POSITIONSPAPIER

DIE FAMILIEN UNTERNEHMER

DIE JUNGEN UNTERNEHMER

Der gläserne Unternehmer wird Realität

Bewertung des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen {COM (2018) 225}

Zukünftig sollen Behörden aus EU-Staaten und selbst den USA, ohne explizite Einbeziehung und Prüfung durch die deutsche Justiz, die sensibelsten Daten bei europäischen Cloud-Anbietern sichern, abfragen und weiterverarbeiten können. Damit wären Daten von mittelständischen Unternehmen selbst in Deutschland nicht mehr sicher.

1. Datensouveränität und europäische Cloud

Ein zentrales Thema der Digitalisierung ist das Bemühen um digitale Datensouveränität. Bundeswirtschaftsminister Peter Altmaier verfolgt mit Gaia-X aktuell den Plan zur Schaffung einer europäischen Cloudinfrastruktur, die deutschen Unternehmen ermöglichen soll, ihre (sensiblen) Daten in Europa zu belassen (und nicht z. B. in den USA). Auf diese Weise sollen deutsche und europäische Unternehmer von US-amerikanischen Anbietern unabhängig werden und die Kontrolle über ihre Schlüsseltechnologien behalten: Mit Gaia-X soll also Sicherheit, Souveränität sowie Datenschutz gewährleistet und so die Wettbewerbsfähigkeit Europas weiter gestärkt werden. Auch Bundeskanzlerin Angela Merkel betont in einer Rede beim Deutschen Maschinenbaugipfel: „Was mir aber große Sorgen macht, ist die Frage der Datenautonomie, der Datensouveränität europäischer Unternehmen. (...) Datenmanagement findet heute in hohem Maße gemeinsam mit amerikanischen Firmen statt. Ich bin der Meinung, wir brauchen in Europa eine eigene Cloud-Bewirtschaftung, eine eigene Hyperscale, wie man sagt, also eine Plattform, auf der wir Daten nicht nur lagern können, sondern auch verarbeiten können, damit aus Daten, über Künstliche Intelligenz, wieder neue Produkte entstehen.“
Eine europäische Cloudlösung könnte durch den strengen Datenschutz zum wirklichen Wettbewerbsvorteil avancieren. Dieser grundsätzlich zu begrüßende Ansatz ist jedoch in Gefahr, bevor er überhaupt umgesetzt ist.

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

2. E-Evidence-Verordnung

Derzeit wird auf europäischer Ebene, von der Öffentlichkeit wenig beachtet, die so genannte E-Evidence-Verordnung verhandelt, die es den Strafverfolgungsbehörden in allen EU-Mitgliedstaaten erlauben soll, Verkehrs-, Bestands- und vor allem Inhaltsdaten in anderen EU-Staaten als elektronische Beweismittel ohne irgendein Rechtshilfegesuch zu sichern. Dazu reicht ein schwacher Anfangsverdacht in Strafangelegenheiten (z. B. Betrug oder Unterschlagung) aus. Konkret bedeutet dies: Behörden in Ländern mit einem niedrigeren Rechtsschutzstandard als Deutschland können zukünftig von deutschen Cloud-Anbietern die Sicherung und Herausgabe umfassender Daten verlangen (z. B. bei GMX gespeicherte E-Mails), ohne dass deutsche Instanzen die Rechtmäßigkeit prüfen und ggf. ihr Veto einlegen können. Anders als beim bisherigen Verfahren des Amtshilfegesuchs ist somit keine explizite Prüfung auf Bewilligungshindernisse (wie etwa Verhältnismäßigkeit etc.) vorgesehen. Der Kreis der „Dienstanbieter“ ist denkbar weit gefasst, sodass auch interne Firmennetzwerke als Adressaten einer Sicherungs- und Herausgabeanordnung nicht ausgeschlossen werden können.

Da das Verfahren grundsätzlich keine aktive Beteiligung inländischer Justizbehörden vorsieht, fällt die Rolle der Prüfung auf Herausgabe der Daten den jeweiligen Dienstanbietern zu – sie müssen die Rechtmäßigkeit der Abfragen prüfen. Ähnlich wie bereits beim NetzDG fände eine Privatisierung hoheitlicher Aufgaben statt. Hierzu würden enge Fristen gelten: Die Cloud-Anbieter sind verpflichtet, die von Behörden angeforderten Daten binnen zehn Tagen oder in Eilfällen innerhalb von 360 Minuten herauszugeben. Die Definition eines „Notfalls“ obliegt dabei dem Anordnungsstaat und wird vermutlich entsprechend divergent ausfallen. Als Sanktionen für den Fall, dass Dienstanbieter nicht oder zu spät reagieren, sind Strafzahlungen von bis zu zwei Prozent des weltweiten Jahresumsatzes vorgesehen. Ein abgestuftes Sanktionsmodell oder klare Ausnahmeregelungen für Kleinunternehmen ist im Verordnungsentwurf nicht berücksichtigt.

Eine staatliche Beteiligung im Vollstreckungsstaat erscheint jedoch angezeigt, da dem Verfahren im Ausland oftmals Handlungen zugrunde liegen könnten, die nach deutschem Recht überhaupt nicht strafbar sind. Zu befürchten ist zudem, dass die Anordnung zur Sicherung und Herausgabe elektronischer Beweise häufig keinem Richtervorbehalt unterliegen, sondern durch nachgeordnete Stellen erfolgen wird. Der Entwurf in seiner jetzigen Form öffnet dem Missbrauch somit Tür und Tor. Insbesondere auch die vorgegebene niedrige Zugriffsschwelle ist problematisch. Denn sollte sich der Anfangsverdacht als unbegründet erweisen, sind die Daten bereits abgeflossen. Eine Pflicht zur Löschung von Daten, wenn sich eine Anordnung nachträglich als rechtswidrig erwiesen haben sollte, ist im gegenwärtigen Entwurf nicht vorgesehen.

Wie so oft ist die Intention der EU-Kommission eigentlich begrüßenswert – nämlich die Erleichterung der Strafverfolgung, der daraus resultierende Vorschlag ist jedoch unausgegoren und schießt vollkommen über das Ziel hinaus.

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

Mit dem Entwurf ist der Grundrechtsschutz in Deutschland latent in Gefahr. Etwa dann, wenn ausländische Strafverfolgungsbehörden z. B. gegen einen deutschen Journalisten aufgrund seiner investigativen Recherche ermitteln. Die Güterabwägung zwischen Grundrechtschutz und innerer Sicherheit fällt einseitig aus. Eine weitere Folge könnte die Asymmetrie bei den ermittlungstechnischen Instrumenten deutscher und ausländischer Behörden sein. Während deutsche Ermittlungsbehörden eng umgrenzte Kompetenzen im Bereich der Telekommunikationsdaten haben (wie die kontroverse Diskussion um die Vorratsdatenspeicherung zeigt), würden ausländische Stellen weitaus größere Zugriffsmöglichkeiten in Deutschland erhalten.

Paradox erscheint in diesem Zusammenhang auch, dass die EU sonst ein hohes Niveau an Datenschutz und das Recht auf informationelle Selbstbestimmung verfolgt, durch die E-Evidence-Verordnung diese Prinzipien jedoch durch die „Hintertür“ aufweicht.

3. Ausweitung auf die USA

Darüber hinaus hat der Entwurf erhebliche wirtschaftspolitische Implikationen und berührt massiv Unternehmerinteressen. Verschärft wird dies durch die derzeit laufenden Verhandlungen die Herausgabeverordnung auf die USA auszuweiten. Ein nicht unrealistisches Szenario ist folgendes: Falls ein deutsches Unternehmen in den USA – zu Recht oder zu Unrecht – ins Visier der US-Justiz gerät, kann diese ohne Einbindung und Kontrolle durch deutsche Behörden geheime, sensible und persönliche Daten, die in der europäischen oder deutschen Cloud gespeichert sind, abfragen und weiterverarbeiten. Eine diesbezügliche Klagemöglichkeit in Deutschland haben die Unternehmen nicht – falls sie diesen Datenabfluss überhaupt bemerken. Zur Durchsetzung ihres Individualschutzes müssten sich die Betroffenen in den Bereich des Rechtsraums des jeweiligen Anordnungsstaates begeben.

4. Abschließende Handlungsempfehlung

Mit der europäischen Herausgabe- und Sicherungsanordnung droht ein faktischer Ausverkauf der Existenzgrundlage des deutschen Mittelstandes. Sie führt den Plan einer europäischen Cloud von Bundeswirtschaftsminister Peter Altmaier zuletzt womöglich ad absurdum. Unternehmensdaten unterliegen nicht länger zwingend dem Schutz der deutschen Rechtsordnung.

Die von Deutschland bei den Verhandlungen im Ministerrat eingebrachten Änderungen (wie etwa eine Notifikationslösung für die grenzüberschreitende Abfrage von Verkehrs- und Inhaltsdaten) sind im Vergleich zum Initiativvorschlag der EU-Kommission vom April 2018 sinnvoll und zu begrüßen, reichen jedoch nicht aus. Trotz der starken Unterstützung der Verordnung durch Spanien und Frankreich und der anstehenden deutschen – mit einer gewissen Neutralitätspflicht verbundenen – Ratspräsidentschaft im zweiten Halbjahr 2020,

sollten die Bundesregierung und das Europäische Parlament zeitnah die Notbremse ziehen und Schlimmeres verhindern. Das Europäische Parlament hat hierzu bereits eine gute Richtung vorgegeben: Der, von der Berichterstatterin im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) Frau Sippel vorgelegte Berichtsentwurf enthält im Vergleich zur Ursprungsvariante viele substantielle Verbesserungen. Gegenwärtig befindet sich der Entwurf im Trilogverfahren und ist damit Gegenstand erneuter Verhandlungen zwischen Kommission, Ministerrat und Parlament.

Auch die Verhandlungen mit den USA laufen aktuell. Deshalb besteht derzeit die einmalige Chance die grundsätzliche Notwendigkeit der E-Evidence-Verordnung kritisch zu hinterfragen. In diesem Zusammenhang wäre es sinnvoll, die Evaluation der 2014 eingeführten Europäischen Ermittlungsanordnung zu berücksichtigen. Zumindest sollte auf die Ausgestaltung der Verordnung sowie der sie ergänzenden Richtlinie eingewirkt und auf sachgerechte Sicherungsmechanismen gedrängt werden. Dabei wären Überprüfungsmöglichkeiten im Falle von Sicherungs- und Herausgabeanordnungen zwingend erforderlich: Denkbar wäre es beispielsweise, dass ohne die Zustimmung der Behörden im Vollstreckungsstaat keine Herausgabe von Daten erfolgen darf. In jedem Fall sollte eine Veto-Möglichkeit für den Ausführungsstaat vorgesehen werden, falls die inländischen Behörden eine fundamentale Verletzung von Grundrechten feststellen sollten.

Dieses sollte mit weiteren Anpassungen des zurzeit in der Umsetzungsgesetzgebung befindlichen einfachen EU-Rechts an die verfassungsrechtlichen Vorgaben des EU- und des deutschen Rechts einhergehen. Zu denken ist hier insbesondere an die 5. Geldwäsche-Richtlinie und das dort vorgesehene „Transparenzregister“. Stets sollte das Gebot gelten: Datenschutz auch für Unternehmer.

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu