ZUSAMMENFASSUNG

Die fortschreitende Digitalisierung, die zunehmende Komplexität globaler Liefer- und Wertschöpfungsketten sowie der rasante Einsatz autonomer Technologien verändern das Risikoprofil von Verbraucher- und Industrieprodukten grundlegend: Softwaregetriebene Störungen wie der CrowdStrike-Vorfall vom 19. Juli 2024, bei dem ein ungeprüftes Update zahlreiche Microsoft-basierte Systeme lahmlegte und in der Folge Flughäfen, Banken und Krankenhäuser ihren Betrieb einstellen mussten, verdeutlichen eindrucksvoll, wie anfällig hochgradig vernetzte Ökosysteme geworden sind. Ebenso zeigt das jüngst vom Bundesgerichtshof entschiedene „Battery-Lock-out"-Verfahren, in dem ein Elektrofahrzeug nach Ratenzahlungsverzug über einen Fernbefehl deaktiviert wurde, dass Eigentumsrechte an physischen Gütern immer stärker von Software- und Datenkontrollmechanismen abhängen. Parallel dazu vervielfacht die massenhafte Verbreitung von Internet-of-Things-Geräten und KI-gestützten Anwendungen die Angriffsflächen für Cyberkriminalität, Datenmanipulation und algorithmische Fehlentscheidungen. All diese Entwicklungen stellen klassische Konzepte der ex-ante-orientierten Produktsicherheit und der ex-post-wirkenden Produzentenhaftung auf die Probe und erzwingen weltweit eine Neubewertung ihrer dogmatischen Fundamente.

Die vorliegende Untersuchung vergleicht in diesem Licht das modernisierte Unionsrecht zur Produktsicherheit und Produkthaftung mit dem türkischen Gesetz Nr. 7223 über Produktsicherheit und technische Vorschriften. Ausgangspunkt der Analyse sind die historischen Leitplanken des europäischen Rechts: der New Approach von 1985, der detailverliebte technische Vorschriften durch abstrakte „essential requirements" ersetzte und die konkrete Umsetzung harmonisierten Normen überließ, sowie das New Legislative Framework von 2008, bestehend aus Beschluss 768/2008/EG und Verordnung 765/2008/EG, das ein horizontales Referenzsystem aus einheitlichen Begriffsdefinitionen, acht modularen Konformitätsbewertungsverfahren und der CE-Kennzeichnung als Marktzutrittsvoraussetzung etablierte. Dieses System hat sich als bemerkenswert flexibel erwiesen, musste jedoch angesichts globaler E-Commerce-Strukturen, Cloud-Dienstleistungen und softwarelastiger

Wertschöpfung weiterentwickelt werden. Die Marktüberwachungsverordnung (EU) 2019/1020 setzt deshalb auf risikobasierte Online-Kontrollen, auf Datenplattformen wie das ICSMS und bindet erstmals Fulfillment-Dienstleister in die Regulierungskette ein; die Allgemeine Produktsicherheitsverordnung (EU) 2023/988 verdrängt ab Dezember 2024 die frühere Richtlinie 2001/95/EG und verlangt für sämtliche Verbraucherprodukte obligatorische interne Risikoanalysen, Cyber-Security-Checks und im Fernabsatz bereits zum Zeitpunkt des Angebots umfassende Informationspflichten über Hersteller, Produkt und Gefahren. Besonders innovativ ist ihr Anspruch, sicherheitsbedingte Rückrufe mit einem Verbraucherrecht auf Reparatur, Ersatz oder Erstattung zu verknüpfen, womit sich öffentlich-rechtliche Gefahrenabwehr und privatrechtliche Gewährleistungsinstrumente gegenseitig ergänzen.

Auf der haftungsrechtlichen Ebene ersetzt die Richtlinie (EU) 2024/2853 die fast vier Jahrzehnte alte Richtlinie 85/374/EWG. Sie erweitert den Produktbegriff ausdrücklich auf Software, digitale Fertigungsdateien, definiert den Fehlerbegriff anhand eines offenen Katalogs von neun Kriterien, der Cyber-Sicherheitsanforderungen, autonome Lernfähigkeiten und Interaktionsrisiken zwischen vernetzten Produkten ausdrücklich nennt, und zieht außerdem Plattformbetreiber, Fulfillment-Dienstleister sowie Hersteller digitaler Komponenten in den Kreis der potentiell Haftenden ein. Beweislasterleichterungen wie widerlegbare Vermutungen bei Verstößen gegen Offenlegungs- oder Aktualisierungspflichten und die Abschaffung einheitlicher Haftungshöchstgrenzen stärken die Position geschädigter Nutzer deutlich. Die klassische Entwicklungsrisikoverteidigung bleibt zwar dem Wortlaut nach erhalten, ihre praktische Reichweite schrumpft jedoch, weil Produzenten dank Over-the-Air-Updates typischerweise weiterhin Kontrolle über das Produkt behalten und neu bekannt gewordene Schwachstellen unverzüglich beheben müssen.

Das unionsrechtliche Zusammenspiel von Produktsicherheit und Produkthaftung folgt dem Leitbild einer komplementären Verzahnung. Sicherheitskonformität des Herstellers ist lediglich ein widerlegbares Indiz gegen, Non-Compliance ein widerlegbares Indiz für das Vorliegen eines Produktfehlers; damit fungiert die Haftung als Sicherheitsnetz für Risiken, die der Gesetzgeber mangels Erkenntnisstand nicht vorwegnehmen kann. Ganz

anders verhält es sich im türkischen Recht: Das Gesetz Nr. 7223 vereint Sicherheits- und Haftungsvorschriften in einem überwiegend öffentlich-rechtlich geprägten Statut und betrachtet die Einhaltung von Sicherheitsanforderungen als vollumfängliche Haftungsbefreiung. Art. 6 verlangt vom Geschädigten den Nachweis, dass das Produkt „nichtkonform" sei; Nichtkonformität ist jedoch per Definition die Verletzung von Sicherheitsrecht. Erweist sich das Produkt als regelkonform, gibt es keine Haftung – das zuvor skizzierte Sicherheitsnetz existiert nicht. Dieses starre Kopplungsdogma mag in einer rein physischen Güterwelt noch vertretbar gewesen sein; im Kontext softwareintensiver Produkte aber führt es dazu, dass Risiken aus Cyber-Angriffen, algorithmischen Fehlfunktionen oder fehlgeschlagenen Updates ohne haftungsrechtliche Antwort bleiben. Hinzu kommt, dass der türkische Produktbegriff weiterhin an körperliche Gegenstände gebunden ist; Software und digitale Dienstleistungen fallen nicht darunter, und das Gesetz kennt weder Pflichten zur Sicherheits-Update-Bereitstellung noch Mindestsupportzeiten. In einem Schadensfall bliebe damit nur das deliktsrechtliche Verschuldensprinzip, dessen Beweislastverteilung angesichts komplexer KI-Systeme praktisch unüberwindbar wäre.

Die Gegenüberstellung führt zu drei wesentlichen Reformimperativen für die Türkei. Erstens bedarf es einer dogmatischen Entkopplung von Sicherheits- und Haftungsrecht, ohne deren inhaltliche Komplementarität zu vernachlässigen: Das Haftungsrecht sollte eine multifaktorielle Fehlerprüfung nach europäischem Vorbild übernehmen, in dem Sicherheitskonformität lediglich eines von mehreren widerlegbaren Indizien darstellt. Zweitens muss der Produktbegriff software- und datenzentrierte Güter, KI-Modelle und digitale Komponenten samt ihrer Updates ausdrücklich einschließen, weil nur so die von ihnen ausgehenden Risiken adäquat adressiert werden können. Drittens sind update- und monitoringbezogene Pflichten erforderlich, die dem Cyber-Resilience Act und der GPSR ähnlichen Anspruchsniveaus genügen: Hersteller sollten für eine angemessene Mindestlaufzeit Sicherheits-Patches bereitstellen, deren Wirksamkeit überwachen und relevante Unterlagen mindestens zehn Jahre lang vorhalten müssen. Nur wenn diese Pflichten konsequent mit verschuldensunabhängiger Haftung und verfahrensrechtlichen Beweiserleichterungen kombiniert werden, kann das Haftungsrecht seine Kompensations- und Präventionsfunktion zurückgewinnen.

Zusammenfassend zeigt die Untersuchung, dass eine ausschließliche Orientierung am öffentlichen Produktsicherheitsrecht den vielfältigen Gefahren digitaler Wertschöpfung nicht gerecht wird. Ein wirksamer Verbraucherschutz sowie eine kohärente Annäherung an den europäischen Binnenmarkt erfordern ein duales, aber eng verzahntes Modell: strikte ex-ante-Sicherheitsanforderungen, flankiert von einer modernisierten, strikt und zugleich innovationssensibel ausgestalteten ex-post-Haftung. Geschieht dies nicht, drohen türkischen Nutzerinnen und Nutzern vernetzter Produkte kompensationslose Schäden, während in grenzüberschreitenden Lieferketten Rechtsunsicherheit entsteht. Die Reform des Gesetzes Nr. 7223 hin zu einem zweigliedrigen, EU-kompatiblen Rahmen, der immaterielle Software-Risiken ausdrücklich einbezieht und durchsetzbar macht, ist mithin unerlässlich, um die wachsenden Risiken vernetzter Produkte wirksam abzufedern und zugleich die Wettbewerbsfähigkeit der türkischen Industrie im digitalen Binnenmarkt zu sichern.