ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Zwischen regulatorischem Anspruch und praktischer Umsetzbarkeit: Start-ups im Spannungsfeld von Cyber Resilience Act und AI Act

Erkenntnisse aus einer qualitativen Befragung von Start-ups

Autorin:
Maxine Joanne Folschweiller
Fraunhofer SIT, ATHENE und HNFIZ 7

Impressum

Kontakt
Nationales Forschungszentrum für angewandte
Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

1. Einleitung

In den vergangenen Jahren hat die Europäische Union ihre Haltung gegenüber der Regulierung und Einführung digitaler Technologie deutlich verschärft. Insbesondere unter der ersten Kommission von Ursula von der Leyen wurden zwischen 2019 und 2024 zahlreiche Rechtsakte verabschiedet, die Entwicklung, Einsatz und gesellschaftliche Auswirkungen digitaler Technologien adressieren und vielfach als Ausdruck einer europäischen Regulierungswelle verstanden werden. Diese verstärkten politischen Investitionen sind Teil eines programmatischen Ansatzes, der unter dem Begriff der EU-Digitalpolitik zusammengefasst wird und technologische Innovation, Sicherheit und Grundrechtsschutz miteinander verbinden soll. Vor diesem Hintergrund verfolgt die EU das Ziel, digitale Souveränität zu stärken und ihre Rolle im globalen digitalen Wettbewerb neu zu definieren [Bj25].

Start-ups und jungen Unternehmen kommt dabei eine besondere Bedeutung zu. Als zentrale Träger digitaler Innovation sind sie ein wesentlicher Schlüsselfaktor für technologischen Fortschritt und die Entwicklung neuer Geschäftsmodelle [HP25]. Insbesondere im Technologiebereich – etwa in den Feldern Künstliche Intelligenz, Software, vernetzte Produkte und Cybersicherheit – treiben Tech-Start-ups Innovationen voran und prägen maßgeblich die Dynamik der digitalen Transformation [Bö19].
Diese zentrale Rolle junger Unternehmen für die digitale Transformation steht jedoch in einem Spannungsverhältnis zur Ausgestaltung der europäischen Technologieregulierung. Die einschlägigen Rechtsakte sind weitgehend unternehmensgrößenneutral konzipiert und adressieren Start-ups, KMUs und etablierte Großunternehmen gleichermaßen [HP25]. Demgegenüber stehen junge Unternehmen, die typischerweise durch begrenzte finanzielle und personelle Ressourcen, hohe Unsicherheit, erheblichen Zeitdruck sowie einen starken Investorenfokus auf Wachstum und schnellen Markteintritt gekennzeichnet sind. Daraus ergibt sich eine strukturelle Asymmetrie zwischen regulatorischem Anspruch und der Umsetzungsrealität von jungen Unternehmen.

Vor diesem Hintergrund stellt sich die Frage, wie junge Unternehmen mit den neuen regulatorischen Anforderungen in der Praxis umgehen. Insbesondere ist zu untersuchen, ob die Verordnung über Cyber Resilienz und die KI-Verordnung unter den spezifischen Bedingungen junger Unternehmen innovationsfördernd wirken oder vielmehr zusätzliche Belastungen erzeugen. Von zentralem Interesse ist dabei, inwieweit Gründerteams in der Lage sind, die formalen rechtlichen Anforderungen zu verstehen und in ihre Entwicklungs- und Geschäftsprozesse zu integrieren. Die vorliegende Untersuchung zielt vor diesem Hintergrund darauf ab, Unterschiede zwischen regulatorischem Anspruch und tatsächlicher Umsetzungspraxis aus der Perspektive junger Technologieunternehmen empirisch zu beleuchten.

2. Forschungsmethode

Die Untersuchung folgt einem qualitativen, explorativen Forschungsdesign und zielt darauf ab, Wahrnehmungen und Herausforderungen von Gründerteams im Zusammenhang mit der Umsetzung der Verordnung über Cyber Resilienz (CRA) und der KI-Verordnung (KI-VO) zu erfassen. Angesichts der Neuartigkeit beider Rechtsakte und des bislang begrenzten empirischen Erkenntnisstands wurde ein qualitatives Vorgehen gewählt.

Die Datenerhebung erfolgte im Zeitraum vom 16. Oktober 2025 bis zum 2. Dezember 2025 in Form von Experten-Workshops. Befragt wurden sieben Gründer, aufgeteilt auf drei Gründerteams, jeweils in einem teamweisen Experten-Workshop. Die Interviews fanden als Videokonferenzen über Microsoft Teams statt. Die Teilnehmenden verfügten über unmittelbare Erfahrung mit der Entwicklung digitaler Produkte bzw. KI-basierter Anwendungen. Grundlage der Erhebung war ein teilstrukturierter Fragenkatalog zu Bekanntheit, Relevanz und wahrgenommenen Herausforderungen im Zusammenhang mit CRA und KI-VO. Der Fragenkatalog wurde vorab mit drei potenziellen Workshopteilnehmenden (zwei am 26.09.2025, eine am 29.09.2025) hinsichtlich Verständlichkeit und Eindeutigkeit validiert und anschließend angepasst. Der Fragenkatalog wurde in deutscher Sprache abgefasst, alle Experten-Workshops wurden in deutscher Sprache durchgeführt.

Die Auswertung erfolgte qualitativ anhand einer thematischen Strukturierung der Aussagen entlang der zentralen Themenfelder. Ziel war die Identifikation wiederkehrender Muster und Spannungsfelder. Die Aussagekraft der Untersuchung ist insbesondere durch die Anzahl der Befragten (bzw. durchgeführten Experten-Workshops) sowie die Beschränkung auf den deutschsprachigen Kontext begrenzt. Zudem basiert die Analyse auf Selbstauskünften der Teilnehmenden und stellt eine Momentaufnahme in einer frühen Phase der regulatorischen Implementierung dar.

3. Erkenntnisse zum CRA

Der CRA ist am 10. Dezember 2024 in Kraft getreten und stellt einen zentralen Baustein der europäischen Cybersicherheitsregulierung dar [HP25]. Ziel der Verordnung ist es, ein höheres Cybersicherheitsniveau im digitalen Binnenmarkt zu gewährleisten, indem insbesondere die bislang häufig unzureichende Sicherheit vernetzter Produkte adressiert wird. Angesichts der hohen Komplexität moderner Soft- und Hardware und der damit einhergehenden erheblichen Angriffsflächen für Cyberangriffe sollen durch den CRA strukturelle Schwachstellen reduziert und Verbraucher wie auch gewerbliche Nutzer besser geschützt werden [HP25]. Zu diesem Zweck setzt der CRA auf einen zweistufigen Regulierungsansatz: Einerseits sollen durch grundlegende Cybersicherheitsanforderungen die Anzahl von Schwachstellen in Produkten mit digitalen Elementen gesenkt werden; andererseits sollen Nutzer mit hinreichenden Informationen ausgestattet werden, um Cybersicherheitsaspekte bei Marktentscheidungen angemessen berücksichtigen und Produkte sicher betreiben zu können [HP25]. Der CRA reagiert damit auf zwei zentrale Problemlagen, nämlich das strukturell niedrige Cybersicherheitsniveau vieler digitaler Produkte sowie die unzureichende Informationslage der Nutzer [HP25]. Im Gefüge des europäischen Cybersicherheitsrechts verfolgt der CRA das übergeordnete Ziel, ein hohes gemeinsames IT-Sicherheitsniveau innerhalb der Europäischen Union zu schaffen [HP25].

3.1 Begrenzte Bekanntheit bei gleichzeitig hoher wahrgenommener Umsetzungsintensität

Der sachliche Anwendungsbereich des CRA ist nach Art. 2 Abs. 1 S. 1 CRA weit gefasst und erfasst grundsätzlich alle auf dem Unionsmarkt bereitgestellten Produkte mit digitalen Elementen. Er umfasst sowohl Hardware als auch Software, einschließlich eingebetteter Software, eigenständig bereitgestellter Stand-Alone-Software sowie autonomer Software- und Hardwarekomponenten, sofern diese gesondert in Verkehr gebracht werden [HP25]. Hintergrund dieser weiten Begriffsbestimmung ist das regulatorische Ziel, ein möglichst hohes Cybersicherheitsniveau in der Europäischen Union zu erreichen, indem nicht nur einzelne Produktkategorien, sondern ein breites Spektrum digitaler Produkte – insbesondere auch Software – in den Anwendungsbereich einbezogen wird [HP25]. Der CRA richtet sich in persönlicher Hinsicht zudem an verschiedenen Wirtschaftsakteure entlang der Wertschöpfungskette und verpflichtet insbesondere Hersteller, Einführer und Händler, sicherheitsrelevante Anforderungen über den gesamten Produktlebenszyklus hinweg zu beachten, etwa im Hinblick auf Schwachstellenmanagement und Sicherheitsvorfallmeldungen.

Die Erhebung zeigt eine heterogene Bekanntheit des CRA unter den befragten Gründerteams. Während zwei Gründerteams – darunter auch ein im Bereich Cybersicherheit tätiges Unternehmen – mit dem CRA und seinen Zielsetzungen vertraut waren, verfügte ein Gründerteam über keine Kenntnis des Rechtsakts. Innerhalb der Gruppe der informierten Gründerteams zeigten sich zudem Unterschiede im Grad der inhaltlichen Vertrautheit: Während beide die übergeordnete Zielsetzung des CRA, die Stärkung der Cybersicherheit im EU-Binnenmarkt, benennen konnten, war das im Bereich Cybersicherheit tätige Gründerteams darüber hinaus in der Lage, spezifischere Zielsetzungen und Regelungsinhalte des CRA zu konkretisieren. Unabhängig vom individuellen Kenntnisstand gingen jedoch alle drei Gründerteams[1] davon aus, dass der CRA für ihr Unternehmen bzw. ihr Projekt relevant ist oder künftig eine Rolle spielen wird, entweder aufgrund der Entwicklung von Produkten mit digitalen Elementen oder aufgrund der inhaltlichen Relevanz des CRA für ihre Dienstleistungen. Die Auswertung der Experten-Workshops zeigt, dass die mit dem CRA vertrauten Gründerteams den Rechtsakt als regulatorisch anspruchsvoll und operativ tief eingreifend wahrnehmen. Insbesondere die Unklarheit konkreter Anforderungen, die Vielzahl technischer Pflichten sowie der erwartete Ressourcenaufwand prägen ihre Einschätzung des CRA als erhebliche Umsetzungsherausforderung für junge Unternehmen. Darüber hinaus wird die hohe fachliche Komplexität des Themenfeldes Cybersicherheit sowie der Mangel an entsprechender Expertise – auch vor dem Hintergrund eines begrenzten Angebots an qualifizierten Fachkräften – als zentrale Herausforderung hervorgehoben. Das Gründerteam ohne Kenntnis des CRA konnte demgegenüber keine CRA-spezifischen Herausforderungen benennen und ordnete bestehende Schwierigkeiten ausschließlich der allgemeinen Gewährleistung von Cybersicherheit zu.

Zusammenfassend zeugt die Auswertung der Experten-Workshops, dass der CRA von jungen Unternehmen frühzeitig als relevanter regulatorischer Rahmen antizipiert wird, unabhängig vom jeweiligen Kenntnisstand. Auch ein Gründerteam ohne konkrete Vertrautheit mit dem CRA geht davon aus, dass der Rechtsakt für ihr Unternehmen oder Projekt künftig eine Rolle spielen wird. Die wahrgenommene Relevanz des CRA ist damit nicht zwingend an detaillierte Kenntnisse einzelner Regelungsinhalte gebunden, sondern Ausdruck einer allgemeinen Erwartung zunehmender Regulierung im Bereich digitaler Produkte und Cybersicherheit. CRA-spezifische Herausforderungen werden jedoch ausschließlich von denjenigen Gründerteams benannt, die mit dem Rechtsakt vertraut

[1] Nach einer kurzen Belehrung des Gründerteams ohne Vorkenntnisse zum CRA über dessen Ziele.

sind. Fehlende Kenntnis geht daher nicht mit fehlender Betroffenheit einher, sondern mit fehlender Zuschreibung bestehender Schwierigkeiten zur Regulierung. Dort, wo eine Auseinandersetzung mit dem CRA stattfindet, wird dieser vor allem als umsetzungsintensiv und komplex wahrgenommen. Die Belastungswahrnehmung resultiert dabei weniger aus einzelnen Pflichten als aus der Unsicherheit hinsichtlich der praktischen Umsetzung, der Vielzahl technischer Anforderungen und des damit verbundenen Ressourcenaufwands.

3.2 CRA-Pflichten im Spannungsverhältnis zu agilen Entwicklungsprozessen

Der CRA begründet umfassende Pflichten für Wirtschaftsakteure entlang der Wertschöpfungskette von Produkten mit digitalen Elementen [Wi25]. Für Gründerteams und junge Unternehmen ist dabei besonders relevant, dass sie als Hersteller im Sinne des CRA gelten können und damit die primäre Verantwortung für die Cybersicherheit ihrer Produkte tragen können. Unter den Begriff des Herstellers fällt jede natürliche oder juristische Person, die ein Produkt mit digitalen Elementen selbst entwickelt, herstellen lässt und unter eigenem Namen oder Marke vermarktet (Art. 3 Nr. 13 CRA).

Als Hersteller sind junge Unternehmen nach Art. 13 Abs. 1 CRA verpflichtet, Produkte von Beginn an sicher zu konzipieren und zu entwickeln (Security by Design) [Wi25], ein wirksames Schwachstellenmanagement zu etablieren (Art. 13 Abs. 8 CRA) sowie während des gesamten Produktlebenszyklus Sicherheitsupdates bereitzustellen. Darüber hinaus ist vor dem Inverkehrbringen eine Konformitätsbewertung durchzuführen und eine CE-Kennzeichnung anzubringen, die die Einhaltung der CRA-Anforderungen bestätigt (Art. 13 Abs. 12 CRA). Auch Melde- und Informationspflichten im Zusammenhang mit Sicherheitsvorfällen gehören zu den fortlaufenden Verpflichtungen (Art. 14, 31 CRA). Der CRA verfolgt einen risikobasierten Ansatz: Je höher das von einem Produkt ausgehende Cybersicherheitsrisiko bzw. je höher die möglichen Folgen, desto strenger sind die regulatorischen Anforderungen.

Für junge Unternehmen bedeutet dies, dass Cybersicherheit nicht mehr nachgelagert adressiert werden kann, sondern als dauerhafte organisatorische und prozessuale Aufgabe in Produktentwicklung und Betrieb integriert werden muss. Die unternehmensgrößenneutrale Ausgestaltung der Pflichten führt dazu, dass diese Anforderungen unabhängig von Teamgröße oder Ressourcenausstattung gleichermaßen gelten.

Die Auswertung der Experten-Workshops zeigt, dass zwei von drei befragten Gründerteams zentrale Pflichten des CRA als schwer vereinbar mit gründungstypischen, agilen Entwicklungsprozessen wahrnehmen. Insbesondere Anforderungen an Security by Design, die fortlaufende technische Dokumentation, das systematische Schwachstellenmanagement sowie perspektivisch die Durchführung von Konformitätsbewertungen wurden von diesen Gründerteams als Faktoren benannt, die mit kurzen Release-Zyklen, iterativem Arbeiten und experimenteller Produktentwicklung in Spannung stehen. Beide Gründerteams führten aus, dass die Erfüllung dieser Pflichten mit einem erheblichen zusätzlichen Zeit- und Ressourcenaufwand verbunden sei, der die Geschwindigkeit von Entwicklungs- und Innovationsprozessen spürbar verlangsamen könne. Hervorgehoben wurden dabei insbesondere begrenzte personelle Kapazitäten sowie fehlende spezialisierte Expertise im Bereich Cybersicherheit. Ein Gründerteam äußerte demgegenüber keine CRA-spezifischen Spannungen zwischen regulatorischen Anforderungen und Entwicklungsprozessen, was jedoch darauf zurückzuführen war, dass dieses Team nicht mit dem CRA vertraut war und bestehende Herausforderungen

ausschließlich der allgemeinen Gewährleistung von Cybersicherheit zuschrieb. Insgesamt deuten die Aussagen der CRA-kundigen Gründerteams darauf hin, dass der CRA weniger als punktuelle rechtliche Verpflichtung, sondern vielmehr als prozessualer Eingriff in bestehende Entwicklungspraktiken wahrgenommen wird. Die unternehmensgrößenneutrale Ausgestaltung der Pflichten wird dabei von einzelnen Befragten explizit als problematisch bewertet, da deren Umsetzung aus ihrer Sicht Skaleneffekte voraussetzt, über die junge Unternehmen regelmäßig nicht verfügen.

4. Erkenntnisse zur KI-VO

Mit der am 1. August 2024 in Kraft getretenen KI-VO hat die Europäische Union erstmals einen umfassenden und unionsweit einheitlichen Rechtsrahmen zur Regulierung von KI geschaffen. Die KI-VO verfolgt das übergeordnete Ziel, die Entwicklung und Nutzung von KI-Systemen in der EU so zu steuern, dass technologische Innovation, wirtschaftliche Wettbewerbsfähigkeit und der Schutz gesellschaftlicher Grundwerte miteinander in Einklang gebracht werden (Erwgr. 1 KI-VO). Im Zentrum steht dabei das Bestreben, Vertrauen in KI-Technologien zu stärken und Risiken für Sicherheit, Grundrechte und demokratische Prozesse frühzeitig zu adressieren [Vo25]. Zugleich soll ein klarer und vorhersehbarer Ordnungsrahmen geschaffen werden, der verantwortungsvolle Innovation ermöglicht und die Position der EU im globalen digitalen Wettbewerb stärkt.

4.1 Hohe Bekanntheit, geringe unmittelbare Betroffenheit

Der Anwendungsbereich der KI-VO ist besonders weit gefasst. Nach Art. 2 KI-VO gilt sie grundsätzlich für alle KI-Systeme, die innerhalb der EU in Verkehr gebracht, bereitgestellt oder verwendet werden. Der Begriff des KI-Systems wird in Art. 3 Nr. 1 KI-VO technologieoffen definiert und erfasst maschinengestützte Systeme, die mit einem gewissen Grad an Autonomie arbeiten und darauf ausgelegt sind, für explizite oder implizite Ziele Ergebnisse wie Vorhersagen, Empfehlungen, Inhalte oder Entscheidungen zu erzeugen, die physische oder virtuelle Umgebungen beeinflussen können. In persönlicher Hinsicht erstreckt sich der Anwendungsbereich der KI-VO auf eine Vielzahl von Akteuren entlang der gesamten Wertschöpfungskette von KI-Systemen. Erfasst werden insbesondere Anbieter, Betreiber, Händler, Einführer sowie Produkthersteller, sofern sie KI-Systeme entwickeln, in Verkehr bringen oder innerhalb der EU einsetzten (Art. 2 KI-VO).

Zugleich verfolgt die KI-VO einen risikobasierten Regulierungsansatz (Erwgr. 26 KI-VO): Je höher das potenzielle Risiko eines KI-Systems für Menschen, Gesellschaft oder Grundrechte, desto strenger sind die rechtlichen Anforderungen. Die Verordnung unterscheidet dabei zwischen vier Risikoklassen: KI-Systeme mit unannehmbarem Risiko (verbotene Praktiken), mit hohem Risiko, mit begrenztem Risiko sowie mit minimalem oder keinem Risiko. Während KI-Systeme mit unannehmbarem Risiko grundsätzlich verboten sind, konzentriert sich die Regelungsdichte der KI-VO vorrangig auf Hochrisiko-KI-Systeme; KI-Systeme der übrigen Risikoklassen unterliegen demgegenüber deutlich geringeren oder garkeinen Anforderungen.

Die Auswertung der Experten-Workshops zeigt, dass die KI-VO unter den befragten Gründerteams eine hohe Bekanntheit aufweist. Alle drei Gründerteams gaben an, die KI-VO zu kennen und sich zumindest auf einer allgemeinen Ebene mit deren Zielsetzung und

Grundstruktur auseinandergesetzt zu haben. Insbesondere der risikobasierte Ansatz der VO wurde von mehreren Befragten explizit benannt und als prägendes Element der Regulierung wahrgenommen. Gleichzeitig äußerten zwei der drei Gründerteams, dass sie sich derzeit nicht unmittelbar von den Pflichten der KI-VO betroffen sehen. Diese Einschätzung wurde jeweils damit begründet, dass die entwickelten oder geplanten KI-Anwendungen nach eigener Einschätzung nicht in den Bereich der Hochrisiko-KI-Systeme fallen. Vor diesem Hintergrund wurden die mit der KI-VO verbundenen rechtlichen Anforderungen nicht als unmittelbar handlungsleitend für den operativen Betrieb wahrgenommen. Die Auswertung macht damit deutlich, dass die wahrgenommene Betroffenheit durch die KI-VO weniger von deren grundsätzlicher Bekanntheit abhängt, sondern maßgeblich von der Selbsteinordnung der eigenen KI-Anwendung innerhalb der Risikoklassifizierung der Verordnung bestimmt wird. Solange die eigenen Systeme nicht dem Hochrisikobereich zugeordnet werden, wird die KI-VO von den befragten Gründerteams nicht als praktisch relevant eingeordnet.

4.2 Punktuelle Unsicherheit im Umgang mit unbestimmten Rechtsbegriffen

In den Experten-Workshops wurde vereinzelt auf Unsicherheiten im Zusammenhang mit unbestimmten Rechtsbegriffen der KI-VO hingewiesen. Konkret thematisierten zwei Gründerteams einzelne Regelungsbereiche, die aus ihrer Sicht eine erhöhte Auslegungsbedürftigkeit aufweisen. Die angesprochenen Unsicherheiten bezogen sich insbesondere auf abstrakt formulierte Anforderungen, etwa im Zusammenhang mit der Einordnung von KI-Systemen, der Abgrenzung technischer und rechtlicher Bewertungen sowie der praktischen Anwendung zentraler Begriffe der Verordnung.

4.3 Chancen der KI-VO werden ambivalent bewertet

Die Auswertung der Experten-Workshops zeigt eine ambivalente Einschätzung der KI-VO im Hinblick auf ihre Auswirkungen auf Innovation und Marktchancen. Zwei der drei Gründerteams äußerten sich zurückhaltend bis kritisch zu den potenziellen Effekten der KI-VO und verwiesen darauf, dass regulatorische Anforderungen – insbesondere bei wachsender Regelungsdichte – als zusätzliche Belastung für junge Unternehmen wahrgenommen werden könnten. In diesen Fällen wurde die KI-VO eher mit einem erhöhten administrativen Aufwand und potenziellen Einschränkungen für agile Entwicklungs- und Innovationsprozesse assoziiert. Demgegenüber betonte ein Gründerteam ausdrücklich auch mögliche positive Effekte der KI-VO. Dieses hob hervor, dass ein klarer und einheitlicher Rechtsrahmen langfristig Vertrauen in KI-Systeme schaffen könne und dadurch Marktchancen eröffne, etwa durch höhere Akzeptanz bei Kunden, Geschäftspartnern oder Investoren. Die Regulierung wurde in diesem Zusammenhang nicht primär als Innovationshemmnis, sondern als potenzielles Instrument zur Legitimation und Qualitätsdifferenzierung wahrgenommen. Insgesamt verdeutlichen die Aussagen, dass die KI-VO von den befragten Gründerteams weder einheitlich negativ noch eindeutig positiv bewertet wird. Vielmehr schwankt die Wahrnehmung zwischen der Befürchtung regulatorischer Einschränkungen und der Erwartung eines möglichen Vertrauens- und Wettbewerbsgewinns. Die positive Perspektive bleibt dabei im Rahmen der Erhebung eine Minderheitsposition.

5. Fazit

Die Europäische Union verfolgt mit ihrer Digitalpolitik das Ziel, technologische Innovation, Sicherheit und Grundrechtsschutz miteinander zu verbinden und digitale Souveränität zu stärken. Start-ups und junge Unternehmen sind als zentrale Träger digitaler Innovation ein wesentlicher Schlüsselfaktor für technologischen Fortschritt, stehen jedoch einer unternehmensgrößenneutral ausgestalteten Technologieregulierung gegenüber. Junge Unternehmen sind typischerweise durch begrenzte finanzielle und personelle Ressourcen, hohe Unsicherheit, erheblichen Zeitdruck sowie einen starken Investorenfokus auf Wachstum und schnellen Markteintritt gekennzeichnet.

Die vorliegende Untersuchung folgt zielte darauf ab, Wahrnehmungen und Herausforderungen von Gründerteams im Zusammenhang mit der Umsetzung des CRA und der KI-VO im Rahmen dreier Experten-Workshops zu erfassen.

Aus der Auswertung der Experten-Workshops ergibt sich eine strukturelle Asymmetrie zwischen regulatorischem Anspruch und der Umsetzungsrealität von jungen Unternehmen. Dort, wo eine Auseinandersetzung mit dem CRA stattfindet, wird dieser weniger als punktuelle rechtliche Verpflichtung, sondern vielmehr als prozessualer Eingriff in bestehende Entwicklungspraktiken wahrgenommen. Die Belastungswahrnehmung resultiert dabei weniger aus einzelnen Pflichten als aus der Unsicherheit hinsichtlich der praktischen Umsetzung, der Vielzahl technischer Anforderungen und des damit verbundenen Ressourcenaufwands.

Die KI-VO wird von den befragten Gründerteams weder einheitlich negativ noch eindeutig positiv bewertet, sondern schwankt zwischen der Befürchtung regulatorischer Einschränkungen und der Erwartung eines möglichen Vertrauens- und Wettbewerbsgewinns. Die positive Perspektive bleibt dabei im Rahmen der Erhebung eine Minderheitsposition.

Literatur

[Bö19] Böhm, M. et al.: Die Rolle von Startups im Innovationssystem – Eine qualitativ - empirische Untersuchung. Technische Universität München, 2019.

[Bj25] Björk, A. et al.: At the Conceptual Crossroads of Politics and Technology: An Exploration Into EU Digital Policy. Politics and Governance 13/25, Article 9736, 2025.

[HP25] Heckmann, Dirk/Paschke, Anne, Cyber Resilience Act, 1. Auflage, 2025.

[Wi25] Wiebe, Gerhard, Das neue Recht der Cyberresilienz, 1. Auflage, 2025.

[Vo25] Voigt, Paul: Schefzig, Jens/Kilian, Robert, Beck OK KI-Recht, 4. Edition, 2025.