TPM- oder PKI-spezifische Parameter (vgl. Datei „Stamm-TSE" nach Tz. 3.2.7 DSFinV-K sowie Kap. 9.3.2 der TR-03153, Version 1.1.1).

181 So *Kowallik*, DB 2022, 2697, 2699, unter Hinweis auf den Prozess gegen Alfons Schubeck vor dem LG München wegen Kassenmanipulationen.

182 Dies erst recht nicht, wenn es aufgrund der Neuheit der Materie auch keinen in internationalen oder EU-Normen festgelegten „Stand der Technik" gibt, auf den zurückgegriffen werden kann.

waltung als auch bei juristischer Auslegung –, die allgemeinen Rahmenvorgaben des Gesetzes, wie die einzelne, vollständige, richtige, zeitgerechte und geordnete Aufzeichnung in § 146a Abs. 1 S. 1 AO, als nur durch ganz bestimmte technische Umsetzungen eingehalten anzusehen. So aber, wie auch aus einer (fiktiven) gesetzgeberischen Anforderung, dass ein System „gegen Eingriffsmaßnahmen Unbefugter geschützt" sein muss, nicht gefolgert werden kann, dass Antiviren-Software mit bestimmten KI-Algorithmen verwendet werden muss, kann aus der Aufzählung in § 146a Abs. 1 S. 1 AO nichts über die Anforderungen an eine PKI des TSE-Herstellers oder über eine notwendige „physische Nähe" einzelner IT-Komponenten von elektronischem Aufzeichnungssystem und TSE gefolgert werden.

Es gibt gute (verfassungsrechtliche) Gründe dafür, warum ein Gesetzgeber im Rahmen der Gewaltenteilung die grundlegenden Abwägungen zu treffen hat und nicht nachgelagerte „Regelungsausfüller". Weder der Verordnungsgeber BMF noch eine „technische Behörde" wie das BSI haben das Verhältnis zwischen Risikobewertung und Risikosteuerung im Blick, weil sie sich dafür – anders als ein Gesetzgeber, der abgewählt werden kann – niemandem gegenüber rechtfertigen müssen. Das (absehbare) Argument, dass bestimmte technische Lösungen „notwendig" seien und deshalb die Vorgaben in diesem Sinne ausfallen „müssen", stößt hier an Grenzen, denn keine technische Lösung „muss" so oder so sein, sie „kann" immer auch so oder so sein. Genau diese Abwägung zwischen Aufwand (der Normadressaten) und Nutzen (für das Gemeinwohl) darf der Gesetzgeber nicht grundsätzlich, sondern allenfalls in den Details der Ausgestaltung aus der Hand geben. Ein Beispiel für eine gelungenere Umsetzung in einer mindestens ähnlich schwierigen „Digitalmaterie" sind die gesetzgeberischen leitlinienhaften Vorgaben in § 165 TKG, zum Teil unter Verweis auf den Stand der Technik, deren Konkretisierung dann – „unter Beachtung der verschiedenen Gefährdungspotenziale" und mit einem verbürgten Anhörungsrecht von Herstellern und Verbänden – in § 167 TKG der Bundesnetzagentur und dem BSI überlassen wird.

Abseits der fehlenden gesetzgeberischen „Leitplanken" betreffen die neuen Vorgaben des BSI sogar Bereiche, die gänzlich außerhalb der gesetzlichen Ermächtigung liegen, und nachdem eine Begründung des Bedarfs nach besonderen PKI- und Umgebungsschutz-Vorgaben im Rahmen der Regelsetzung durch das BSI nicht aufgezeigt, sondern einfach implizit vorausgesetzt wurde, ist auch nicht ersichtlich, wie die in diesen Vorgaben liegenden Grundrechtseingriffe „erforderlich" sein können, zumal die Vorgaben zum Umgebungsschutz auf der ungleichen Behandlung gleichartiger Sachverhalte beruhen.

Das letztlich vom BSI formulierte technische Grundprinzip der Fiskalisierung durch Signierung – der Gesetzestext selbst ging nicht zwangsläufig von einer elektronischen Signatur aus, sondern ließ offen, was im Sicherheitsmodul genau vor sich gehen würde[183] – hätte bereits im Gesetzestext des § 146a AO umrissen werden müssen: Vorfallsdaten des elektronischen Aufzeichnungssystems werden in Quasi-Echtzeit lückenlos und in einem definierten Datenformat an die TSE übermittelt, dort mit einem sicheren Zeitstempel versehen und gemeinsam mit einem jeweils verlässlich inkrementierten Transaktions- und Signaturzähler elektronisch signiert, um dann für den späteren Zugriff durch die Finanzverwaltung gespeichert zu werden. Im Rahmen einer solchen abstrakten Datenflussbeschreibung hätte dann – unter Beachtung des Übermaßverbots, insbesondere bei genauer Analyse der Erforderlichkeit – vorgegeben werden müssen, dass und nach welchem abstrakten Maßstab die sich dabei ergebenden Funktionseinheiten und Schnittstellen zwischen diesen Funktionseinheiten abzusichern sind.

Dabei hätte im Bereich der Signierung selbst auf bestehende gesetzliche Konzepte zurückgegriffen werden können, die aus gutem Grund keine dedizierten technischen Vorgaben wie die Verwendung eines TPM-2.0-Moduls oder zur „physischen Nähe" zwischen einzelnen Funktionseinheiten machen. Im Falle der Signatur und der zugehörigen Infrastruktur war damit schon keine weitere Ebene der Rechtssetzung (wie hier die BSI-Vorgaben) notwendig; wie genau der einzelne Anbieter im Rahmen von Auditierungen die Einhaltung der abstrakten Vorgaben etwa der eIDAS-VO nachweist, ist seine Sache. Ebenso hätte der Gesetzgeber vorgeben können, dass die einzelnen funktionalen Komponenten, über die der Datenfluss abgewickelt wird, jeweils durch „sichere Übermittlungswege nach dem Stand der Technik" verbunden werden dürfen – oder eben auch nicht, wenn das (aus welchen gesetzgeberischen Motiven heraus auch immer) nicht gewollt gewesen wäre. Auf diese Weise hätten sich spätere Ungleichbehandlungen bei feingranularer technischer Ausgestaltung nicht mehr ergeben können.

Ergänzend ist darauf hinzuweisen, dass sowohl der EU- als auch der deutsche Gesetzgeber zunehmend dazu übergehen, von den Rechtsadressaten „risikoangemessene Maßnahmen" zu fordern. Prominentes Beispiel ist Art. 32 DSGVO, aber auch Art. 19 Abs. 1 eIDAS-VO und auf nationaler Ebene § 91 AktG oder § 25a Abs. 1 S. 3 KWG. Stets geht es darum, dass (Sicherungs-)Maßnahmen mit dem (vom Normadressaten zu bewertenden) Maß des individuell zu steuernden Risikos korrespondieren müssen. Pauschale Vorgaben, insbesondere auf granularer technischer Ebene, werden der anzustrebenden Einzelfallgerechtigkeit nicht gerecht und erübrigen sich damit. Das ist für die Rechtsadressaten eine große Herausforderung, weil sie eigenständig die individuell bestehenden Risiken identifizieren und bewerten müssen, um dann eine adäquate Risikosteuerung betreiben zu können. Ob dies dann auditiert oder zertifiziert wird, ist nur noch eine untergeordnete Folgefrage. Nur dadurch kann aber Technikgesetzgebung verhindern, dass mit einem „one size fits all"-Ansatz (der beispielsweise der DSGVO aufgrund ihrer Vorgabe der Risikoangemessenheit von Maßnahmen häufig zu Unrecht vorgeworfen wird) teils unter- und teils überreguliert wird. Das sollte auch im Kontext von § 146a AO gelten: Die Manipulationsszenarien im Hinblick auf Kassendaten und damit das Risikoprofil sind in einem kleinen Restaurant mit einer altmodischen „Digitalziffern-Kasse" ganz anders zu bewerten als in einem Großkonzern mit tausenden Filialen, komplexer IT-Landschaft, hohem Compliance-Anspruch und seit jeher schriftlich dokumentierten (GoBD-)Prozessen. Im Rahmen von gerichtlichen Auseinandersetzungen über Schätzungen und der von § 158 Abs. 2 Nr. 1 AO geforderten Einzelfallprüfung (s. o.) zeigt sich, dass das individuelle „Risikoprofil" durchaus schon berücksichtigt wird – wenn auch erst im Streitfall, zu dem es viele Steuerpflichtige verständlicherweise erst gar nicht kommen lassen wollen. Übertragen auf § 146a

183 Vgl. BT-Drs. 18/9535, 20: „Das Sicherheitsmodul dient der effizienten und sicheren Aufzeichnung der Geschäftsvorfälle und anderen Vorgänge, z. B. durch kryptographische Operationen oder Applikationen." Dazu auch Stellungnahme des Bundesrates in BT-Drs. 18/9957, 2, wonach die Effektivität des Gesetzes davon abhängt, dass es gelingt, „zeitnah ein auch für die Prüfungspraxis handhabbares Sicherheitssystem zu entwickeln, zu testen und zu implementieren. Das kann aufgrund der allgemein gehaltenen Aussagen im Gesetzentwurf zum heutigen Zeitpunkt nicht sicher beurteilt werden". Das vom BSI entwickelte, auf Quasi-Echtzeit-Signierung beruhende Grundmodell der Fiskalisierung stellt sich nun aber als de-facto-Umsetzung ohne zulässige (vielleicht sogar auch ohne geeignete) Alternative dar.

AO bedeutet dies: Entscheidend ist nicht, ob eine IT-Komponente in „physischer Nähe“ zu einer logisch angrenzenden Komponente platziert wurde, sondern, welche relevanten Manipulationsrisiken nicht ausreichend abgeschirmt wurden mit der Folge einer tatsächlichen unbefugten Datenänderung (retrospektive Betrachtung durch die Finanzgerichte) bzw. mit der Folge einer erhöhten Manipulationsgefahr (prospektive Betrachtung z. B. im Rahmen einer Zertifizierung oder Auditierung).

Es bleibt zu hoffen, dass (auch) der deutsche Steuergesetzgeber, je weiter er die fortschreitende Digitalisierung von steuerrelevanten Daten begleitet, künftig in grundrechtskonformer Weise möglichst präzise Konzepte und Leitplanken vorzeichnet und dabei auch (selbst) definiert, welcher (Sicherheits-)Aufwand vom Rechtsadressaten betrieben werden muss bzw. wie weit ein Eingriff in den „IT-Bestand“ des Rechtsadressaten gehen soll (und warum). Dies erfordert die Erhebung der entscheidungserheblichen Informationen und Risiko- bzw. Szenariobewertungen, eine transparente Abwägung zwischen den Belastungen für die Rechtsanwender und der Sicherung des Steueraufkommens im Rahmen der Lösungsfindung sowie rechtlich eine transparente Abgrenzung von noch angemessener und schon unverhältnismäßiger Risikosteuerung, jeweils unter Beachtung des Gleichbehandlungsgrundsatzes auch und gerade bei technischen Sachverhalten. Und dies wiederum bedingt eine stärkere Durchdringung der technischen Materie durch den Gesetzgeber selbst, denn je digitaler die Lebenswirklichkeit wird, desto mehr muss sich ein Gesetzgeber damit beschäftigen – auch die Gesetzgeber der Landesbauordnungen beschäftigen sich schließlich mit Traufgiebelhöhe, Umwehrungen und Installationsschächten, ohne dies an ein „Bundesamt für Bauvorgaben“ zu delegieren.

Dr. Axel-Michael Wagner, RA, ist Partner der Kanzlei Peters, Schönberger & Partner in München. Er berät Mandanten in den Bereichen Compliance, M&A-Transaktionen, Due Diligence-Prüfungen und Vertragsrecht. Seine Expertise erstreckt sich zudem auf das IT-Recht, den Datenschutz sowie die zivilprozessuale Prozessführung.

Stefan Groß, StB, CISA, ist Partner der Kanzlei Peters, Schönberger & Partner in München. Er berät vornehmlich an der Schnittstelle Steuerrecht und IT sowie rund um das Thema Tax Technologie und KI im Steuerbereich. Er ist Vorstand beim Institut für Digitalisierung im Steuerrecht (IDSt), Mitglied im Fachausschuss IT (FAIT) des IDW, Chefredakteur der REthinking: Tax sowie Initiator von TAXPUNK.de und den Tax Pioneers.

BFH: Anforderung von Unterlagen durch die Finanzbehörde

BFH, Urteil vom 13.8.2024 – IX R 6/23
ECLI:DE:BFH:2024:U.130824.IXR6.23.0
Volltext der Entscheidung: **BB-ONLINE BBL2024-2517-1**
unter www.betriebs-berater.de

AMTLICHE LEITSÄTZE

1. Die Anforderung unter anderem von Mietverträgen durch das Finanzamt (FA) beim Vermieter (Steuerpflichtigen) nach § 97 der Abgabenordnung muss die Vorgaben der Datenschutz-Grundverordnung (DSGVO) beachten.

2. Eine Einwilligung der Mieter in die Weitergabe an das FA ist nicht erforderlich, weil die Verarbeitung nach Art. 6 Abs. 1 Unterabs. 1 Buchst. c DSGVO gerechtfertigt ist.

3. Die Übersendung der Mietverträge an das FA ist als Zweckänderung nach Art. 6 Abs. 4 DSGVO regelmäßig zulässig.

EUV 2016/679 Art. 6 Abs. 1 Unterabs. 1 Buchst. c, Buchst. e, Abs. 4; AO § 29b, § 93, § 97, § 5; GG Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 20 Abs. 3, Art. 101 Abs. 1, Art. 103 Abs. 1; FGO § 96 Abs. 2; BDSG § 42; AEUV Art. 267 Abs. 3

SACHVERHALT

Streitig ist die Rechtmäßigkeit einer Anforderung von Unterlagen durch die Finanzverwaltung.

Mit den Einkommensteuererklärungen für die Jahre 2018 und 2019 legte die Klägerin und Revisionsklägerin (Klägerin) für ihre Einkünfte aus Vermietung und Verpachtung verschiedener Objekte unter anderem Aufstellungen der gesamten Mieteinnahmen, der Abschreibung, der Verwaltungs- und der Instandhaltungsaufwendungen sowie sonstiger Aufwendungen für das jeweilige Objekt vor. Im Rahmen der Bearbeitung der Erklärungen forderte der Beklagte und Revisionsbeklagte (Finanzamt – FA –) mit Schreiben vom 08.06.2021 und Erinnerungsschreiben vom 13.07.2021 für das Objekt … in … Kopien der aktuellen Mietverträge, Nebenkostenabrechnungen sowie Nachweise über geltend gemachte Erhaltungsaufwendungen an. Hierauf legte die Klägerin eine Aufstellung der Brutto- und Nettomieteinnahmen mit geschwärzten Namen der Mieter sowie der Betriebskosten für die verschiedenen Wohnungen und Unterlagen über die Instandhaltungsaufwendungen vor, jedoch nicht die angeforderten Mietverträge und Nebenkostenabrechnungen. Die Offenlegung dieser Unterlagen sei im Hinblick auf die Grundsätze der Datenschutz-Grundverordnung (DSGVO) ohne vorherige Einwilligung der Mieter nicht möglich. Zudem sei das FA zur Unterlagenanforderung nicht berechtigt, da die Mietverträge zur Prüfung der tatsächlichen Einkünfte untauglich seien. Das FA forderte daraufhin mit Schreiben vom 02.09.2021 und Erinnerungsschreiben vom 28.09.2021 unter Hinweis auf die Mitwirkungspflichten der Klägerin nach §§ 90, 93, 97 der Abgabenordnung (AO) nochmals die Mietverträge und gegebenenfalls die Schreiben über Mietänderungen zum Zweck der Prüfung der in der Steuererklärung gemachten Angaben an.

Den hiergegen erhobenen Einspruch wies das FA mit Einspruchsentscheidung vom 28.04.2022 als unbegründet zurück. Ein Steuerpflichtiger sei nach § 90 Abs. 1 AO zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Er komme der Mitwirkungspflicht insbesondere dadurch nach, dass er die für die Besteuerung erheblichen Tatsachen vollständig und wahrheitsgemäß offenlege und die ihm bekannten Beweismittel angebe. Das FA könne nach pflichtgemäßem Ermessen bestimmen, welche Beweismittel im Sinne