Digitale Disruption trifft auf Insolvenzrecht

__Hannover.__ Die im August 2024 in Kraft getretene KI-Verordnung sieht fortlaufende Übergangsfristen bis August 2026 vor. Aktuell befinden wir uns in einer Umsetzungsphase, in der Spannungen zwischen den Beteiligten bestehen und gleichzeitig innovative Lösungen erforderlich sind. Zugleich existieren Risiken, welche mit diesem digitalen Wandel einhergehen. Dem Zeitgeist folgend veranstaltete das Institut für Insolvenzrecht e. V. am 23.06.2024 seinen KI- und Cybertag 2025, der sich u. a. mit Cyberrisikostrategien und KI in der Insolvenzverwaltung beschäftigte und viel Stoff für Nachfragen und Diskussionen bot.

Text: *Marian Bolz, Wirtschaftsjurist (LL. M.), M. Sc. (Digital Management & Transformation), Brinkmann & Partner*

Nach der offiziellen Eröffnung durch **RA Prof. Dr. Volker Römermann**, Vorstandsvorsitzender des Instituts für Insolvenzrecht e. V., erwartete die Teilnehmenden eine Reihe fundierter Fachvorträge zu Aspekten einer unternehmerischen Cyberstrategie, Erfahrungen des Verfassungsschutzes zur Täterschaft sowie Cloud und die Integration künstlicher Intelligenz in die juristische Praxis und Unternehmenskommunikation. Den Einstieg bildete ein Vortrag von **Maria Backs** (Head of Customer Success & Account Management (Perseus/HDI)) zum Thema Prävention und Risikobewertung als essenzielle Bausteine einer ganzheitlichen

Maria Backs neben RA Jens Wilhelm V (li.)

Cyberrisikostrategie. Nach einer kurzen Vorstellung des Anbieters von Cybersicherheitslösungen folgte ein Bericht aus der Schadenpraxis und eine Demonstration der drastischen Auswirkungen bei fehlender Cyberrisikostrategie. Die Referentin zeigte auf, dass Cybervorfälle und Betriebsunterbrechungen unter den Top 10 der Geschäftsrisiken 2025 führend sind. Im Anschluss leitete sie aus dem Allianz Risk Barometer 2025 Erkenntnisse ab. Demzufolge stellt ein Cyberangriff das größte Risiko dar. Vor dem Hintergrund der Schadensminimierung sei ein sog. Notfallplan, mithin die Früherkennung eines derartigen Angriffs, weiterhin von sehr großer Bedeutung. Kleinere Unternehmen stünden aufgrund des dortigen Stands der Technik als Angriffsziele im Vordergrund. Vermehrt würden Cyberangriffe als Dienstleistung angeboten. Häufigstes Ziel der Cyberkriminellen seien sensible Daten. Weit verzweigte Lieferketten und Fristendruck stellten Risikofaktoren dar. Daraufhin trug Backs zur aktuellen Cybersicherheitslage vor. Demnach waren acht von zehn Unternehmen im Jahr 2024 von Cyberkriminalität betroffen. Die daraus resultierenden Schäden belaufen sich für das Jahr 2024 auf 267 Mrd. Euro. Rund zwei Drittel der Unternehmen sähen ihre Existenz dadurch gefährdet.

Cyberangriff auf Kanzlei und IT-Dienstleister

Ein realer Cybervorfall in einer Kanzlei diente dazu, das Risikobewusstsein der Teilnehmenden zu stärken. Backs stellte Angriffe und Ziele von Cyberkriminellen dar. Hierunter fallen beispielsweise der Erhalt täuschend echter E-Mails, gefälschte Log-in-Seiten zur Erlangung der Zugangsdaten, Spionage der E-Mail-Kommunikation mit Datenraub und der Versand von Schadsoftware an Mandanten von echtem Kanzlei-Account. Die Folgen sind Daten-, Reputations- und Vertrauensverluste und/oder ggf. meldepflichtige DSGVO-Verstöße. Im Zuge eines Praxistransfers stellte die Referentin den Cyberangriff auf die Infrastruktur des IT-Dienstleisters Convotis (u. a. GeigerCloud, GeigerASP), welcher von Steuerkanzleien für DATEV-Anwendungen verwendet wird, vom 21.11.2023 vor. Es wurde dabei eine Schadsoftware mit Ransom-Note verwendet, jedoch keine konkrete Forderung gestellt. Unmittelbar danach wurden die Systeme vom Netz getrennt und die Datenschutzbehörde wurde über diesen meldepflichtigen Vorfall informiert. In der Folge hatten die Kunden keinen Zugriff mehr auf die Cloud-Dienste. Insbesondere die Lohnbuchhaltung war betroffen. Es waren Notlösungen erforderlich, die Kunden mussten ihre Passwörter ändern. Datenabflüsse seien nicht bekannt geworden. Backs leitete daraus Empfehlungen ab: Neben klar definierten Verantwortungsbereichen zur Kontrolle innerhalb des Unterneh-

Dipl.-Ing. (FH) Jörg Peine-Paulsen und RA Prof. Dr. Volker Römermann (re.)

mens sollte ein Krisenplan für den Fall eines Cyberangriffs konzipiert werden. Ferner sollten IT-Sicherheitsmaßnahmen wie eine Multi-Faktor-Authentifizierung etabliert und regelmäßige Sicherheitsprüfungen durch simulierte Hackerangriffe durchgeführt werden. Daneben sollten die Mitarbeiter durch Fortbildungen zu Phishing und Bedrohungen geschult und es sollte in ausreichendem Umfang eine Cyberversicherung abgeschlossen werden. Ein ganzheitliches proaktives Sicherheitsmanagement sei essenziell zur Schadensminimierung und Resilienz, so die Referentin. Die Cloud sei außerdem nicht von Cyberangriffen verschont, da kein Schutz vor Phishing und menschlichen Fehlern besteht und Cloud-Konten ein bevorzugtes Angriffsziel von Cyberkriminellen darstellten. Backs verwies außerdem auf das Berufsgeheimnis, welches zu einem hohen Schutzniveau verpflichtet, sowie auf die grundsätzliche Verantwortung der Kanzleien. Cloud-Anbieter sicherten sich für den Schadenfall durch Haftungsbegrenzungen (keine Folgeschäden) und vertraglich abgegrenzter Verantwortungen ab. Von den entsprechenden Anbietern bescheinigte Zertifizierungen und hohe Transparenz wiesen lediglich nach, dass pflichtgemäß gehandelt wurde. Im Ergebnis müssten Unternehmen selbst, z. B. mit Cyberversicherungen, Wiederherstellungslösungen, Überwachung/Protokollierung der eigenen Cloud-Systeme, vorsorgen. Zur Verdeutlichung eines ganzheitlichen Ansatzes illustrierte die Vortragende die vier Dimensionen der Cybersicherheit, bestehend aus den Gruppierungen der Risikoverringerung mit den Dimensionen Mensch und Technik sowie der Abschwächung der Auswirkungen mit den Dimensionen Notfall und Restrisiko. Menschliche Fehler gälten als Hauptursache für Cyberangriffe, weshalb Präventionsmaßnahmen mit Aufklärungsmaßnahmen wie beispielsweise Fortbildungen, automatisierte Phishing-Simulationen und Malware-Scan durchgeführt werden sollten. Gleichzeitig stelle die menschliche Firewall das stärkste Schutzschild gegen Cyberrisiken und damit den wichtigsten Erfolgsfaktor dar. Daneben sei im Rahmen der Stärkung des technischen Schutzschilds die eigene Risikobewertung und -evaluation von Relevanz. Bei den Untersuchungen sollte eine ausreichende Objektivität gewahrt werden. Interne und externe Faktoren sowie ein Cybersicherheitsexperte sollten mit einbezogen und es sollten konkrete Empfehlungen zur Verbesserung ausgesprochen werden. Es könne diesbezüglich ein Security Baseline Check als Instrument verwendet werden. Um dem Restrisiko entgegenzuwirken, würden von den Versicherern weitere nachzuweisende Schutzmaßnahmen wie beispielsweise ausreichende Authentifizierungen und Back-ups gefordert. Eine Nachfrage aus dem Publikum, ob Cybervorfälle zu dem elektronischen Anwaltspostfach bekannt sind, verneinte die Referentin.

Im nachfolgenden Vortrag berichtete **Dipl.-Ing. (FH) Jörg Peine-Paulsen**, Niedersächsisches Ministerium für Inneres und Sport, Wirtschaftsschutz, über moderne Gefahrenquellen der IT-Sicherheit: Innentäter, Cloud-Dienste und Passwortmissbrauch. Zunächst definierte der auch den Verfassungsschutz vertretende Referent den Begriff Innentäter und deren Beweggründe. Hier wurden insbesondere die Entfremdung zum Unternehmen, personelle Notlagen und Radikalisierung benannt. Darauf folgend stellte er die Ergebnisse der Studie des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) für das Jahr 2019 vor, dabei handelt es sich um eine Auswertung von 2400 Schadenfällen. Für 63 % der Fälle von Wirtschaftskriminalität waren Innentäter verantwortlich. Diese verursachten 75 % des Gesamtschadens. Jährlich würden 5–10 % der Unternehmen von eigenen Mitarbeitern betrogen. Schließlich erläuterte Peine-Paulsen die Täter-Typen-Risikofaktoren. Demnach sei, resultierend aus überhöhten eigenen Ansprüchen und dadurch selbst legitimierten Taten, die Anspruchsgier (40 %) unter den Kategorien führend. Von dieser Gruppierung würden Gelegenheiten aktiv gesucht. Privater oder beruflicher Krisenauslöser sei die Bedrohung des bisherigen Lebensstils und -status. Als weiteren Typ nannte der Referent die Gelegenheitstäter (25 %), welche als unauffällig beschrieben werden. Diese tendierten zu einem maßvollen, aber regelmäßigen Konsum. Die Gelegenheit diene dabei als Auslöser. Als dritter Typ zählte der Referent die Aktivposten (20 %) auf, welche aktiv die Gelegenheit suchten und schafften. Als Auslöser agiere das ungebremste Leben

Dipl.-Ing. Frank Lembke

RA Jens Decieux

im Augenblick. Als Letztes wurde der Abhängige (15 %) aufgelistet, welcher ebenfalls vorhandene Gelegenheiten ausnutze. Im Allgemeinen sei dieser dem »Haupttäter« hierarchisch untergeordnet bzw. handle aus Verpflichtung oder aus Angst vor negativen Konsequenzen. Eine Kompromittierung sei der Auslöser. Sodann ging Peine-Paulsen auf Low-Level-Agents ein. Er verdeutlichte verschiedene kognitive Verzerrungen wie beispielsweise Bestätigungsfehler (confirmation bias) sowie Dunning-Kruger- und Halo-Effekt. Im Vortrag präsentierte der Referent das Leipziger Verlaufsmodell zur Erklärung wirtschaftskriminellen Handelns. Er empfahl ein ausreichendes Compliance-Management und weitere Maßnahmen wie z. B. Hinweisgebersysteme. Hinsichtlich eines adäquaten Passwortmanagements riet er von Passwortgeneratoren ab. Vielmehr sollten Nutzer im Alltag neben Zwei-Faktor-Authentifizierungen individuelle und sich unterscheidende Passwörter auswählen.

Neue Arbeitswelt mit Chatbots und virtuellen Assistenten

Anschließend gaben **Dipl.-Ing. Frank Lembke** (CPO) und **RA Jens Decieux** (Vice President Strategy & Alliances) von der stp.one einen Überblick über künstliche Intelligenz in der Insolvenzpraxis und auftretende Herausforderungen. Zu Beginn wurde ein Verstoß gegen die Datenschutzvorschriften dahin gehend simuliert (Negativbeispiel), als dass die Referenten ChatGTP durch einen fiktiven Insolvenzverwalter diverse Mietverträge mit persönlichen Daten (Beispiele) zur Prüfung von Change-of-Control-Klauseln zur Verfügung stellten. Sodann zeigten sie anhand einer im Mai 2025 veröffentlichten Umfrage der Bain & Company zur Bereitschaft für generative KI auf, dass der Legal-Tech-Bereich zwar Zuwachs im prototypischen Bereich verzeichnet, jedoch insgesamt bei der Adaption von generativer KI hinter Anwendungsfeldern wie z. B. Kundenservice, Marketing und Personalmanagement zurückliegt. Die Agenda der Vortragenden sah insbesondere die Vorstellung von Einsatzfeldern und Wirkungsweisen von KI im Legal-Tech-Bereich sowie zu bewältigenden Problemfeldern (z. B. Datenschutz) vor und in welchen Bereichen die KI Veränderungen bewirken wird. Zunächst nahmen sie auf die Ursprünge von KI vor der Einführung von ChatGTP Bezug. Erste Anwendungsbereiche waren vor allem die Dokumenten- und Vertragsprüfung. Durch den technologischen Wandel seien in der Folgezeit weitere Einsatzfelder wie Chatbots und virtuelle Assistenten, Vertrags- und Klauselerstellung, Wissensdatenbanken und Zusammenfassungsfunktionen hinzugekommen. Die Referenten gingen in diesem Zusammenhang kurz auf aktuelle Anwendungen wie Libra von Libratech, Beamon AI von Bryter und Beck-Noxtua ein. Hieraufhin wurde die eigens von STP entwickelte KI-Anwendung Legal Twin erläutert und deren Anwendung anhand eines Praxisbeispiels vorgeführt. Ferner werde KI in der prädiktiven Analyse, mithin Mustererkennung von gerichtlichen Entscheidungsfindungen auf Grundlage historischer Falldaten, herangezogen. Exemplarisch prüften die STP-Vertreter im Rahmen des Legal Twin Contract Insights einen Mietvertrag, wobei die KI die involvierten Parteien, das Rechtsgebiet und die Sprache im Zuge des Smart Checks feststellte. Weiterhin könne damit eine Risikoprüfung durchgeführt werden.

Dr.-Ing. Steffen Marx

Mit dem zweiten vorgestellten Bereich, dem Playbook, ließen sich spezifische Geheimhaltungsvereinbarungen erstellen sowie gewerbliche Verträge nach expliziten Vorgaben mit vorgebenen oder individuellen Bausteinen erstellen. Der dritte Bereich bildete die Vertragserstellung bzw. -bibliothek. Dort lassen sich z. B. Due-Diligence-Prüfungen effizient für eine Vielzahl von verschiedenen Vorgängen mit unterschiedlichen Beteiligten automatisiert durchführen. Die Referenten verglichen die entsprechende analoge, zumeist zeitaufwendige Arbeitsweise mit der digitalen Massenprüfung durch KI. Im Anschluss gingen die Vortragenden kurz auf einen weiteren Anwendungsbereich, die KI-Telefonie, ein, wonach KI die Mandantenanrufe automatisch versteht, mittels Intent-Erkennung das passende Routing für den Anrufenden durchführt und eine entsprechende Dokumentation vornimmt.

Anschließend thematisierten sie die Herausforderungen, welche mit der Verwendung von KI einhergehen. Diese umfassen insbesondere zwingend zu beachtende datenschutzrechtliche Anforderungen sowie berufsrechtliche Vorgaben. Insbesondere im Rahmen des KI-Learnings und Finetunings bestehe die Problematik, dass keine personenbezogenen Daten herangezogen werden dürfen. Weiter bestünden Probleme bei der Löschbarkeit dieser Daten und der Erteilung der Auskunftsrechte. Die Referenten erläuterten zusammenfassend die in Kraft getretene KI-Verordnung und stellten anhand eines Zeitstrahls einen Ausblick dar. Aus der Praxis ergäben sich Fragestellungen zur Verantwortlichkeit und Haftung. Als weitere Herausforderung stellten sich die Bias der KI und daraus resultierende (unabsichtliche) Diskriminierungen dar. Es sei unklar, auf welche historischen Daten die KI zurückgreift und wie diese gewichtet werden. Die Entscheidungsprozesse blieben daher intransparent und schwer nachvollziehbar – ein typisches Merkmal sog. Blackbox-Systeme.

Die Regulierung in Europa schütze vor disruptiven Veränderungen (EuGH-Urteil zum Fremdbesitzverbot). Dennoch seien aktuelle Entscheidungen (»Smart Law«-BGH-Urteil) richtungsweisend. Durch die digitalen Assistenzen könnten sich zudem künftig neue Abrechnungsmodelle (Festpreisvergütung und/oder Erfolgsvergütungen oder Abomodelle) etablieren. Abschließend gaben die Referenten eine Zukunftsperspektive. Die künftige Arbeit im Rechtsbereich werde derart ausgestaltet sein, dass der Anwaltsberuf einen Rollenwechsel als Stratege und KI-Versteher erfährt, neue Berufszweige entstehen (z. B. Legal Engineers) und KI fortschreitend in die alltäglichen juristischen Aufgaben integriert wird. Daher sollten bereits im Zuge der Ausbildung und des Studiums entsprechende digitale Inhalte bzw. Grundzüge von Legal Tech vermittelt werden.

Dr.-Ing. Steffen Marx (tagodi GmbH) hielt abschließend einen Vortrag über den Einsatz von künstlicher Intelligenz in der PR-, Marketing- und Medienarbeit und erläuterte, wie sich dabei Potenziale erschließen und mögliche Problemstellungen erfolgreich angehen lassen. Der Referent wies zunächst darauf hin, dass lange vor dem ChatGTP-Hype, nämlich in den 1950er-Jahren, die erste Konferenz zum Thema künstliche Intelligenz abgehalten wurde. Der KI-Markt erfahre nunmehr einen wachsenden Trend um die Vorreiter USA und China. Der Referent ging zu den unterschiedlichen Methoden der KI, mithin unüberwachtes Lernen, überwachtes Lernen, verstärkendes Lernen und tiefgehendes Lernen, über. Insbesondere die letztgenannte Methode komme mit ihren neuronalen Netzen den Menschen am nächsten. Verwendet der Mensch circa 86 Milliarden Parameter bei der Entscheidungsfindung, seien bei dem Modell GPT 5 bereits 3500 Milliarden Parameter vorhanden. Der Vortragende leitete sodann auf die großen Sprachmodelle (Large Language Models (LLMs)) über und darauf, wie diese genutzt werden können. Durch den digitalen Wandel hätten sich neue Berufssparten wie z. B. Big Data Specialist oder Fintech Engineers herausgebildet. Gleichzeitig würden einfache administrative Berufe gänzlich wegfallen. Anhand von Illustrationen zeigte der Referent auf, welchen Fortschritt Image-, Video- und Audiogenerationen in den letzten Jahren gemacht haben. Marx gab nützliche Tipps für den Umgang mit LLMs für neue Nutzer und zeigte mit seinen Vorlagen, wie ein richtiges Prompting – so werden die Aufforderungen in der Eingabemaske der Anwendung genannt – aussieht, um so die gewünschten Antworten auf seine Fragestellungen zu erhalten. Es sei wichtig, unbedingt darauf zu achten, dass die KI nicht halluziniere, da diese das wahrscheinlich nächste Wort berechne und nicht die Wahrheit. Umso wichtiger seien präzise Eingrenzungen als Vorgabe innerhalb der Prompts. Beispielhaft veranschaulichte der Referent den Teilnehmenden umfangreich Promptvorlagen für Aufgaben wie Pressemitteilungen, Rundschreiben oder Protokolle und zeigte Best Practices auf. Auch Präsentationen, Kundenavatare, Customer Journey mit klaren Rollenzuweisungen sowie Marketing-Content für entsprechende Kampagnen stellte er praxisnah vor. Ebenfalls könnten für den Kundensupport entsprechende Anwendungen unterstützend herangezogen werden, weshalb Marx zum Abschluss ein Schaubild einer automatisierten Supportschleife zeigte. «