Dr. Stefan Hanloser, Rechtsanwalt in München mit den Schwerpunkten Datenschutzrecht und Recht der kommerziellen Datennutzung

Bremst der Datenschutz die smarte Zukunft aus? – Konsequenzen aus der EuGH-Entscheidung „Fashion ID“

Smart Entertainment, Smart Mobility, Smart Homes, Smart Cities – egal welchen Lebens- oder Gesellschaftsbereich die smarten Zukunftsmodelle betreffen, sie sind stets kollaborativ und datenintensiv. Das marktpolitische Zielbild für die Kollaboration der Marktteilnehmer ist klar definiert: Die Akteure schaffen die digitalen Zukunftsprodukte arbeitsteilig auf anbieteroffenen Plattformen – Interaktion und Interoperabilität als Gegenbild zu monolithischen Ökosystemen und Marktverengung. Abhängig von der Datenintensität sind digitale Geschäftsmodelle datenschutzrechtlich relevant. Die Datenwirtschaft orientiert sich deshalb an den Zielgrößen Datenautonomie und Partizipation an der Wertschöpfung. Der Nutzer soll – außerhalb der Grenzen seiner Sozialpflichtigkeit – über den Umgang mit seinen Daten selbst entscheiden und am generierten Mehrwert teilhaben, also auch Nutznießer der Datenverarbeitung sein.

Die in der Datenschutzkonferenz (DSK) vereinten deutschen Datenschutzbehörden haben sich im Zielkonflikt zwischen Marktoffenheit und Datenschutz klar positioniert: Durch die steigende Anzahl an Akteuren steige das Risiko einer Datenschutzverletzung und sinken die Eingriffsmöglichen, weil die Akteure räumlich entfernt sind und unterschiedlichen Jurisdiktionen unterliegen. Da hätte man doch lieber alles aus einer Hand. Wenig bemerkt sind zwei weitere datenschutzrechtliche Tendenzen, die die Akkumulation großer Datenmengen bei wenigen Playern fördern und dezentrale Strukturen behindern: das Einwilligungsprimat und die Erweiterung gemeinsamer Verantwortlichkeit.

Die arbeitsteilige Bereitstellung eines digitalen Endprodukts bedingt, dass sich die verantwortlichen Diensteanbieter und Intermediäre personenbezogene Daten übermitteln. Die DSGVO folgt dem Verbotsprinzip; eine solche Datenübermittlung zwischen Diensteanbietern bedarf stets einer Rechtsgrundlage. Die globalen Giganten können hingegen Datenflüsse unterhalb des datenschutzrechtlichen Radars innerhalb derselben juristischen Person abwickeln. Das Verbotsprinzip ist somit strukturell nachteilig für vertikale Diversifikation auf vor- und nachgelagerten Wertschöpfungsstufen. Das Verbotsprinzip schließt Teilnehmer vom Markt sogar aus, wenn sie sich aufgrund der restriktiven Auslegungspraxis der Aufsichtsbehörden nicht mehr auf ein berechtigtes Verarbeitungsinteresse als Rechtsgrund berufen können; fehlt ihnen der Kontakt zum Nutzer, können sie auch nicht auf die Einwilligung als alternativen Rechtsgrund ausweichen. Das Einwilligungsprimat führt zu einer Marktkonsolidierung. Spiegelbildlich erstarken Konglomerate und damit – als unbeabsichtigter negativer Reflex – der Anteil der rechtlich ungeregelten Binnenverarbeitung.

Ein weiterer Konzentrationsschub ist von der *Fashion ID*-Entscheidung des EuGH zu erwarten. Wer willentlich eine fremde Datenverarbeitung ermöglicht, wird in den datenschutzrechtlichen Pflichten- und Haftungskreis einbezogen. Hierzu muss man wissen, dass datenschutzrechtlich nur verantwortlich ist, wer entscheidet, für welchen Zweck und mit welchen Mitteln personenbezogene Daten verarbeitet werden. Entscheiden mehrere Akteure über das Wofür und Womit gemeinsam, sind sie gemeinsam Verantwortliche (Joint Controllers). Die Anforderungen an die wenig geschätzte datenschutzrechtliche Gesamtschuld hat der EuGH in mehreren Entscheidungen immer weiter herabgesetzt. So kann mitverantwortlich sein, wer auf die personenbezogenen Daten gar nicht zugreifen kann, sondern eine fremde Verarbeitungshandlung ermöglicht (EuGH, 5.6.2018 – C-210/16 – Wirtschaftsakademie Schleswig-Holstein, BB 2018, 1480). In der jüngsten Entscheidung (29.7.2019 – C-40/17 – Fashion ID) verzichtet der EuGH auch auf einen gestaltenden Einfluss auf die Datenverarbeitung, etwa durch Parametrierung. Aus dieser streng kausalen Perspektive reicht jeder Ermöglichungsbeitrag, ohne den die fremde Verarbeitungssequenz nicht in ihrer konkreten Form stattgefunden hätte. Auch setzt die gemeinsame Zweckentscheidung keine abgestimmte Entscheidungsfindung der Akteure, d.h. keinen gemeinsamen Entscheidungsprozess voraus. Gemeinsame Zweckentscheidung übersetzt der EuGH mit der Verfolgung gleichlaufender wirtschaftlicher Interessen – in Abgrenzung zum Auftragsverarbeiter, der eine fremde Datenverarbeitung im Rahmen eines synallagmatischen Austauschverhältnisses ermöglicht. Unterm Strich erfindet der EuGH die datenschutzrechtliche Beihilfe – mit weitreichenden Konsequenzen. Der Gehilfe muss eine Rechtsgrundlage für seine Ermöglichung der fremden Datenverarbeitungshandlung nachweisen. Ihn treffen gesamtschuldnerisch die datenschutzrechtlichen Primärpflichten, insbesondere die Erfüllung der Betroffenenrechte. Er begibt sich in einen Haftungsverbund mit anderen Plattformteilnehmern. Und in Netzwerken müsste man ein Geflecht von Joint Controller Agreements erst einmal administrativ auf die Beine stellen. Das bloße Risiko, gemeinsam mit anderen Marktteilnehmern als Joint Controller verhaftet zu sein, ist ein Hemmschuh für die arbeitsteilige Digitalwirtschaft.

> *Das bloße Risiko, gemeinsam mit anderen Marktteilnehmern als Joint Controller verhaftet zu sein, ist ein Hemmschuh für die arbeitsteilige Digitalwirtschaft.*

Fazit: Kausal betrachtet hat die datenschutzrechtliche Entscheidungspraxis der Gerichte und Aufsichtsbehörden einen strukturierenden Einfluss auf die europäische Digitalwirtschaft. Final betrachtet können datenschutzrechtliche Wertungsentscheidungen aber durchaus marktpolitische Zielbilder berücksichtigen, insbesondere wenn sie das künftige Datenschutzniveau positiv prägen. Hier steht die datenschutzrechtliche Diskussion aber noch ganz am Anfang.