Autor: Thomas Hoeren, Stefan Pinelli
Dokumenttyp: Aufsatz
Literaturnachweis: CR 2025, 834-840 juris
Quelle: CR
Verlag Dr. Otto Schmidt, Köln
Fundstelle: CR 2025, 834-840
Normen: DSGVO , NIS-2-Richtlinie , Cyber Resilience Act
Zitiervorschlag: Hoeren/Pinelli, CR 2025, 834-840

Quantencomputing und Recht - Herausforderungen für Datenschutz, Beweisrecht und Produkthaftung

Warum es normative Kriterien für den Umgang mit Unsicherheit zur Stärkung digitaler Rechtsstaatlichkeit braucht

Thomas Hoeren / Stefan Pinelli

Der Übergang in das Zeitalter des Quantencomputings stellt das Informationsrecht vor grundlegende Umbrüche. Die Kombination aus Künstlicher Intelligenz und Quantencomputing verändert die Voraussetzungen von Datenschutz, Beweisrecht und Produkthaftung grundlegend. Der Beitrag untersucht, wie sich bestehende europäische Rechtsakte - von der Datenschutz-Grundverordnung über die NIS-2-Richtlinie bis zum Cyber Resilience Act - auf die neuen technischen Gegebenheiten einstellen müssen, um die Integrität, Rechtssicherheit und Verantwortlichkeit im digitalen Raum zu wahren.

I. Einleitung

[1]

Die Entwicklungen in der Quantenphysik eröffnen nicht nur neue technische Horizonte, sondern konfrontieren das Recht mit bislang unbekannten Herausforderungen. Quantencomputer, Quantenkryptografie und quantenbasierte Kommunikationsnetze galten lange als fernes Zukunftsprojekt; inzwischen jedoch sprechen Wirtschaft und Wissenschaft von einem beschleunigten Übergang in das postklassische Zeitalter der Informationsverarbeitung.[1] Nach dem Quantum Technology Monitor 2025 von *McKinsey* könnte der Weltmarkt für Quantentechnologien bis 2035 ein Volumen von 97 Mrd. US-$ erreichen.[2] Die Kombination aus Künstlicher Intelligenz und Quantencomputing gilt als strategischer Schlüssel für Wettbewerbsfähigkeit und Datensouveränität.[3] Entsprechend wächst der Druck auf den europäischen Rechtsrahmen, kohärent auf diese disruptive Technologie zu reagieren.[4]

[2]

Im Rahmen einer realistischen Einschätzung sollte berücksichtigt werden, dass sich die Prognosen zur zeitlichen Verfügbarkeit kryptografisch relevanter Quantencomputer (CRQC) erheblich unterscheiden. Während das BSI davon ausgeht, dass insbesondere hoch-sensible Verarbeitungen bereits in den 2030er-Jahren mit einer Gefährdung durch Quantencomputer

rechnen sollten[5], halten andere Fachstellen diese Prognose für zu optimistisch.[6] Eine solche Unsicherheit verdeutlicht die Notwendigkeit einer frühzeitigen Migrationsplanung zu post-quantensicheren Verfahren.

II. Datenschutzrechtliche Implikationen

[3]

Die gegenwärtige Verschlüsselungsarchitektur, insbesondere RSA und ECC, beruht auf mathematischen Problemen, deren Lösung für klassische Computer praktisch unmöglich ist.[7] Quantencomputer können diese durch den Shor-Algorithmus[8]in polynomialer[9]Zeit berechnen. Damit verliert die heutige Kryptografie ihre Schutzwirkung - und der Stand der Technik nach Art. 32 DSGVO ist neu zu definieren.[10] Eine Technologie, die in wenigen Jahren angreifbar wird, kann nicht mehr als angemessen gelten. Unternehmen und Behörden trifft daher bereits heute die Pflicht, den Übergang auf post-quantensichere Verfahren zu planen.[11]

1. NIS-2

[4]

Die NIS-2-Richtlinie verpflichtet Betreiber kritischer Infrastrukturen, geeignete technische und organisatorische Maßnahmen umzusetzen. Der Cyber Resilience Act (CRA) weitet diese Pflicht auf Hersteller digitaler Produkte aus. Unzureichende Kryptografie kann künftig als Produktfehler gewertet werden, was die Haftung erheblich ausdehnt. Der Stand der Technik im Sinne der DSGVO ist dynamisch; mit der erwartbaren Quantenüberlegenheit wird sich dieser Maßstab erneut verschieben.

[5]

Hinzu treten datenschutzrechtliche Sekundärpflichten: Wer bekannte Risiken ignoriert und keine Migration zu quantensicheren Verfahren einleitet, könnte im Schadensfall fahrlässig handeln. Bußgelder nach Art. 83 DSGVO und zivilrechtliche Schadensersatzansprüche sind denkbar.

[6]

Die gegenwärtige Public-Key-Kryptografie[12] stützt sich bei RSA auf die Faktorisierung großer Semiprimzahlen und bei elliptischer Kurvenkryptografie (ECC) auf das diskrete Logarithmusproblem auf Kurven. Für klassische Rechner sind beide Problemklassen bei hinreichenden Schlüssellängen praktisch unlösbar; ein ausreichend großer, fehlertoleranter Quantencomputer könnte sie hingegen mit dem Shor-Algorithmus[13] in Polynomialzeit[14]bewältigen. Damit geraten Vertraulichkeit, Authentizität und Integrität in all den Protokollen unter Druck, die heute auf RSA/ECC aufbauen - von TLS-Zertifikaten bis zu elektronischen Signaturen. Rechtlich schlägt sich das im Maßstab des „Stands der Technik“ nach Art. 32 DSGVO nieder: Was in absehbarer Zeit kompromittierbar ist, kann nicht dauerhaft als angemessen gelten. Der Stand der Technik ist dynamisch konzipiert und verlangt die Berücksichtigung

von Risiko, Implementierungskosten und Zweckbindung; mit wachsendem Quantum-Risiko erfordert dieser Maßstab die Beachtung post-quantensichere Verfahren und organisatorische Migrationspfade.

[7]

Zu den zentralen technischen Antworten zählt die Post-Quantum-Kryptografie (PQC).[15] Die ersten verbindlichen US-Standards liegen vor: NIST hat 2024/2025 ML-KEM (ehemals Kyber) als FIPS 203 und ML-DSA (ehemals Dilithium) als FIPS 204 sowie SPHINCS+ als FIPS 205 finalisiert.[16] Diese Verfahren sind so konstruiert, dass sie auch gegen einen Angreifer mit Quantenrechner sicher sein sollen. Für Europa wurde im Juni 2025 zudem eine koordinierte Umstiegs-Roadmap der Kommission vorgelegt, um Mitgliedstaaten und Sektoren auf einen geordneten Wechsel zu PQC vorzubereiten.[17] ENISA flankiert dies mit Lagebildern und Migrationsleitfäden.[18] Für Unternehmen und Behörden folgt daraus keine Option, sondern eine Planungs- und Umsetzungsaufgabe: Kryptoinventare erfassen, Prioritäten setzen (insbesondere bei „Harvest-now-Decrypt-later"-Risiken), hybride Übergänge gestalten und Validierungs- sowie Zertifikatsketten rechtzeitig auf quantenfeste Profile weiterstempeln.

2. Datensicherheit, „Krypto" und Produkthaftung

[8]

Regulatorisch wird der Druck durch Sektor- und Querschnittsrecht erhöht. Die NIS-2-Richtlinie verpflichtet eine große Zahl „wesentlicher" und „wichtiger" Einrichtungen zu risikobasierten technischen und organisatorischen Maßnahmen und verweist dabei ausdrücklich auf Verschlüsselung, Schwachstellenmanagement, Vorfallbehandlung und Lieferkettensicherheit. Spätestens mit dem Eintritt in den Geltungsbereich von NIS-2 ist die Frage, ob und wann auf PQC migriert wird, Teil der Pflicht zum angemessenen Sicherheitsniveau; dokumentierte Migrationspläne und Roadmaps werden damit prüf- und aufsichtsrelevant. Der neue Cyber Resilience Act (CRA) dehnt die Anforderungen auf Hersteller und Inverkehrbringer „digitaler Produkte" aus: Produkte mit digitalen Elementen müssen während ihres gesamten Lebenszyklus grundlegende Cybersicherheitsanforderungen erfüllen; mangelhafte Kryptografie oder fehlende Aktualisierbarkeit können zur Nichtkonformität führen, was Marktüberwachungsmaßnahmen und Sanktionen nach sich zieht. In der Praxis bedeutet das: Unzureichende oder nicht migrierte Kryptografie wird vom Compliance-Problem zum Produktmangel - mit begleitenden Pflichten zu *Secure-by-Design*, Schwachstellenmanagement und Sicherheitsupdates. Unzureichende oder nicht migrierte Kryptografie wird nicht mehr nur als Compliance-Defizit, sondern sowohl unionsrechtlich als auch national-zivilrechtlich als eigenständiger Produkt- bzw. Leistungsmangel qualifiziert. Die Richtlinie (EU) 2024/2853 erweitert den Produktbegriff ausdrücklich auf Software, digitale Fertigungsdateien und eingebettete digitale Komponenten (Art. 4 Abs. 1 lit. a-c) und verlangt die Einhaltung sicherheitsrelevanter Anforderungen, insbesondere durch *Secure-by-Design*-Konzepte (Art. 6 Abs. 1 lit. a, b), ein fortlaufendes Schwachstellen- und Patch-Management (Art. 10 Abs. 1-3) sowie regelmäßige Sicherheitsupdates über den vorgesehenen Lebenszyklus (Art. 10 Abs. 2, 4). Werden bekannte kryptografische Schwächen nicht behoben oder erfolgt keine Migration auf sichere Verfahren, liegt damit typischerweise ein Produktmangel im haftungs- wie im vertragsrechtlichen Sinne vor.

[9]

National wird diese Qualifikation durch das Regime der §§ 327 ff. BGB gespiegelt: Für digitale Produkte begründet die Pflicht zur Bereitstellung von Sicherheits- und Funktionsupdates (§ 327f BGB) eine dauerhafte Aktualisierungsverantwortung des Unternehmers, deren Nichterfüllung einen Mangel i.S.v. § 327e Abs. 2 BGB darstellt. Die fehlende oder verspätete Bereitstellung eines sicherheitsrelevanten Updates - etwa zum Schließen kryptografischer Schwachstellen - führt damit unmittelbar zur Schlechtleistung.

[10]

Im Kaufrecht gilt Entsprechendes: Ein sicherheitsrelevanter Mangel der digitalen Komponenten oder der eingebetteten Software begründet einen Sachmangel nach § 433 Abs. 1 S. 2 BGB i.V.m. § 475b Abs. 2-4 BGB; dies umfasst insbesondere die Abweichung von objektiven Anforderungen, wozu auch der Schutz gegen bekannte Sicherheitsrisiken zählt. Veraltete oder kompromittierte Kryptografie führt damit regelmäßig zum Sachmangel, selbst wenn die Parteien hierzu keine ausdrückliche Beschaffenheitsvereinbarung getroffen haben.

[11]

Für mietrechtliche Konstellationen - etwa bei der langfristigen Überlassung softwarebasierter Systeme oder IoT-Infrastrukturen - greifen darüber hinaus die Gewährleistungsregeln des Mietrechts, die über § 548a BGB ausdrücklich an die Vorgaben der §§ 327 ff. BGB anknüpfen: Auch hier führt ein Defizit bei sicherheitsrelevanten Aktualisierungen oder ein Ausbleiben einer notwendigen Kryptografie-Migration zu einem Mangel der Mietsache.

3. Datensicherheit, Compliance und Art. 32 DSGVO

[12]

Für das Datenschutzrecht hat das unmittelbare Folgen. Art. 32 DSGVO nennt ausdrücklich Verschlüsselung, aber nur „unter Berücksichtigung des Stands der Technik“; dieser ist kein statischer Katalog, sondern ein Zeitindex. Wer heute Systeme mit „kurzen Halbwertszeiten“ der Kryptostärke plant - etwa reine ECC-Termini ohne PQ-Absicherung für langfristig schützenswerte Daten -, muss mindestens eine belastbare Crypto-Agility vorsehen: dokumentierte Roll-over-Konzepte, hybride Signaturen während der Übergangsphase, PQ-fähige Schlüssel- und Zertifikatsinfrastrukturen, LTV-Zeitstempelketten und Verfahren zur validen Nachsignatur. Wo das fehlt und später ein Schaden eintritt, können Aufsichtsbehörden argumentieren, der Verantwortliche habe ein vorhersehbares Risiko ignoriert und gegen Art. 32 verstoßen; Bußgelder nach Art. 83 DSGVO und zivilrechtliche Haftung wegen fahrlässiger Pflichtverletzung sind dann keineswegs fernliegend. Das gilt besonders bei Daten mit langer Schutzdauer (Gesundheit, IP-Geheimnisse, staatliche Schutzgüter), die für „*Harvest-now-Decrypt-later*“ attraktiv sind.

[13]

Aus Governance-Sicht kristallisieren sich vier Arbeitspakete heraus. Erstens die Bestandsaufnahme: Welche Protokolle, Bibliotheken, Zertifikate, Geräte und Lieferketten hängen an RSA/ECC, und wie lange müssen die jeweiligen Daten vertraulich bleiben „Crypto Bill of Materials“ (CBOM)? Zweitens das Zielbild: Festlegung, wo kurz- bis mittelfristig hybride Profile (klassisch + PQC) sinnvoll sind und wo sofort PQ-nativ gearbeitet werden kann. Drittens die Umsetzung: Aufbau PQ-fähiger PKI, Anpassung von TLS/IPsec/QUIC-Termini, Auswahl zertifizierter oder zumindest standardkonformer PQ-Imple-

mentierungen, Härtung von Schlüsselmanagement und Hardware-Roots-of-Trust, sowie LTV-konforme Weiterzeitstempelung signierter Artefakte. Viertens die Recht- und Nachweisseite: Verankerung der Migrationspflichten in internen Richtlinien und externen Verträgen, Abbildung in NIS-2 - und CRA-Compliance, dokumentierte Risikoabwägung nach DSGVO und regelmäßige Wirksamkeitsprüfungen. Diese Schritte sind nicht nur „Best Practice“, sondern spiegeln den sich verdichtenden europäischen Erwartungshorizont wider, wie ihn NIS-2, CRA und die PQC-Roadmap setzen.

[14]

Kurz gesagt: Shor-Algorithmen machen die klassischen Säulen RSA und ECC prinzipiell angreifbar, und damit verschiebt sich der rechtliche Maßstab für „angemessene Sicherheit“. Wer personenbezogene Daten verarbeitet oder kritische Dienste erbringt, muss die Post-Quantum-Migration heute planen und schrittweise umsetzen. Unterbleibt das, drohen nicht nur technische, sondern auch aufsichts- und haftungsrechtliche Folgen - vom DSGVO-Bußgeld über Maßnahmen der NIS-2-Aufsicht bis zu Marktinterventionen nach dem CRA. Eine angemessene Sicherheitsarchitektur im Jahr 2025 ist deshalb eine, die PQC-fähig ist, Crypto-Agility institutionell abgesichert und langfristige Beweis- sowie Vertraulichkeitsanforderungen lückenlos adressiert.

III. Beweisrechtliche Herausforderungen

[15]

Elektronische Signaturen nach der eIDAS-Verordnung gelten derzeit als gleichwertig mit handschriftlichen Unterschriften. Sobald aber der Algorithmus, auf dem sie beruhen, kompromittiert ist, verliert das Zertifikat seine Beweiskraft.[19] Eine rechtssichere Signatur heute kann in wenigen Jahren technisch fälschbar sein. Um die Integrität digitaler Beweise zu wahren, bedarf es einer rechtlichen Verankerung von Crypto-Agility - der Fähigkeit, Signaturverfahren ohne Verlust der Rechtswirkung an neue kryptografische Standards anzupassen.[20]

[16]

Das Beweisrecht (§ 371a ZPO, § 126a BGB) wird dadurch herausgefordert, dass sich die Zuverlässigkeit elektronischer Dokumente zeitlich relativiert. Für Gerichte entsteht die Aufgabe, den technischen Gültigkeitszeitraum digitaler Signaturen zu berücksichtigen. Parallel müssen Beweisverwertungsverbote für quantengestützte Ermittlungsverfahren diskutiert werden, wenn Teilrechenoperationen unzulässig durchgeführt wurden.

[17]

Im Detail: Elektronische Signaturen nach der eIDAS-Verordnung (EU) Nr. 910/2014 - in der seit dem 11.4.2024 geänderten Fassung durch die „eIDAS 2“-Verordnung (EU) 2024/1183 - entfalten, sofern sie qualifiziert sind, die gleiche Rechtswirkung wie handschriftliche Unterschriften. Diese Gleichwertigkeit ist ausdrücklich normiert und bildet die dogmatische Basis für die elektronische Form im Privatrecht (§ 126a BGB) sowie für den Urkundenbeweis im Zivilprozess (§ 371a ZPO). Zugleich aber ist die

Beweiskraft elektronischer Dokumente nicht statisch, sondern technisch kontextabhängig: Die Aussage „gültig unterschrieben“ trägt nur so weit, wie die zugrunde liegenden Algorithmen und Parameter (Signatur- und Hashverfahren, Schlüssellängen, Zertifikats-Policies) als vertrauenswürdig gelten und die Validierungsdaten (Zeitstempel, OCSP/CRL-Nachweise, Zertifikatsketten) nachprüfbar verfügbar sind[21]. Bricht ein Verfahren weg - etwa durch kryptanalytische Fortschritte oder künftig quantenbasierte Angriffe - relativiert sich der Beweiswert. Genau deshalb gehört „Crypto-Agility“, also die rechtlich und organisatorisch verankerte Fähigkeit, Signatur- und Zeitstempelketten ohne Rechtsverlust auf neue Verfahren zu migrieren, ins Herzstück des Beweis- und Vertrauensdiensterechts.

[18]

Rechtlich bedeutet Crypto-Agility zunächst, dass die Form- und Beweiswirkungen entkoppelt werden von einem einzelnen, im Ausstellungszeitpunkt verwendeten Algorithmus. § 126a BGB ersetzt die Schriftform nur dann dauerhaft, wenn ein qualifiziert signiertes elektronisches Dokument vorliegt; ob dessen Signatur auch Jahre später noch „kryptografisch stark“ ist, sagt die Norm nicht. Die Brücke schlägt § 371a ZPO: Die dort statuierte Beweiskraft knüpft an die Authentizität im Signaturzeitpunkt an (qualifizierte eSignatur, qualifiziertes Zertifikat), bleibt aber der freien richterlichen Beweiswürdigung zugänglich, wenn substantiiert bestritten wird - etwa mit dem Einwand, das Verfahren sei kompromittiert oder die Validierungsnachweise seien unvollständig. In der Praxis wird sich daher die Beweisführung zunehmend um den technischen Gültigkeitszeitraum drehen: Gerichte müssen berücksichtigen, wann signiert wurde, welche Algorithmen/Parameter galten und welche Validierungs-Artefakte (insb. qualifizierte Zeitstempel, OCSP-Responses, CRLs) dem Dokument beigefügt oder nachträglich gesichert wurden.

[19]

Technisch ist der Schlüsselfaktor die Langzeitvalidierung (LTV).[22] ETSI-Profile für CAdES, XAdES und PAdES verlangen, dass die zur Prüfung nötigen Nachweise (Zertifikatsketten, Widerrufsinfos) im Dokument mitgeführt und durch qualifizierte Zeitstempel fortlaufend „eingefroren“ werden. So lässt sich beweisen, dass eine Signatur zu einem bestimmten Zeitpunkt gültig war, selbst wenn das zugrunde liegende Verfahren später als unsicher gilt. Für PDFs regelt das ETSI EN 319 142-1 (PAdES LTV) inklusive „Document Time-Stamp“; ergänzend existieren aktuelle Profile zur Integration/Langzeitvalidierung und zu Migrationspfaden. Für CAdES und XAdES normieren EN 319 122-1 bzw. EN 319 132-1 die Baseline- und Langzeit-Level; das Validierungsreporting ist in TS 119 102-2 beschrieben. Zeitstempel-Dienste selbst unterliegen EN 319 421. Diese Standards operationalisieren Crypto-Agility: Nachsignieren, Neuzeitstempeln, Beweisketten verlängern - ohne die ursprüngliche Erklärung zu ändern

[20]

Daraus folgt eine doppelte Compliance-Pflicht: Zum einen müssen qualifizierte Vertrauensdiensteanbieter (QTSP) organisatorisch und prozessual in die Lage versetzt sein, Zertifikate, Zeitstempel und Validierungsdaten über Jahrzehnte beweissicher vorzuhalten und - falls Standardwechsel anstehen - Migrationsprozesse anzustoßen (Signature-und Hash-Agility, Parameter-Erhöhungen, Mehrfach-Hashung). Zum anderen brauchen Dokumenteninhaber klare Policies für Beweiswerterhaltung (regelmäßiges Erneuern von Zeitstempeln; Speichern von OCSP/CRL-Belegen; Einbetten der Validation-Informationen im LTV-Format). Diese Pflichten sind im eIDAS-Ökosystem angelegt (Qualifizierung, Aufsicht, Vertrauenslisten) und werden durch eIDAS 2, NIS 2 und künftige Zertifizierungsschemata weiter erhärtet.

[21]

Crypto-Agility ist zugleich das Brückenkonzept zur Post-Quantum-Ära. Mit der Standardisierung der ersten PQC-Algorithmen (FIPS 203/204/205; Kyber/ML-KEM, Dilithium/ML-DSA, SPHINCS+) ist absehbar, dass Signatur-Workflows schrittweise PQ-fähige Verfahren aufnehmen müssen - sei es durch hybride Signaturen (klassisch + PQC), sei es durch vollständige Migration, sobald Ökosystem und Tools reif sind. ENISA hat wiederholt betont, dass Organisationen dafür Migration-Roadmaps, Inventare kryptografischer Abhängigkeiten und Übergangsszenarien benötigen. Für den Zivilprozess bedeutet das: Ein elektronisches Dokument, das heute korrekt qualifiziert signiert und mit qualifiziertem Zeitstempel versehen wurde, bleibt prozedural beweisfähig, wenn seine Validierungs- und Zeitstempelketten rechtzeitig auf PQ-feste Verfahren „weitergestempelt" werden. Fehlt diese Pflege, kann die Gegenseite mit Hinweis auf die obsolet gewordene Krypto erfolgreich den Anscheinsbeweis erschüttern.

[22]

Zwingend ist aus alldem eine gesetzliche Klarstellung zur Erhaltungs- und Migrationswirkung: Der Rechtsrahmen sollte ausdrücklich festhalten, dass (1) LTV-Erhaltungsmaßnahmen - insbesondere qualifizierte Nach-Zeitstempel im Einklang mit ETSI - die ursprüngliche Form- und Beweiswirkung nicht beeinträchtigen, sondern erhalten; (2) die algorithmische Ersetzung innerhalb qualifizierter Vertrauensdienste (hash/signature roll-over) keinen Neubeginn der Erklärung darstellt, sondern eine prozessuale Sicherungsmaßnahme; (3) Gerichte bei der Beweiswürdigung den technischen Gültigkeitszeitraum berücksichtigen und die Vorlage eines vollständigen Validierungs-Dossiers (Signatur, Zertifikatskette, OCSP/CRL, qualifizierte Zeitstempel-Kette, Validierungsreport) verlangen können. Parallel sollten aufsichtsrechtliche Leitlinien QTSPs zu Crypto-Agility-Plänen verpflichten (z.B. verbindliche Umstiegs-Timelines auf PQC, Mindestfristen für Erhaltungszeitstempel), damit sich die zivilprozessuale Erwartungshaltung mit der eIDAS-Aufsicht verzahnt.

[23]

Besonderer Diskussionsbedarf besteht schließlich bei Beweisverwertungsverboten im Lichte quantengestützter Ermittlungen. Das Strafprozessrecht kennt - anders als das Zivilprozessrecht - eine fein austarierte, am Grundsatz der Verhältnismäßigkeit orientierte Dogmatik zu Verwertungsverboten. Überträgt man diese Linie auf quantengestützte Teilrechenoperationen (etwa das Brechen eines konkret eingesetzten Signaturalgorithmus entgegen rechtlichen Schranken), werden Straf- und Zivilgerichte voraussichtlich entlang bekannter Kriterien entscheiden: Schwere und Art des Verstoßes, Gewicht des verfolgten Delikts, gezielte vs. flächendeckende Maßnahme, Existenz milderer Mittel sowie die Auswirkungen auf das Vertrauenssystem sicherer Kommunikation. Wo Behörden verbotenerweise kryptografische Hürden aushebeln - etwa gegen explizite gesetzliche Zugriffsschranken oder Aufsichtsvorgaben - spricht vieles für ein Verwertungsverbot bzw. für eine strenge Abwägung zu Lasten der Verwertung, zumal eIDAS und Unionsrecht die Integrität qualifizierter Vertrauensdienste positiv schützen. Dasselbe gilt mittelbar im Zivilprozess: Eine Partei, die Beweise unter rechtswidriger Aufhebung kryptografischer Sicherungen beibringt, riskiert deren Zurückweisung oder zumindest eine gewichtige Beweiswürdigungs-Sanktion.

[24]

Praktisch empfiehlt sich daher ein Dreiklang: (i) Governance - Verankerung von Crypto-Agility in Verträgen, Signaturrichtlinien und Aufbewahrungskonzepten (Rollen, Fristen, Verantwortlichkeiten, LTV-Profile).[23] (ii) Technik - konsequente Nutzung qualifizierter Zeitstempel, vollständiges Einbetten aller Validierungsartefakte, periodisches Weiter-Zeitstempeln sowie - sobald verfügbar - hybride oder PQ-native Signaturen; begleitend ein unternehmensweiter Krypto-Inventar- und Migrationsplan. (iii) Prozessrecht - klar dokumentierte Validierung im Streitfall (ETSI-konformer Prüfbericht), dezidierte Darlegung des Gültigkeitsfensters und - wo erforderlich - gerichtsfeste Erläuterung von Migrationsschritten. So bleibt die Integrität digitaler Beweise auch dann gewahrt, wenn sich die Krypto-Werkbank wandelt: Die Rechtswirkung haftet nicht am einzelnen Algorithmus, sondern an einem prüfbaren, fortgeschriebenen Vertrauenspfad.

IV. Produkthaftung und Sicherheitspflichten

[25]

Die Erweiterung der Produkthaftung auf digitale Komponenten durch die Richtlinie (EU) 2024/2853 führt dazu, dass Hersteller künftig auch für unzureichende Verschlüsselung haften können.[24] Nach dem Cyber Resilience Act sind sie verpflichtet, während des gesamten Produktlebenszyklus Sicherheitsupdates bereitzustellen und neue Bedrohungen zu adressieren. Die Quantenüberlegenheit gilt hierbei als vorhersehbares Risiko. Unterbleibt die Anpassung, kann ein Haftungsfall entstehen. Damit entwickelt sich eine dauerhafte Überwachungspflicht der Sicherheit digitaler Systeme.

[26]

Parallel dazu konkretisieren sich die Sorgfaltspflichten aus § 823 Abs. 1 BGB in Verbindung mit der DSGVO und NIS-2: Ein Unternehmen, das sich auf veraltete Kryptografie stützt, könnte zivilrechtlich schadensersatzpflichtig sein. Damit entstehen neue Maßstäbe technischer Zumutbarkeit, deren Konturen erst durch Rechtsprechung entwickelt werden müssen.

[27]

Die Erweiterung der Produkthaftung in Art. 4 Abs. 1 und 2 RL (EU) 2024/2853, die Software, digitale Fertigungsdateien sowie digitale Komponenten ausdrücklich als Produkte erfassen, führt dazu, dass Hersteller künftig auch für unzureichende Verschlüsselung haften können. Die neue Richtlinie dehnt den Produktbegriff ausdrücklich auf Software, digitale Fertigungsdateien und eingebettete Komponenten aus. Damit wird die Sicherheit der Kryptografie zu einem wesentlichen Bestandteil der Produktsicherheit. Ein Produkt gilt als fehlerhaft, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände berechtigterweise erwartet werden kann. Wenn also ein Hersteller bekannte Schwachstellen in der verwendeten Verschlüsselung nicht behebt oder den Übergang auf sichere Verfahren versäumt, kann dies einen Produktmangel darstellen.[25]

[28]

Diese Entwicklung wird durch den Cyber Resilience Act verstärkt, der für alle Produkte mit digitalen Elementen gilt. Hersteller müssen künftig während des gesamten Produktlebenszyklus technische und organisatorische Maßnahmen treffen, um Sicherheitslücken zu schließen, Bedrohungen zu überwachen und rechtzeitig Sicherheitsupdates bereitzustellen. Kryptografische Verfahren sind dabei keine einmalige Entscheidung, sondern ein fortlaufend zu pflegendes Element der Produktsicherheit. Mit Blick auf die absehbare Quantenüberlegenheit wird erwartet, dass Unternehmen rechtzeitig Post-

Quantum-fähige Verfahren oder hybride Übergangsformen einsetzen. Da diese Entwicklung in der Fachwelt allgemein bekannt und von europäischen Institutionen bereits als sicherheitstechnische Herausforderung anerkannt ist, gilt sie als vor

- 838 -

Hoeren/Pinelli, CR 2025, 834-840

- 839 -

hersehbares Risiko. Unterbleibt die Anpassung, kann ein Haftungsfall entstehen, weil der Hersteller seiner Pflicht zur Gefahrenabwehr nicht nachgekommen ist.

[29]

Auf diese Weise entsteht eine neue Form der Dauerhaftigkeit von Sicherheitsverantwortung. Hersteller müssen ihre Produkte kontinuierlich beobachten und reagieren, wenn neue Schwachstellen oder Bedrohungen bekannt werden. Sicherheitsupdates und Migrationsmaßnahmen sind keine freiwillige Leistung mehr, sondern Teil der rechtlich geschuldeten Produktsicherheit. Unterlässt ein Hersteller die Anpassung an den Stand der Technik, verliert das Produkt seine rechtliche Konformität, und es können Rückrufe, Marktüberwachungsmaßnahmen und Schadensersatzforderungen drohen.

[30]

Parallel dazu konkretisieren sich zivilrechtliche Sorgfaltspflichten aus § 823 Abs. 1 BGB in Verbindung mit der Datenschutz-Grundverordnung und der NIS-2-Richtlinie. Unternehmen, die veraltete oder unsichere Kryptografie einsetzen, riskieren den Vorwurf, fahrlässig gehandelt zu haben. Art. 32 DSGVO verlangt ausdrücklich ein dem Risiko angemessenes Sicherheitsniveau unter Berücksichtigung des Stands der Technik. Wird dieser Standard nicht erfüllt und kommt es zu einem Datenverlust oder zu einer Kompromittierung personenbezogener Informationen, kann dies Schadensersatzansprüche der Betroffenen nach sich ziehen. Auch eine aufsichtsrechtliche Ahndung mit Bußgeldern ist möglich.

[31]

Im Zusammenspiel dieser Vorschriften entsteht ein dynamischer Haftungsmaßstab, der sich am fortlaufenden technischen Fortschritt orientiert. Die Grenze der Zumutbarkeit wird künftig durch die Fähigkeit eines Unternehmens bestimmt, Sicherheitslücken zu erkennen, Updates bereitzustellen und auf absehbare technologische Risiken zu reagieren. Die Gerichte werden in den kommenden Jahren zu klären haben, in welchem Umfang Hersteller und Betreiber verpflichtet sind, ihre Kryptografie auf dem neuesten Stand zu halten, und wie weit diese Pflicht reicht, wenn neue Bedrohungen wie die Quantenüberlegenheit die bestehenden Schutzmechanismen entwerten. Damit entwickelt sich eine dauerhafte Überwachungspflicht der Sicherheit digitaler Systeme, die die rechtliche Verantwortung von Herstellern und Betreibern weit über den Zeitpunkt der Markteinführung hinaus ausdehnt.

V. Staatlicher Zugriff und Grundrechtsabwägung

[32]

Die Quantenkryptografie, insbesondere die Quantum Key Distribution (QKD), ermöglicht eine theoretisch unknackbare Kommunikation. Damit wird der staatliche Zugriffsanspruch auf verschlüsselte Daten - der sog. *lawful access* - faktisch ausgeschlossen.[26] Aus Sicht des Datenschutzes und der informationellen Selbstbestimmung (Art. 8 GRCh) ist dies begrüßenswert; für Sicherheitsbehörden jedoch pro-

blematisch. Die Diskussion um ein gesetzliches Entschlüsselungsgebot wird sich verschärfen, sobald QKD-Netze großflächig eingesetzt werden.

[33]

Die Quantenkryptografie, insbesondere die Quantum Key Distribution (QKD), markiert einen grundlegenden Paradigmenwechsel in der Kommunikationssicherheit. Sie ermöglicht die Verteilung kryptografischer Schlüssel auf der Basis physikalischer Prinzipien, nicht nur mathematischer Annahmen. Das bedeutet, dass jeder Versuch, den Schlüsselaustausch abzuhören, nachweisbar ist und den betroffenen Schlüssel sofort unbrauchbar macht. Unter idealen Bedingungen gilt QKD damit als informationstheoretisch sicher - also theoretisch unknackbar. Für den Datenschutz und die informationelle Selbstbestimmung i.S.d. Art. 8 der EU-Grundrechtecharta ist das ein erheblicher Fortschritt. Bürgerinnen und Bürger, Unternehmen und Behörden können ihre Kommunikation so absichern, dass ein unbemerkter Zugriff durch Dritte, auch durch staatliche Stellen, ausgeschlossen ist.

[34]

Gerade dieser Punkt führt jedoch zu einer zunehmenden Spannung zwischen dem Grundrechtsschutz auf der einen und den Ermittlungsinteressen staatlicher Sicherheitsbehörden auf der anderen Seite. Während herkömmliche Verschlüsselungsverfahren - etwa symmetrische oder asymmetrische Kryptosysteme - theoretisch durch Zugriff auf Schlüssel, Backdoors oder zentrale Entschlüsselungspflichten angreifbar bleiben, entzieht sich die QKD jeder Form des nachträglichen Zugriffs. Die Diskussion um einen sog. „*lawful access*“, also das staatlich legitimierte Recht auf Entschlüsselung im Rahmen von Strafverfolgung oder Gefahrenabwehr, stößt angesichts systemweit implementierter starker Kryptografie technisch an klare Grenzen. Zwar spricht vieles dafür, dass generelle Entschlüsselungspflichten oder Eingriffe in Ende-zu-Ende-Mechanismen sicherheits- wie grundrechtlich kaum vertretbar sind. Gleichwohl arbeitet die *Europäische Kommission* - gestützt auf ihre „*Roadmap for lawful and effective access to data for law enforcement*“ vom 24.4.2025 - an alternativen Zugriffskonzepten, die trotz flächendeckender Verschlüsselung eine effektivere Beweismittelgewinnung ermöglichen sollen. Diese Initiativen sind allerdings ambivalent: Sie adressieren reale Ermittlungsprobleme, bewegen sich zugleich aber in einem Spannungsfeld zu den regulatorischen Vorgaben für starke Kryptografie, *Secure-by-Design* und kontinuierliche Sicherheitsupdates. Es sei zumindest darauf hingewiesen, dass die *EU-Kommission* solche Konzepte prüft, zugleich aber offengelassen, ob diese Ansätze technisch tragfähig sind oder gar strukturell in Konflikt mit den Sicherheitsanforderungen der Produktregulierung treten. Ein gesetzliches Entschlüsselungsgebot ließe sich auf QKD schlicht nicht anwenden: Es existiert kein universeller Schlüssel, keine zentrale Kopie und keine Möglichkeit, eine Kommunikationssitzung nachträglich zu entschlüsseln. Jede „Hintertür“ würde das Sicherheitsprinzip selbst zerstören.

[35]

Aus grundrechtlicher Sicht ist das durchaus begrüßenswert. Die durch QKD technisch garantierte Vertraulichkeit verwirklicht unmittelbar den Schutz der Privat- und Kommunikationssphäre und trägt dem unionsrechtlichen Gebot Rechnung, Eingriffe in Art. 7 und 8 GRCh nur in engen, verhältnismäßigen Grenzen zuzulassen. Im Kern übersetzt QKD also den Grundrechtsschutz in eine physikalische Sicherheitsarchitektur. Zugleich stellt diese Entwicklung Sicherheitsbehörden vor ein Dilemma: Je stärker die Verschlüsselung, desto schwieriger werden strafprozessuale Ermittlungen, Terrorismusbekämpfung oder nachrichtendienstliche Tätigkeiten. Schon heute verlagern sich die staatlichen Zugriffsmöglichkeiten zunehmend vom Kommunikationskanal auf die Endgeräte - etwa durch Quel

len-Telekommunikationsüberwachung oder forensische Datenerhebung auf kompromittierten Systemen. Diese Form der „Endpunktstrategie“ dürfte auch im Zeitalter der Quantenkommunikation das hauptsächliche Ermittlungsinstrument bleiben.

[36]

Sobald Quantenkommunikationsnetze auf Basis von QKD, wie sie im Rahmen der europäischen Initiative „EuroQCI“ vorgesehen sind, in der Fläche implementiert werden, wird sich die politische Debatte um ein gesetzliches Entschlüsselungsgebot weiter zuspitzen. QKD-basierte Schlüsselverteilung entzieht sich strukturell jedem nachträglichen Zugriff; selbst hypothetische „*lawful access*“-Mechanismen lassen sich in solchen Architekturen nur schwerlich integrieren. An dieser Stelle erscheint ein Hinweis auf die „*Roadmap for lawful and effective access to data for law enforcement*“ der *EU-Kommission* vom 24.4.2025 angezeigt, da die *EU-Kommission* dort ausdrücklich alternative Zugriffskonzepte prüft, um die zunehmende Verbreitung starker und flächendeckender Verschlüsselung zu adressieren.

[37]

Spannend - und bislang ungelöst - ist, wie diese Roadmap sich zu dem angekündigten „European Quantum Act“ verhalten wird. Dieser soll nach den bisherigen Vorankündigungen die Entwicklung und den Einsatz quantensicherer Kommunikationstechnologien, einschließlich QKD-Infrastrukturen, strategisch fördern. Je stärker der Quantum Act auf unverhandelbare Integrität und Sicherheit kryptografischer Grundinfrastrukturen setzt, desto größer wird der systemische Konflikt mit Initiativen, die einen staatlichen Zugriff auf verschlüsselte Kommunikation ermöglichen sollen. Es wäre daher sinnvoll, im Text darauf hinzuweisen, dass beide Stränge der EU-Politik - Förderung unkompromittierbarer Quantenkommunikation einerseits und Suche nach *lawful-access*-Mechanismen andererseits - potentiell kollidieren und bislang nicht normativ harmonisiert sind.

[38]

Die Konsequenz ist insgesamt eine Verschiebung des Sicherheitsparadigmas: Datenschutz und staatliche Sicherheit müssen nicht länger als Gegensätze gedacht werden, sondern als komplementäre Schutzgüter, deren Ausgleich in der Architektur der Netze, der Endpunktsicherheit und der rechtlichen Kontrollmechanismen liegt. Die europäische Linie „*security through and despite encryption*“ - also Sicherheit durch und trotz Verschlüsselung - bringt diesen Ansatz auf den Punkt. QKD steht dabei nicht für ein Ende der Strafverfolgung, sondern für eine neue Epoche des Grundrechtsschutzes, in der die Unverletzlichkeit digitaler Kommunikation zur technischen Realität wird.

[39]

Der Konflikt zwischen technischer Unentschlüsselbarkeit und staatlicher Überwachungskompetenz verlangt eine Neubestimmung des Verhältnisses von Privatsphäre und Sicherheit. Verfassungsrechtlich stellt sich die Frage, ob der Staat verpflichtet ist, eine Entschlüsselungsmöglichkeit offen zu halten, oder ob Bürger ein Recht auf absolute Vertraulichkeit haben. Das Grundgesetz und die EU-Grundrechtecharta geben darauf bislang keine eindeutige Antwort.

VI. Ausblick

[40]

Das Recht steht vor einem Paradoxon: Quantencomputing kann einerseits eine nie dagewesene Datensicherheit gewährleisten, andererseits die Fundamente der bisherigen Informationsordnung erschüttern. Der europäische Rechtsrahmen reagiert bislang nur punktuell auf diese Entwicklungen. Eine kohärente Regelung - etwa in Form eines European Quantum Act[27]- könnte die Anforderungen an Kryptografie, Signaturen, staatliche Zugriffsrechte und Haftung systematisch zusammenführen. Solange eine solche Regelung fehlt, bleibt das Informationsrecht in einer Übergangsphase, in der technische Gewissheiten zu rechtlichen Unsicherheiten werden.

[41]

Die Verantwortung der Rechtswissenschaft liegt darin, diese Übergangsphase zu begleiten und normative Kriterien für den Umgang mit Unsicherheit zu entwickeln. Nur so kann gewährleistet werden, dass die Quantenrevolution nicht zu einem Kontrollverlust des Rechts führt, sondern zu einer Stärkung der digitalen Rechtsstaatlichkeit in Europa.

Prof. Dr. Thomas Hoeren

Universitätsprofessor und Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Uni Münster (ITM)

Informationsrecht, Urheberrecht, Gewerblicher Rechtsschutz

hoeren@uni-muenster.de

www.uni-muenster.de/jura.itm/hoeren

Stefan Pinelli

Leiter des Bereiches Recht Digital im Konzernrechtswesen der Volkswagen AG

Rechtliche Beratung von nationalen und internationalen Themen und Projekten mit Bezug zu Digitaltechnologien

Fußnoten

1) For a first introduction see *Kaye, P.*, *Laflamme R.*, & *Mosca, M.*, An Introduction to Quantum Computing, Oxford University Press. (2007); and *Michael A. Nielsen* & *Isaac L. Chuang*, Quantum Computation and Quantum Information (2010) Cambridge University Press.

2) https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025?utm.

3) *De Jong, E.*, Own the Unknown: An Anticipatory Approach to Prepare Society for the QuantuAge, Digital Society, Quantum-ELSPI TC, 1, Springer Nature, (2022); *Stephanie Wehner*, *David Elkouss* & *Ronald Hanson*, Quantum Internet: A Vision for the Road Ahead, 362 Science 303 (2018).

4) *Schön, Hans*, Quantencomputing als Herausforderung für Cybersicherheit und Datenschutz, München 2025; *Balarabe*, Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap, European Journal of Risk Regulation, Volume 16, Issue 2, June 2025, 794 ff.

5) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v= 3&utm_.

6) *Beullens, W.*, *D'Anvers, J.-P.*, *Hülsing, A.T.*, *Lange, T.*, *Panny, L.*, *de Saint Guilhem, C.*, & *Smart, N.P.* (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*. ENISA.

7) *Fumy, Walter*, Kryptographie im Wandel, DuD 2017, 1.

8) *P.W. Shor*, „Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994), IEEE 1994, S. 124-134 - Erstbeschreibung des Faktorisierungs- und Diskreten-Logarithmus-Algorithmus.

9) Was heute Milliarden Jahre dauern würde, könnte mit einem ausreichend großen Quantencomputer in Stunden oder Tagen berechnet werden. Gut beschreiben bei https://schneppat.de/shor-algorithmus/?utm.

10)

Paal/*Pauly*, Datenschutz-Grundverordnung - Kommentar, 3. Aufl. 2024, Art. 32 DSGVO; *Braun, Susanne*, Post-Quantum-Kryptografie: Warum benötigen wir PQC und wo bleiben die Standards?, veröffentlicht am 14.5.2025, abrufbar unter: https://www.elektronikpraxis.de/post-quantum-kryptografie-warum-benoetigen-wir-pqc-und-wo-bleiben-die-standards-ad28c015c41db438c2e5657512736f2e3/ (Stand v. 8.1.2026)

11) *Willemsen*, Privacy at a crossroads in the age of AI and quantum, https://www.computerweekly.com/opinion/Privacy-at-a-crossroads-in-the-age-of-AI-and-quantum.

12) *Hao, Feng*/*Yuan, Zhe* (Eds.): Quantum-Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, Springer 2023.

13) Der Shor-Algorithmus ist ein Quantenalgorithmus, der zwei fundamentale kryptografische Härteprobleme - die Faktorisierung großer Zahlen und die Berechnung diskreter Logarithmen - nicht wie klassische Verfahren in exponentieller, sondern in polynomialer Zeit löst. Er nutzt quantenmechanische Überlagerungszustände und die Quanten-Fourier-Transformation, um die Periodenstruktur einer Funktionenfamilie effizient zu bestimmen, was letztlich zur schnellen Berechnung der gesuchten Faktoren oder Logarithmen führt. Damit würde ein hinreichend großer und fehlertoleranter Quantencomputer die mathematische Grundlage von RSA und ECC aufbrechen können, weil ihre Sicherheit gerade darauf beruht, dass diese Probleme für klassische Rechner praktisch unlösbar sind. Siehe dazu *Michael Sipser*, Introduction to the Theory of Computation, 3. Aufl., Cengage 2012, insbesondere Kapitel 7 („Time Complexity“).

14) In der Komplexitätstheorie bedeutet „polynomial“, dass der Rechenaufwand eines Verfahrens nur in einem polynomiellen Verhältnis zur Größe des Eingabeproblems wächst. Das heißt, die Laufzeit steigt etwa proportional zu n, n^2, n^3 oder allgemein n^k, wobei n die Eingabelänge und k eine feste Konstante ist. Solche Algorithmen gelten als effizient, weil der Aufwand auch bei größeren Eingaben beherrschbar bleibt. Demgegenüber stehen exponentielle Verfahren, bei denen die Laufzeit beispielsweise wie 2^n anwächst und damit schon bei moderaten Eingabegrößen praktisch unberechenbar wird. „Polynomial“ beschreibt somit einen Algorithmus, dessen Ressourcenverbrauch moderat skaliert und der im praktischen Sinne als effizient gilt.

15) https://www.mpg.de/22498867/post-quanten-kryptografie-standards?

16) https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

17) https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

18) https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf?

19) *Müller-Quade, Jörn* (Hauptautor der Wissenschaftlichen Arbeitsgruppe Nationaler Cyber-Sicherheitsrat), Quantencomputer und ihr Einfluss auf die Cybersicherheit, März 2024, abrufbar unter: https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2024-03-impulspapier-quanten-cybersicherheit.pdf (Stand v. 8.1.2026). *Mitglieder der Wissenschaftlichen Arbeitsgruppe Nationaler Cyber-Sicherheitsrat* sind: Thomas Caspers, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner.

20) Schweizer Eidgenössisches Institut für Metrologie (METAS): Quantum Readiness in the Swiss Digital Infrastructure, Bern 2024.

21) Siehe im Detail etwa Https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1_3.pdf?__blob=publicationFile&v=4&.

22) So u,a, https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/1.2.2001_60/en_31912201v010201p.pdf.

23) Hinzuweisen wäre vor allem auf die Ausgestaltung technischer und organisatorischer Maßnahmen in Auftragsverarbeitungsverträgen (Art. 28 Abs. 3 lit. c i.V.m. Art. 32 DSGVO), die Vorgaben für Kryptografie und Schlüsselmanagement in BSI-Grundschutz-Bausteinen (SYS. 1.2, OPS. 1.1.4) sowie auf einschlägige Guidance zur Crypto-Agility (z.B. ENISA, NIST SP 800-57/800-208), die im Rahmen von Governance- und Migrationsstrategien heranzuziehen sind.

24) *Deutsche Industrie- und Handelskammer*, DIHK-Stellungnahme Cyber Resilience Act (CRA), Berlin, 21. Februar 2023, abrufbar unter: https://www.dihk.de/resource/blob/92998/b8f77de58f07d3c8f95bc29f7cff13df/eu-dihk-stellungnahme-cra-data.pdf (Stand v. 8.1.2026)

25) *Borghetti*, Taking EU Product Liability Law Seriously: How Can the Product Liability Directive Effectively Contribute to Consumer Protection? (September 15, 2023). (2023) 1 French Journal of Public Policy, Available at SSRN: https://ssrn.com/abstract=4502351.

26) *Fiessler, Andreas*, Staatliche Regulierung von Kryptografie - ein Überblick, abrufbar unter: https://www.genua.de/fileadmin/Knowledgebase/Article/Insights/Staatliche-Regulierung-von-Kryptografie/staatliche-regulierung-von-kryptografie.pdf (Stand v. 8.1.2026); *Hoffmann-Riem, Wolfgang*, Digitale Disruption und Transformation. Herausforderungen für Recht und Rechts-

wissenschaft, in Eifert, Martin (Hrsg.), Digitale Disruption und Recht - Workshop zu Ehren des 80. Geburtstags von Wolfgang Hoffmann-Riem, Baden-Baden 2020, S. 143-195.

27) Die EU plant einen „European Quantum Act“, dessen Vorschlag 2026 kommen soll. Insgesamt hat die EU-Kommission im Juli die „Quantum Europe Strategy“ vorgeschlagen (COM (2025) 363 final), vgl. hier: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0363. See European Commission, Communication from the Commission, Quantum Europe Strategy: Quantum Europe in a Changing World, COM(2025) 363 final (July 2, 2025). See also European Declaration on Quantum Technologies (Dec. 6, 2023); Eur. Quantum Flagship, Strategic Research and Industry Agenda (SRIA) 2030 (2024); and Eur. Quantum Indus. Consortium (QuIC), Strategic Industry Roadmap (SIR) (2025).