7. Cyberversicherungsrechtstag am 10. Oktober 2025 an der FU Berlin – Rückblick und Ausblick

Am 10. Oktober 2025 fand an der Freien Universität erneut der Cyberversicherungsrechtstag in Zusammenarbeit mit dem Deutschen Verein für Versicherungswissenschaft e.V. (DVfVW) sowie dem Verein zur Förderung der Versicherungswissenschaft in Berlin e.V. statt. Über 100 Teilnehmerinnen und Teilnehmer folgten der Einladung der Organisatoren **Prof. Dr. Christian Armbrüster** (FU Berlin), **Thomas Pache** (BHSI) und **Dr. Dan Schilbach** (Clyde&Co) und nahmen vor Ort im Hörsaal oder online an der Veranstaltung teil.

Bereits am Abend zuvor bot die informelle Vorabendveranstaltung in den Kanzeleiräumen von Wilhelm Rechtsanwälte in Charlottenburg die Möglichkeit, sich mit anderen Teilnehmern auszutauschen. **Petra Ruf** und **Dr. Fabian Herdter** hießen die Gäste willkommen und stellten auch den Berliner Künstler Volker Bartsch vor, dessen Werke in den Räumen der Kanzlei ausgestellt sind.

Der Cyberversicherungsrechtstag am Freitag wurde von Prof. Armbrüster eingeleitet, der aktuelle Cybervorfälle – etwa beim Flughafen BER und bei Jaguar Land Rover – als Beleg für die anhaltende Relevanz der Veranstaltungsreihe anführte. Dies werde die zunehmende Teilnehmerzahl gegenüber den Vorjahren bestätigt.

Im ersten Vortrag widmete sich **Christian Taube** (Beazley Security) den Schadensentwicklungen in der Cyberversicherung. Er knüpfte an seinen Vortrag auf dem 5. Cyberversicherungsrechtstag 2023 an und stellte fest, dass sich viele seiner damaligen Prognosen bestätigt hätten: KI spiele inzwischen eine größere Rolle bei Cyberangriffen und es ließen sich sowohl Lieferketten- als auch Social-Engineering-Angriffe vermehrt beobachten. Der Referent stellte sodann die Kosten eines Ransomware-Angriffs dar und wies darauf hin, dass die Fälle, in denen ein Lösegeld gezahlt wird, rückläufig sind. Er illustrierte die zunehmenden Lieferketten-Angriffe anhand eines aktuellen Beispiels („Shai-Hulud-Wurm"). Abschließend adressierte er auch die Bedeutung von KI im Cyberbereich als „Elefant im Raum": KI könne nicht nur als Werkzeug der Angreifer, sondern auch zur Verteidigung gegen Cyberangriffe eingesetzt werden. Sowohl Versicherer als auch Versicherungsnehmer müssten den Umfang ihrer Cyberdeckung kritisch prüfen und gegebenenfalls an mögliche KI-Schäden anpassen (Nutzung von geistigem Eigentum, Personenschäden, Halluzinationen).

Nach einer ersten Kaffeepause präsentierten **Dominik Schürger** (FU Berlin) und **Thomas Droberg** (Marsh) Cyberrisiken als Kumulrisiken und stellten Überlegungen zu deren Bewältigung an. Droberg leitete den Vortrag mit einer Einführung in das Thema Kumulrisiken ein und wies insbesondere auf die Besonderheiten des globalen „Cyberkumuls" hin. Neben den klassischen gesetzlichen und vertraglichen Instrumenten stünden dem Cyberversicherer insbesondere die Serienschadenklausel als auch die sog. Kumulschadengrenze zur Verfügung, um Kumulrisiken zu bewältigen. Schürger illustrierte dies anhand der Cyber-AVB und verwies auf die in der Schweiz etablierte aufsichtsrechtliche Lösung („Schweizer Kappungsgrenze"). Droberg gab aus der Praktikerperspektive hierzu einen kurzen Marktüberblick und ging dann auf die Problematik „Silent Cyber" ein. Neben der Cyberversicherung könnten demnach auch andere Sparten durch Cyberrisiken betroffen sein, wobei das Deckungsverhältnis hierbei oft unklar sei. Auch hierfür stünden dem Versicherer verschiedene Instrumente im Underwriting oder in der Vertragsgestaltung zur Verfügung, die die Referenten abschließend aufzeigten.

Es folgte der Vortrag von **Dr. Christian Eley** (Aon) zum Verhältnis der Cyberversicherung zur Vertrauensschadensversicherung (VSV). Der Referent stellte zunächst die einer VSV zugrundeliegenden Konstellationen vor: Die vorsätzliche Schädigung des Versicherungsnehmers könne demnach sowohl durch eine Vertrauensperson („Innentäter") als auch durch Dritte erfolgen. Dies wurde anschließend anhand des Urteils des LG Hagen (Urt. v. 15.10.2024 – 9 O 258/23) veranschaulicht, bei dem das Gericht eine Netzwerksicherheitsverletzung bei einem Dritten (Lieferant) nicht als versichert ansah. Der Referent legte dar, dass eine Deckung in der VSV unabhängig von der Netzwerksicherheitsverletzung bestehe, und arbeitete die Unterschiede zwischen den Deckungskonzepten heraus. Zuletzt erörterte er konkrete Deckungssituationen (BU, Wiederherstellung, Lösegeld) und wies auf Probleme bei dem Verhältnis von Cyberversicherung und VSV im Regulierungsverhalten des Versicherers hin.

Nach der Mittagspause erörterte **Dr. Florian Höld** (BLD) die Deckung von Phishing und Pharming in der Cyber- und Hausratversicherung. Er eröffnete seinen Vortrag mit einem kompakten Problemaufriss („Mensch als Schwachstelle") und erläuterte die Begrifflichkeiten. Mangels Legaldefinition bestimme sich die Deckung im Einzelfall nach den individuellen AVB, wie im Folgenden anhand der Urteile des LG Hamburg (Urt. v. 12.12.2024 - 332 O 187/23), LG Berlin II (Urt. v. 27.05.2025 - 24 O 250/24) und LG Hagen (Urt. v. 15.10.2024 – 9 O 258/23) dargelegt wurde. In den ersten beiden Fällen beinhaltete der Hausratsversicherungsvertrag eine Zusatzklausel für „Cyberschutz" bzw. „Zahlungsverkehr im Internet". Die Gerichte legten unter Zugrundelegung der Zahlungsmodalitäten im Sachverhalt die AVB dahingehend aus, dass kein Versicherungsschutz bestehe. In Anknüpfung an den vorherigen Vortrag erörterte der Referent letztlich die Argumente des LG Hagen und würdigte die Entscheidung im Hinblick auf die Wirksamkeit der Klausel positiv.

Hieran schloss **Jan Spittka** (Clyde&Co) seinen Vortrag zum Schadensersatz bei DSGVO-Verstößen an. Nach einem Verweis auf ein aktuelles Urteil des BGH (Urt. v. 18.11.2024 – VI ZR 10/24) zur Schadensbestimmung beim „reinen Kontrollverlust" von Daten stellte der Referent die verschiedenen Modelle individueller und kollektiver Rechtsdurchsetzung von DSGVO-Schadensersatzansprüchen nach einem Cyberangriff in einem Überblick dar. Mangels hoher Streitwerte sei eine Tendenz von Legal-Tech-Kanzleien in Richtung Inkassounternehmen und Prozessfinanzierer bzw. Verbraucherverbände zu erkennen. Bemerkenswert sei hierbei, dass Verbraucher aus anderen Mitgliedstaaten, etwa den Niederlanden, Verbandsklagen vor deutschen Gerichten erheben würden. Der Referent äußerte sich sodann zur (eher beklagtenfreundlichen) Beweislast und zu verschiedenen Schadenspositionen. Er wies in diesem Zusammenhang auf die EuGH-Rechtsprechung zu den Sicherheitsmaßnahmen (TOMs) sowie den neu eingeführten § 273a ZPO (Schutz von Geschäftsgeheimnissen) hin. Sein Vortrag wurde von Auszügen aus vorvertraglichen Anschreiben und Klageschriften begleitet, die die vorgestellten Probleme anschaulich illustrierten.

Abgerundet wurde der Cyberversicherungstag durch den Vortrag von **Daniel Schätzle** und **Prof. Niko Härting** (beide Härting Rechtsanwälte) zu den regulatorischen Hintergründen der Cybersicherheit. Er begann mit einem Überblick über die Rechtsgrundlagen auf nationaler und europäischer Ebene. Im Vordergrund stand dabei die NIS-2-RL, welche derzeit in deutsches Recht umgesetzt werden soll. Schätzle legte dar, dass der Anwendungsbereich sehr weit gefasst sei und die Anwendung im Einzelfall durch unbestimmte Rechtsbegriffe erschwert werde („vernachlässigbare Geschäftstätigkeiten"). Er nannte einige Beispiele und erörterte den im Umsetzungsgesetz vorgesehenen Pflichtenkatalog, der neben Melde- und Informationspflichten auch das Risikomanagement betreffe. Der Referent widmete sich sodann dem Digital

Operational Resilience Act (DORA), der sich an die Finanzwirtschaft und damit auch an Versicherungsunternehmen richte. Auch hierbei stünden umfassende Risikomanagement-pflichten im Mittelpunkt. Insbesondere die Prüfung von IKT-Drittparteienrisiken stelle eine bedeutsame Herausforderung dar. Im Folgenden präsentierte Schätzle einen Überblick über den Cyber Resilience Act (CRA) und hob die Einteilung von Produkten in verschiedene Sicherheitsstufen und hieran anknüpfende Pflichten hervor. Zum Abschluss äußerten sich beide Referenten zu aktuellen Entwicklungen, wie dem Vorschlag einer stärker zentralisierten Datenschutzaufsicht.

Prof. Armbrüster dankte in seinen Schlussworten den Referenten, Teilnehmern und Unterstützern der Veranstaltung. Er wies abschließend darauf hin, dass Themenvorschläge für den nächsten Cyberversicherungsrechtstag, der am 2. Oktober 2026 stattfinden wird, bereits entgegengenommen werden.

Victor Claussen

Wissenschaftliche Mitarbeiter

Lehrstuhl Univ.-Prof. Dr. Christian Armbrüster

Freie Universität Berlin