MMR

Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

4/2026

EDITORIAL

Achtung, Betrugsepidemie!

Lesedauer: 7 Minuten

Die EU-Betrugsbekämpfungsarchitektur hat sich in der Vergangenheit sehr stark auf den Schutz der finanziellen Interessen der EU konzentriert. Der Schutz des Vermögens der in der EU beheimateten Unternehmen und insbesondere der Verbraucher vor betrügerischen Aktivitäten im digitalen Kontext stand weder unter Präventionsaspekten noch in regulatorischer und spezifisch repressiver Hinsicht im Fokus. Maßnahmen hatten eher fragmentarischen Charakter und führten lediglich mittelbar zu einem erhöhten Schutzniveau, zB durch die RL (EU) 2019/71320 betreffend die Bekämpfung von Betrug im bargeldlosen Zahlungsverkehr. Ein ganzheitlicher, systematischer Ansatz mit dem Ziel einer konzentrierten und konzertierten Bekämpfung von Online-Betrug auf breiter Front war bislang nicht erkennbar.

Epidemische Ausmaße

Dies war umso unbefriedigender, als es in internationalen Fachkreisen schon seit längerem einen Gemeinplatz darstellt, dass global eine regelrechte „Scamdemic" um sich greift, dem dringend entschlossen und nachhaltig entgegengewirkt werden muss. Zahlreiche Berichte und Strategiepapiere, zB von Interpol (zuletzt Global Financial Fraud Threat Assessment, Second Edition 2026) und der UNODC (Organized Fraud, Issue Paper 2024), ließen in dieser Hinsicht kaum Raum für Zweifel. Sehr deutlich wurde die besorgniserregende Situation jüngst nochmals beim „Global Fraud Summit" in Wien (vgl. https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf).

Dr. Nino Goldbeck

In der EU deutet sich nun aber ein Umdenken an. Die EU-Kommission hat die – unübersehbaren – Zeichen der Zeit erkannt, das Kind beim Namen benannt („Online-Betrug stellt den am schnellsten wachsenden Bereich der organisierten Kriminalität dar.") und erstmals in der im April 2025 veröffentlichten ProtectEU-Strategie mit Blick auf die gravierenden finanziellen Schäden einen „Aktionsplan zur Bekämpfung von Online-Betrug (einschließlich Telefonbetrug)" angekündigt. Kurz zuvor war in dem von Europol unter dem Titel „The changing DNA of serious and organised crime" veröffentlichten EU-SOCTA Bericht 2025 eine „weit verbreitete Betrugsepidemie" diagnostiziert und konstatiert worden: „Das Ausmaß, die Vielfalt und die Raffinesse der betrügerischen Aktivitäten sind beispiellos und werden durch Fortschritte in den Bereichen Automatisierung und Künstliche Intelligenz vorangetrieben."

Brüssel: Aktionsplan in Vorbereitung

Mitte Januar 2026 hat die EU-Kommission nun Worten erste Taten folgen lassen. Sie hat Details zum angekündigten Aktionsplan bekanntgegeben und ist in die Phase der öffentlichen Konsultation eingetreten, um die inhaltliche Ausarbeitung auf eine möglichst breite Grundlage zu stellen (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16313-Bekampfung-von-Online-Betrug-Aktionsplan_de). Bis Mitte Februar bestand für alle berührten Interessengruppen die Gelegenheit, zu den Erwägungen und geplanten Maßnahmen der Kommission Stellung zu nehmen. Hiervon wurde von Behörden, Verbraucherschutzverbänden, NGOs, dem privaten

Sektor und anderen reichlich Gebrauch gemacht. Die Rückmeldungen deuten darauf hin, dass die Kommission mit ihrem angekündigten Aktionsplan offene Türen einzurennen scheint.

Auch aus der Perspektive der deutschen Strafverfolgung ist die Initiative aus Brüssel nachdrücklich zu begrüßen. Es ist ein wichtiger, richtiger und überfälliger Schritt, der auf europäischer Ebene endlich unternommen wird. Die Bekämpfung von massenhaft begangenem Cyberbetrug – besonders schadensträchtig auch hierzulande: Online-Investmentbetrug – gleicht innerhalb der EU einem Flickenteppich, der dringend gestopft werden muss. Dieser Zustand lässt sich auf zahlreiche system- und phänomenbedingte Ursachen zurückführen; dazu zählt auch, dass es sich bei Cyberbetrug regelmäßig um Massenphänomene mit Bezügen zu Cybercrime, klassischer Betrugskriminalität und „wirtschaftsnaher" Delinquenz sowie starken Überschneidungsbereichen zu transnationaler organisierter Kriminalität (OK) und Geldwäsche handelt. Zu Recht betont die EU-Kommission, dass Professionalisierung und Industrialisierung von Online-Betrug in Bezug auf Umfang, Komplexität, Verbreitung und Auswirkungen immer weiter zunehmen.

Data sharing, PPPs und Asset recovery

Ein sich auch in Detailfragen klar positionierender Aktionsplan dürfte das Potenzial haben, über die mit ihm verbundene Signalwirkung hinaus mittelfristig zu spürbaren Verbesserungen zu führen. Die Schwerpunkte und Zielsetzungen der Initiative (namentlich: 1. Stärkung der grenzüberschreitenden Zusammenarbeit zwischen öffentlichen und privaten Akteuren; 2. Verbesserung der Kriminalprävention, zB durch effiziente Bekämpfung betrügerischer Werbung, aber auch im Bereich Finanztransaktionen; 3. Ausbau des Schutzes und der Unterstützung von Geschädigten; 4. Verbesserung der Rückverfolgung, Sicherstellung und Wiedererlangung betrügerisch erlangter Vermögenswerte) würden sicherlich zu einer stärker integrierten Bekämpfung von Online-Betrug beitragen. Derzeit lassen sich bei Prävention, Repression und Kompensation gleichermaßen – horizontal wie vertikal, national wie international – mannigfaltige und allein den Täterstrukturen nützliche Silo-Effekte beobachten. Für den Bereich der Strafverfolgung kann die Notwendigkeit einer Stärkung der Koordinierung und Kooperation, nicht zuletzt durch den Austausch relevanter Informationen (Stichwort: Global Signal Exchange), und der Ermöglichung niederschwelliger und (datenschutz-)rechtlich nicht angreifbarer transnationaler „Public Privat Partnerships" (PPPs) nicht genug unterstrichen werden. Synergiepotenziale bleiben gegenwärtig viel zu häufig ungenutzt.

Globale Bekämpfungsstrategien

Völlig zu Recht betont die EU-Kommission auch in ihrer Mitteilung, dass die Bekämpfung organisierten Cyberbetrugs nicht an den Grenzen der EU Halt machen darf und es vielmehr einer Intensivierung der internationalen Zusammenarbeit mit solchen Drittstaaten bedarf, die in erheblichem Maße mit Betrugsdelikten in Verbindung stehen. An dieser Stelle muss der Wahrheit ins Auge gesehen werden: Einzelne hochlukrative Betrugsformen lassen sich häufig eindeutig in bestimmten Regionen der Welt eindeutig verorten. Während etwa Love Scams klassischerweise in Westafrika begangen werden, können viele Erscheinungsformen von Online-Investmentbetrug auf Täternetzwerke zurückgeführt werden, die primär aus den Balkan- und Kaukasusstaaten agieren. Andere „moderne" und milliardenschwere Betrugsphänomene wie zB der sog. Pig Butchering Scam werden hingegen aus südostasiatischen Betrugsfabriken kaum vorstellbarer Größe gesteuert (vgl. hierzu nur United States Institute of Peace, Transnational Crime in Southeast Asia, 2024). Wenn die EU und die Mitgliedstaaten hier systematisch und damit losgelöst von Insellösungen etwas erreichen möchten, muss viel Zeit und Energie in den Aufbau effizienter und überdauernder Kooperationsformen investiert – und notfalls auch politischer Druck ausgeübt – werden.

Man kann nur hoffen, dass die EU-Kommission ihr Vorhaben ambitioniert und fokussiert vorantreiben wird. Dies gilt erst recht mit Blick auf die Anstrengungen, die in vielen Staaten bei weitgehend identischen Herausforderungen schon seit längerer Zeit unternommen werden. Vielversprechend erscheint etwa der Ansatz, ein nationales „Anti-Scam Centre" einzurichten, wie es in Anbetracht der identischen Herausforderungen – aber mit divergierenden Aufgaben und Schwerpunkten – zB in Australien, Kanada, Singapur, Thailand und Taiwan geschehen ist (instruktiv PwC UK, Uniting against fraud – How anti-scam centres can strengthen national fraud defences, 2025).

Der Ball liegt in Berlin

Und was geschieht in Deutschland? Hier muss schon die Frage aufgeworfen werden, ob an den maßgeblichen Stellen überhaupt ein Bewusstsein für die epidemischen Ausmaße von Cyberbetrug vorhanden ist. Betrug wird hierzulande noch und nur als individuelles Problem, nämlich allein des Geschädigten, betrachtet. Die sozialschädlichen Auswirkungen auf das Gemeinwesen und vor allem auch die volkswirtschaftliche Relevanz des Abflusses von Milliardenbeträgen aus unserem Wirtschaftskreislauf in die Taschen transnationaler OK-Strukturen scheint von vielen nicht gesehen zu werden. Der kriminal-, rechts- und verbraucherschutzpolitische Diskurs der vergangenen Jahre gibt keinen Grund zur Annahme, das Problem könnte zumindest vereinzelt aus diesem Blickwinkel betrachtet werden. Der Koalitionsvertrag von CDU/CSU und SPD zB schweigt sich hierzu ebenso aus wie zuvor die Wahlprogramme zur Bundestagswahl; es finden sich zwar allgemeine Ausführungen zu Cybersicherheit und Strafverfolgung digitaler Kriminalität, aber keine isolierten und spezifischen Betrachtungen von Cyberbetrug. Überraschen kann das fehlende Bewusstsein allerdings schon deshalb nicht, weil in Deutschland systembedingt ein gravierendes Problem bei der Erfassung der tatsächlichen Situation besteht. Statistisch belastbare, das tatsächliche Fallaufkommen einigermaßen realitätsnah abbildende offizielle Zahlen zu Cyberbetrugstaten liegen nirgends vor.

Umso mehr gilt: Die jüngst erfolgte Zustandsbeschreibung durch die EU-Kommission muss zum Anlass genommen werden, den Status quo der präventiven und repressiven Bekämpfung von Online-Betrug schonungslos zu evaluieren und mehrdimensionale Reformprozesse in die Wege zu leiten. Der aus Brüssel zugespielte Ball muss auf jeden Fall aufgenommen werden – und zwar nicht nur von der Politik, sondern auch von den (Aufsichts-)Behörden (BaFin, BNetzA, BSI, BKA), der Wissenschaft, den Verbänden usw. Es bedarf auch in Deutschland eines Aktionsplans und zuvor der Einrichtung eines Gremiums, das sich aus fachkundigen Vertretern aller betroffenen Akteure des öffentlichen und privaten Sektors zusammensetzt. Eine Expertenkommission könnte die komplexen Fragen multidisziplinär aufbereiten, Optionen für strategische und regulatorische Veränderungen diskutieren und konkrete Lösungsvorschläge unterbreiten. Kumulativ liegt die Beauftragung breit konzipierter Studien nahe. Was am Ende eines solchen Prüfprozesses stehen könnte, zeigt ein Blick in die USA. Dort hat vor einem Jahr das überparteiliche Government Accountability Office einen umfangreichen Bericht vorgelegt und – sehr konkrete – „Recommendations for Executive Action" herausgearbeitet. Das Gleiche gilt für eine vom Aspen Institute vorgenommene Analyse („United We Stand: A National Strategy to Prevent Scams"). Viele der Ideen, Anregungen und Forderungen könnten Orientierung geben für die hoffentlich auch in Deutschland bevorstehende Diskussion.

Entscheidend sind natürlich der politische Wille und die Prioritätensetzung. Dies zeigt der kürzlich von der Bundesregierung verabschiedete „Aktionsplan gegen Organisierte Kriminalität". Die ressortübergreifende Zusammenarbeit von Innen-, Finanz- und Justizministerium stimmt positiv und unterstreicht die Bedeutung der ambitionierten Initiative, die partiell als Vorlage für einen (nationalen) „Aktionsplan gegen Cyberbetrug" dienen könnte. Es lassen sich auch angekündigte Maßnahmen identifizieren, die für die Bekämpfung von Online-Betrug ebenfalls von großer Bedeutung sind (zB Schaffung eines gemeinsamen „Finpool" im Datenhaus P20 zur frühzeitigen Erkennung, Auswertung und Verfolgung illegaler Finanzflüsse). Auf der anderen Seite ist die angekündigte „Zeitenwende der Inneren Sicherheit" so breit konzipiert (OK, Finanz- und Rauschgiftkriminalität), dass eine spezifische Adressierung von Kernproblemen und das Herausarbeiten maßgeschneiderter Lösungen unrealistisch erscheint. Die angekündigte Einrichtung von gemeinsamen Kompetenz-, Ermittlungs- und Analysezentren lässt aber hoffen, dass bei einer Neuausrichtung der Bekämpfung von Online-Betrug auch der Aufbau eines deutschen „Anti-Scam Centers" nicht per se ausgeschlossen ist.

Bamberg, im April 2026

Dr. Nino Goldbeck
ist OStA bei der Zentralstelle Cybercrime Bayern, GStA Bamberg.