Alexander Dix

Motor oder Flaschenhals?
Die Regeln der Datenschutz-Grundverordnung zur Zusammenarbeit und Kohärenz der Datenschutzaufsicht

Die Koordination der Datenschutzaufsichtsbehörden in der Europäischen Union soll Auslegung und Vollzug der 2018 in Kraft getretenen Datenschutzgrundverordnung möglichst weitgehend vereinheitlichen. Sie soll auch verhindern, dass sich internationale Konzerne, die in großem Umfang personenbezogene Daten verarbeiten, dort ansiedeln, wo die Datenschutzkontrolle am schwächsten ausgeprägt ist. Der folgende Beitrag zeigt, dass diese Ziele seit 2018 in Teilen, aber noch nicht vollständig erreicht wurden.

Zu den wichtigsten Neuerungen bei der Verabschiedung des einheitlichen europäischen Rechtsrahmens in der Datenschutz-Grundverordnung (DS-GVO) von 2016 gehören die Regeln über die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden in Europa im Kapitel VII der DS-GVO. Der europäische Gesetzgeber hat neben der stärkeren Harmonisierung des materiellen Datenschutzrechts großen Wert auf seine effektive und einheitliche Durchsetzung gelegt. Die Änderungen im materiellen Recht fallen sogar gegenüber der grundlegenden Neuaufstellung der europäischen kooperativen Datenschutzaufsicht bescheiden aus, anders ausgedrückt, viele Pflichten der Datenverarbeiter änderten sich mit dem Inkrafttreten der Grundverordnung nicht prinzipiell, sie wurden nur mit einer schärferen Sanktionsdrohung verknüpft, die vor 2016 fehlte.

Vor allem aber war dem europäischen Gesetzgeber bewusst, dass der beste Rechtsrahmen wenig wert ist, wenn nicht für eine effektive und möglichst einheitliche Rechtsdurchsetzung gesorgt wird. Zu den Problemen mit der Datenschutz-Richtlinie von 1995 zählte neben der mangelnden Harmonisierungswirkung, die durch die Wahl des Rechtsakts „Richtlinie“ bedingt war, das beträchtliche Vollzugsdefizit in den Mitgliedstaaten, auch soweit diese die Richtlinie umgesetzt hatten. Zu den Divergenzen im materiellen nationalen Recht kamen unterschiedliche Rechtsauffassungen bei den Aufsichtsbehörden über die Bedeutung und Anwendung des europaweiten Rechtsrahmens. Dem soll mit der Grundverordnung abgeholfen werden. Auch wenn diese erst

Zitiervorschlag:
Dix, Alexander (2020): Motor oder Flaschenhals? Die Regeln der Datenschutz-Grundverordnung zur Zusammenarbeit und Kohärenz der Datenschutzaufsicht, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 231/232 [59(3-4)], S. 87-97.

etwas mehr als zwei Jahre in Kraft ist, kann man eine erste Zwischenbilanz ziehen, inwieweit dies in einer Welt gelungen ist, in der große global agierende Datenverarbeiter wie *Google* und *Facebook* ihr Geschäftsmodell nach wie vor auf die „Überwachungsdividende" (Shoshana Zuboff) stützen.

Kooperation vor der Grundverordnung

Die Kooperation zwischen den europäischen Datenschutzbehörden hat nicht erst mit dem Inkrafttreten der Grundverordnung 2018 begonnen. Schon die Internationale Datenschutzkonferenz 1989 in Berlin wies in einer Entschließung auf die Notwendigkeit hin, der zunehmenden grenzüberschreitenden Datenverarbeitung und den damit einhergehenden Risiken für den Datenschutz durch eine verstärkte internationale Zusammenarbeit der Aufsichtsbehörden zu begegnen. Mit dem Inkrafttreten der europäischen Datenschutz-Richtlinie von 1995 nahm die sog. Art. 29-Gruppe ihre Arbeit auf, deren Hauptaufgabe es war, „*alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen.*"[1] Sie konnte Stellungnahmen und Empfehlungen zu allen den Datenschutz betreffenden Fragen, insbesondere auch zum Datenschutzniveau in Drittstaaten abgeben. Allerdings waren diese Stellungnahmen und Empfehlungen nicht verbindlich, insbesondere die Europäische Kommission war nicht verpflichtet, sie umzusetzen, sie musste der Gruppe nur mitteilen, welche Konsequenzen sie aus deren Stellungnahmen und Empfehlungen gezogen hatte. So überging die Kommission etwa die kritischen Stellungnahmen der Art. 29-Gruppe und des Europäischen Parlaments zum später vom Europäischen Gerichtshof kassierten Safe-Harbor-Abkommen mit den USA. Diese Schwäche der Art. 29-Gruppe wurde strukturell noch dadurch verschärft, dass ihr Sekretariat bei der Kommission angesiedelt war, die dadurch erheblichen Einfluss auf die Arbeitsweise der Gruppe nehmen konnte. Schließlich hatte die Art. 29-Gruppe keine eigene Rechtspersönlichkeit.

Gerade vor diesem Hintergrund hat die Art 29-Gruppe gleichwohl einen erheblichen Beitrag zur Vereinheitlichung des Datenschutzrechts in Europa geleistet, indem sie zahlreiche Stellungnahmen und Arbeitspapiere veröffentlicht hat, die den Charakter von „soft law" annahmen und – soweit sie grundsätzlichen Charakter hatten – später vom Europäischen Datenschutzausschuss in seiner ersten Sitzung im Mai 2018 übernommen und weiterentwickelt wurden.

Der neue Rechtsrahmen

Mit der Datenschutz-Grundverordnung hat der Unionsgesetzgeber neben einer stärkeren Harmonisierung des materiellen Datenschutzrechts dessen Geltung auch für außereuropäische Datenverarbeiter, die in Europa Geschäfte machen, klargestellt (Marktort-Prinzip). Entgegen der Rechtsprechung des *US-Supreme Court* hatten vor

2016 US-amerikanische Unternehmen wie *Facebook* und *Google* lange Zeit die Auffassung vertreten, auch in Europa nur an das Recht ihres Sitzlandes Kalifornien gebunden zu sein (wo inzwischen ein der Datenschutz-Grundverordnung sehr ähnliches striktes Datenschutzrecht gilt). Zudem hat der Unionsgesetzgeber insbesondere die Aufsichtsbehörden mit stärkeren Befugnissen etwa zur Verhängung empfindlicher Sanktionen bei Rechtsverstößen, aber auch zur Unterbindung von rechtswidrigen Datenverarbeitungen („Ziehen des Steckers") ausgestattet. Letzteres war nach deutschem Recht vor 2018 nur zulässig bei schwerwiegenden Verstößen und Mängeln, wenn diese nicht in angemessener Zeit beseitigt wurden.[2] Die massive Bußgeldandrohung der Grundverordnung von bis zu 4% des weltweit erzielten Jahresumsatzes eines Unternehmens trug wesentlich dazu bei, dass viele Führungsetagen erstmals begannen, Datenschutzprinzipien ernst zu nehmen, die bereits zuvor geltendes, allerdings nur schwach sanktionsbewehrtes Recht gewesen waren.

In prozeduraler Hinsicht hat die Grundverordnung zu Recht keine zentrale Datenschutzkontrolle etwa durch den Europäischen Datenschutzbeauftragten eingeführt, sondern die bisherige dezentrale Kontrolle durch unabhängige Datenschutzbehörden der einzelnen Mitgliedstaaten beibehalten. Der Europäische Datenschutzbeauftragte bleibt ausschließlich für die Institutionen der Europäischen Union zuständig. Wäre ihm auch die Kontrolle aller Unternehmen und Behörden übertragen worden, die in der EU Bürger- und Kundendaten verarbeiten, hätte dies zur Entstehung einer riesigen und zugleich bürgerfernen Kontrollbürokratie geführt. Stattdessen hat der Unionsgesetzgeber ein Verfahren verankert und verallgemeinert, dass die Art. 29-Gruppe bereits bei der Behandlung von bindenden Unternehmensregelungen (*Binding Corporate Rules*) für den Datenexport in außereuropäische Drittstaaten entwickelt hatte, das One-Stop-Shop-Verfahren. Danach kann jedes außereuropäische Unternehmen mit einer Niederlassung in Europa sich ausschließlich an die Datenschutzbehörde des Sitzlandes dieser Niederlassung als alleinigen Ansprechpartner halten und muss nicht befürchten, dass seine Verarbeitung der Daten von Unionsbürgern von 27 verschiedenen Aufsichtsbehörden kontrolliert und ggf. sanktioniert wird. Wenn die Datenverarbeitung in mehr als einem Mitgliedstaat erfolgt oder wesentliche Auswirkungen auf Menschen in mehreren Mitgliedstaaten hat, übernimmt die Datenschutzbehörde, die für die Hauptniederlassung des Unternehmens zuständig ist, als *lead authority* die Federführung und beteiligt die Aufsichtsbehörden der anderen betroffenen Mitgliedstaaten an der Entscheidung über die Rechtmäßigkeit der Datenverarbeitung (z.B. aufgrund der Beschwerde eines betroffenen Bürgers).[3] Dieses One-Stop-Shop-Verfahren ist eine Konzession an die Wirtschaft und soll der von außereuropäischen Unternehmen geübten Kritik an einer abschreckenden Wirkung einer heterogenen Aufsichtsstruktur auf Datenverarbeiter Rechnung tragen, die auf dem europäischen Markt aktiv werden wollen. Außereuropäische Unternehmen, die keine Niederlassung in der EU haben, können sich nicht auf das One-Stop-Shop-Privileg berufen, sondern müssen sich dagegen mit 27 verschiedenen Datenschutzbehörden auseinandersetzen, wenn sie ihre Dienste in allen EU-Ländern anbieten wollen.

Zugleich erlaubt es das neue europäische Datenschutzrecht aber auch jedem betroffenen Bürger, sich an die Datenschutzbehörde seines Aufenthaltsstaates, seines Arbeitsplatzes oder des Ortes des Datenschutzverstoßes zu wenden, die für ihn damit

zum alleinigen Ansprechpartner wird.[4] Soweit Betroffene sich gegen die Datenverarbeitung durch Unternehmen gerichtlich zur Wehr setzen wollen, können sie ebenfalls zuständige Gerichte in ihrem Aufenthaltsstaat anrufen, auch wenn das Unternehmen dort keine Niederlassung hat.[5] Insofern gewährt die Grundverordnung auch den betroffenen Bürgern einen „One-Stop-Shop".

Neu durch die Grundverordnung geschaffen wurde außerdem der Europäische Datenschutzausschuss, der mit eigener Rechtspersönlichkeit ausgestattet wurde und an die Stelle der Art. 29-Gruppe getreten ist.[6] Zugleich wurde die institutionelle Schwäche des Koordinationsgremiums der europäischen Datenschutzbehörden beseitigt, indem das Sekretariat des Europäischen Datenschutzausschusses beim Europäischen Datenschutzbeauftragten statt bei der Kommission angesiedelt wurde.[7] Der Datenschutzausschuss kann im ebenfalls neu geschaffenen Kohärenzverfahren verbindlich in Streitfällen zwischen den nationalen Aufsichtsbehörden entscheiden, wobei diesen unter bestimmten Voraussetzungen die Möglichkeit zu Eilentscheidungen verbleibt.[8]

Die durchwachsene Bilanz der ersten beiden Jahre

Bereits in der Übergangsphase zwischen der Verabschiedung der Grundverordnung 2016 und ihrem Inkrafttreten im Mai 2018 hat der Stellenwert des Datenschutzes in der öffentlichen Diskussion und in den Prioritätenlisten der Unternehmen und Behörden erfreulich deutlich an Bedeutung zugenommen, was weniger an inhaltlichen Änderungen des Rechtsrahmens oder der neu geregelten Zusammenarbeit der Datenschutzbehörden als vielmehr an dem neu geschaffenen Sanktionsinstrumentarium gelegen haben dürfte.

Die Google-Entscheidung der französischen CNIL

Die bisher höchste Sanktion wegen eines Verstoßes gegen die Grundverordnung, eine Geldbuße in Höhe von 50 Mio. Euro hat die französische Datenschutzkommission (*Commission Nationale de l'Informatique et des Libertés – CNIL*) im Januar 2019 gegen den US-Konzern *Google LL.C.* mit seiner französischen Tochter *Google France SARL* verhängt.[9] Diese Geldbuße ist mittlerweile – auf die Klage von *Google* hin – durch den französischen *Conseil d'Etat* bestätigt worden und damit rechtskräftig. Die finanzielle Sanktion wurde damit begründet, dass *Google* die französischen Nutzer seiner Webseiten und des mobilen Betriebssystems Android unzureichend über die dadurch ausgelöste Verarbeitung ihrer Daten informiert hatte. Entsprechende Informationen waren – wenn überhaupt – nur schwer zugänglich und entsprachen zudem nicht den Vorgaben der Grundverordnung, die die Transparenzpflichten der Datenverarbeiter verschärft hatte.

Interessant an dieser Entscheidung ist vor allem, wie die *CNIL* ihre Zuständigkeit begründet hat. Zwar hatte das US-Unternehmen *Google* (mittlerweile eine Tochter des *ALPHABET*-Konzerns) schon zum Zeitpunkt der *CNIL*-Entscheidung einen Großteil ih-

rer europäischen Aktivitäten, insbesondere das Anzeigengeschäft auf ihre irische Tochter *Google Ireland Limited* übertragen und dieses Unternehmen zur europäischen Hauptniederlassung erklärt. Allerdings hatte die US-Mutter *Google LL.C.* in ihrer Datenschutzerklärung von 2018 die irische Niederlassung nicht als Hauptniederlassung erwähnt und gegenüber der *CNIL* im Verfahren erklärt, sie werde erst Ende Januar 2019 die Verantwortung für die Verarbeitung der Daten europäischer Nutzer auf die irische Tochtergesellschaft übertragen. Deshalb hielt die *CNIL* vor dieser Verlagerung der Verantwortung ein One-Stop-Shop-Verfahren nicht für geboten und nahm ihre eigene Zuständigkeit bezüglich der französischen *Google*-Tochter an. Die übrigen europäischen Datenschutzbehörden, darunter auch die irische Datenschutzbeauftragte, teilten diese Auffassung. Die *CNIL* betonte in ihrer Entscheidung auch die Absicht des Unionsgesetzgebers, außereuropäischen Datenverarbeitern nicht die Wahl der für sie zuständigen Datenschutzbehörde (*forum shopping*) zu überlassen. Vielmehr sei die Frage, wer verantwortliche Hauptniederlassung sei, stets nach objektiven Kriterien von den Datenschutzbehörden zu beurteilen.

Der irische Flaschenhals

Mit der Verlagerung der Verantwortung für die europäische Datenverarbeitung nach Irland liegt mittlerweile die Zuständigkeit für *Google* bei der irischen Datenschutzbeauftragten, die damit auch die federführende Aufsichtsbehörde bei künftigen Beschwerden gegen und Datenschutzverstößen durch *Google* ist. Seit dem Inkrafttreten der DS-GVO hat die irische Datenschutzbehörde diese Funktion auch für mindestens drei weitere große Internet-Konzerne, nämlich *Facebook* (einschließlich der zu *Facebook* gehörenden Dienste *WhatsApp* und *Instagram*), *Twitter* und *Apple*. Gegen die Praktiken von *Facebook*, *WhatsApp* und *Instagram* legte die vom österreichischen Datenschutz-Aktivisten Max Schrems gegründete Bürgerrechtsorganisation *None of Your Business* (*noyb*) am Tag des Inkrafttretens der Grundverordnung Beschwerden bei der irischen Datenschutzbeauftragten ein. Schrems hatte 2015 das Urteil des Europäischen Gerichtshofs zur Nichtigkeit des Safe-Harbor-Abkommens zwischen der EU und den USA erstritten.[10] Über die *noyb*-Beschwerden wurde bis heute nicht endgültig entschieden.[11] Stattdessen setzte die irische Datenschutzbeauftragte ihre begrenzten Ressourcen für eine gerichtliche Klärung der Frage ein, ob die von *Facebook* verwendeten Standardvertragsklauseln den Export der Daten von Max Schrems und anderen Nutzern in die USA rechtfertige. Diese Klage führte im Juli 2020 zur zweiten Entscheidung des EuGH in Sachen transatlantischer Datenverkehr, in der dieser erneut das Datenschutzniveau in den USA aufgrund des unbegrenzten Zugriffs der Geheimdienste auf die Daten von Ausländern für unzureichend erklärte und die europäischen Datenschutzbehörden explizit zum Tätigwerden aufforderte.[12] Die von Max Schrems und *noyb* herbeigeführten EuGH-Urteile verdeutlichen, wie wichtig die Aktivitäten von zivilgesellschaftlichen Organisationen für die Durchsetzung der europäischen Datenschutzstandards sind, zumal die Aufsichtsbehörden vielfach aufgrund ihrer begrenzten Kapazitäten nur noch aufgrund von Beschwerden Betroffener tätig werden und keine anlasslosen systematischen Prüfungen mehr durchführen.

Erst zwei Jahre nach Inkrafttreten der Grundverordnung teilte die Datenschutzbeauftragte mit, sie habe die Untersuchung aufgrund der Beschwerde gegen *Facebook* abgeschlossen und befinde sich jetzt im Entscheidungsprozess; zu den Beschwerden gegen *WhatsApp* und *Instagram* wurden diese Unternehmen sowie die Beschwerdeführer zur ergänzenden Stellungnahme aufgefordert. Lediglich in einem Prüfverfahren, das durch die Meldung eines Datenlecks bei *Twitter* ausgelöst worden war, hat die irische Behörde gleichzeitig zum ersten Mal als federführende Behörde den anderen betroffenen europäischen Aufsichtsbehörden einen Beschlussentwurf nach Art. 60 der Datenschutz-Grundverordnung zugeleitet.[13] Insgesamt sind gegenwärtig 23 Verfahren gegen multinationale Datenverarbeiter aus dem Technologie-Sektor in Irland anhängig, die meisten davon gegen *Facebook* mit seinen Tochterunternehmen. Die Gründe für dieses dilatorische Vorgehen der irischen Datenschutzbehörde sind unklar. Sie liegen jedenfalls nicht in den – teilweise formalistisch anmutenden – Regelungen der Grundverordnung über die Zusammenarbeit der europäischen Aufsichtsbehörden. In den ersten zwei Jahren seit dem Inkrafttreten des neuen Rechtsrahmens sind 68 abgestimmte Entscheidungen von 17 verschiedenen Aufsichtsbehörden zu Fällen grenzüberschreitender Datenverarbeitungen im One-Stop-Shop-Verfahren gefällt worden, jedoch ist keine dieser Entscheidungen von der irischen Datenschutzbehörde federführend vorbereitet worden.[14] Die irische Datenschutzbeauftragte Helen Dixon betonte im Februar 2020, dass hohe Bußgelder (bis zu 4% des globalen Jahresumsatzes des betroffenen Unternehmens), die nach der Grundverordnung verhängt werden können, unausweichlich seien, aber gerichtsfest begründet werden müssten. Dazu habe sie externen juristischen Sachverstand eingeschaltet.[15] Auch wenn internationale Technologie-Konzerne in aller Regel jede Möglichkeit ausschöpfen, um gegen sie verhängte Sanktionen gerichtlich überprüfen zu lassen, hat dies etwa die französische *CNIL* nicht davon abgehalten, gegen *Google* ein Bußgeld in Höhe von 5 Millionen EUR zu verhängen, das der *Conseil d'Etat* inzwischen bestätigt hat. Dixon bezeichnete immerhin die von der *US-Federal Trade Commission* wegen Datenschutzverstößen gegen *Facebook* verhängte Geldbuße in Höhe von 5 Mrd. US-Dollar als einen Maßstab auch für europäische Sanktionen.

Auch die finanzielle und personelle Ausstattung der irischen Behörde kann nicht als Rechtfertigung für ihr zögerliches Vorgehen herangezogen werden. Zwischen 2016 und 2019 erfuhr ihr Budget ebenso wie das der Behörden in den Niederlanden, Island, Luxemburg und Finnland den stärksten relativen Zuwachs (wobei die irische Behörde zuvor besonders schlecht ausgestattet war). Allerdings hat die Europäische Kommission darauf hingewiesen, dass gerade in Ländern wie Irland und Luxemburg, wo internationale Technologie-Konzerne ihren europäischen Hauptsitz haben, die Aufsichtsbehörden wegen ihrer Federführungsfunktion in wichtigen Fällen grenzüberschreitender Datenverarbeitung eine bessere Ausstattung benötigen als die Bevölkerungszahlen dieser Länder es nahelegen.[16] Die Bürgerrechtsorganisation *None of Your Business* hat inzwischen Klage vor dem irischen *High Court* gegen die irische Datenschutzbeauftragte wegen Untätigkeit bzw. zögerlicher Behandlung ihrer Beschwerden erhoben. Diese zusätzliche Rechtsschutzmöglichkeit ist erst durch die Grundverordnung 2018 geschaffen worden.[17]

Die Probleme des Vollzugsdefizits bei grenzüberschreitender Datenverarbeitung beruhen auch auf einem zentralen Mangel in der Grundverordnung. Diese sieht zwar in Art. 60 detaillierte Fristen vor, innerhalb derer die betroffenen Aufsichtsbehörden (alle von der Datenverarbeitung berührten Behörden, die selbst nicht federführend sind) sich zu Beschlussentwürfen der *lead authority* äußern müssen. Dagegen ist die federführende Behörde selbst nicht verpflichtet, innerhalb einer bestimmten Frist einen Beschlussentwurf vorzulegen, ohne den das Verfahren gar nicht erst beginnen kann. Sie muss dies nur „unverzüglich" tun.[18] Dieser unbestimmte Rechtsbegriff ermöglicht es ihr, Verzögerungen mit sachlich erscheinenden Begründungen zu rechtfertigen. Welche Rechte die anderen Aufsichtsbehörden haben, solange die federführende Behörde passiv bleibt, ist unklar und wird – auf Vorlage eines belgischen Gerichts hin – möglicherweise demnächst vom Europäischen Gerichtshof geklärt. Zwar hätte jede Aufsichtsbehörde auch das Recht, den Europäischen Datenschutzausschuss um eine Stellungnahme zu bitten, wenn eine federführende Aufsichtsbehörde das Abstimmungsverfahren behindert und dies Auswirkungen in mehreren Mitgliedstaaten hat.[19] Das ist aber bisher nicht geschehen und wäre vermutlich auch wenig zielführend, weil die *lead authority* wenig Probleme haben dürfte zu begründen, weshalb sie ihrer Pflicht zur unverzüglichen Vorlage eines Beschlussentwurfs nicht nachgekommen ist.

Schließlich hat jede Aufsichtsbehörde das Recht, bei dringendem Handlungsbedarf zum Schutz der Interessen betroffener Personen Eilmaßnahmen gegen den Datenverarbeiter zu verhängen, wenn die federführende Aufsichtsbehörde nicht rechtzeitig tätig wird.[20] Von diesem Mittel ist bisher allerdings kein Gebrauch gemacht worden, auch wenn einzelne Aufsichtsbehörden auf diese Möglichkeit hingewiesen und dadurch offenbar die Kompromissbereitschaft der betroffenen Unternehmen erhöht haben. Auch die neu geschaffene Möglichkeit der verbindlichen Streitbeilegung durch den Europäischen Datenschutzausschuss[21] ist in der bisherigen Praxis nicht angewandt worden. Sie sorgt immerhin dafür, dass außereuropäische Unternehmen sich nicht darauf verlassen können, dass sie einer effektiven Datenschutzkontrolle entgehen, weil die Aufsichtsbehörden sich nicht über ihre Zuständigkeit einigen können. Auch derartige Kompetenzkonflikte werden künftig vom Europäischen Datenschutzausschuss geklärt. Dieser hat bisher im sog. Kohärenzverfahren bereits zahlreiche Stellungnahmen abgegeben, die in erster Linie der Vereinheitlichung der nationalen Anforderungen an Datenschutzfolgeabschätzungen dienen.

Kampf dem *Forum Shopping*

Kein Datenverarbeiter kann sich „seine" Aufsichtsbehörde einfach aussuchen. Es war ein wesentliches Anliegen des Unionsgesetzgebers, dieses Prinzip in der Grundverordnung zu verankern. Deshalb wird die Zuständigkeit der Datenschutzbehörden nach objektiven, justiziablen Kriterien bestimmt, nämlich in welcher Niederlassung eines multinational agierenden Unternehmens über die Mittel und Zwecke der Datenverarbeitung entschieden wird.[22] Dies war schon ausschlaggebend für die Entscheidung der

französischen Datenschutzkommission im Fall *Google* (s.o.). Allerdings verändern Unternehmen ihre Struktur und verlagern dabei – ebenfalls wie im *Google*-Beispiel – Verantwortlichkeiten von einem EU-Mitgliedstaat in einen anderen. Dabei mag auch die Überlegung eine Rolle spielen, wie man einer zu strikten Datenschutzkontrolle aus dem Weg gehen kann (obwohl die Datenschutz-Grundverordnung gerade sicherstellen soll, dass der neue einheitliche Rechtsrahmen auch europaweit einheitlich angewandt wird). Deshalb hat sich der Europäische Datenschutzausschuss mit der Frage auseinandergesetzt, welche Folgen die Verlagerung einer verantwortlichen Niederlassung während eines laufenden datenschutzrechtlichen Prüfverfahrens für die Zuständigkeit hat.[23] Nach Auffassung des Ausschusses soll die Zuständigkeit im Rahmen eines begonnenen Prüfverfahrens auf die Aufsichtsbehörde des neuen Sitzstaates übergehen, wenn die datenschutzrechtliche Verantwortlichkeit objektiv auf eine Niederlassung in diesem Staat verlagert worden ist. Auch wenn der Ausschuss betont, dass ein *forum shopping* auch in solchen Situationen verhindert werden muss, ermöglicht es diese Festlegung gleichwohl, dass sich Unternehmen einer unbequemen Datenschutzkontrollinstanz entziehen und den Versuch unternehmen können, eine mildere Aufsichtsbehörde zu finden. Natürlich können Unternehmen nicht aus Gründen der Datenschutzkontrolle an Umstrukturierungen gehindert werden. Es wäre aber ebenso möglich und ein wirksameres Mittel gegen *forum shopping* gewesen, nach dem Vorbild der europäischen Strafverfolgungszusammenarbeit über *EUROJUST* die Zuständigkeit für ein einmal begonnenes Prüfverfahren bei der Behörde zu belassen, die es eingeleitet hat.[24]

Der Europäische Datenschutzausschuss – der Motor kommt auf Touren

Der neu geschaffene Europäische Datenschutzausschuss konnte 2018 an die Arbeit der Art. 29-Gruppe anknüpfen, hat allerdings einen wesentlich umfangreicheren Katalog von Aufgaben übertragen bekommen.[25] Er hat zwar keine zentralen Funktionen bei der Rechtsdurchsetzung auf europäischer Ebene (abgesehen von der Befugnis zur verbindlichen Streitentscheidung), aber durchaus zentrale Bedeutung bei der Harmonisierung der Rechtsanwendung unter den nationalen Datenschutzbehörden. Dafür steht ihm ein Arsenal von Mitteln des *soft law* wie Richtlinien, Empfehlungen und bewährte Verfahren zur Verfügung, das er bisher ausschließlich im Bereich der Grundverordnung einsetzt. Die ihm zustehenden entsprechenden Befugnisse im Bereich von Justiz und Polizei nach der Richtlinie von 2016 hat er bisher noch nicht genutzt, aber angekündigt, dies noch 2020 tun zu wollen.

Der Datenschutzausschuss agiert zunehmend auch mit erheblicher Flexibilität, um zu aktuellen Themen Stellung nehmen zu können, wie dies auch die Art. 29-Gruppe getan hat. Vor Ausbruch der Corona-Pandemie tagte der Ausschuss monatlich, während der Pandemie hat der Ausschuss virtuell teilweise wöchentlich getagt und dabei zu konkreten Fragen etwa der datenschutzgerechten Gestaltung und europaweiten Kompatibilität von Corona-Tracing-Apps Stellung genommen. Zudem hat er z.B. eine

Task Force zum einheitlichen Umgang mit *TikTok* gebildet. Insgesamt zeichnet sich ab, dass der Europäische Datenschutzausschuss zu einem Motor der datenschutzpolitischen Entwicklung in Europa werden kann, wenn er die richtigen Prioritäten setzt und die von der Grundverordnung bereitgestellten Instrumente klug einsetzt.

Wichtig ist auch die Weiterentwicklung des vom verstorbenen Europäischen Datenschutzbeauftragten Buttarelli ins Leben gerufenen *Digital Clearinghouse* aller europäischen Regulierungsbehörden, in dem Datenschutzbehörden mit Kartell- und Verbraucherschutzbehörden zusammenarbeiten. Freiheitsbeschränkende Marktmacht manifestiert sich zunehmend auch im Zugriff auf Nutzerdaten, wie der Bundesgerichtshof in Deutschland anerkannt hat.[26]

Evaluation durch die Kommission

Die Europäische Kommission hat im Juni 2020 ihren ersten Evaluationsbericht zur Anwendung der Datenschutz-Grundverordnung vorgelegt.[27] Darin zieht sie insgesamt eine positive erste Zwischenbilanz für das neue europäische Datenschutzgesetz. Allerdings weist sie auch auf Schwächen in der Kooperation zwischen den Datenschutzbehörden in Europa hin, ohne einzelne Behörden zu kritisieren. So sei die Entwicklung einer „*gemeinsamen europäischen Datenschutzkultur unter den Aufsichtsbehörden*" ein noch nicht abgeschlossener Prozess. Diese hätten die Möglichkeiten der Grundverordnung zur Zusammenarbeit noch nicht voll ausgeschöpft. Tatsächlich haben die Datenschutzbehörden seit dem Inkrafttreten der Grundverordnung noch keine gemeinsamen europaweiten Prüfungen durchgeführt, die vor 2018 immerhin dreimal stattgefunden haben.[28] Ein wesentliches Hindernis bei der Zusammenarbeit ist offenbar auch die mangelnde Harmonisierung des Verwaltungsverfahrens in den einzelnen Mitgliedstaaten. Das reicht von fehlenden Fristen für die maximale Dauer von Verfahren bis hin zu der Frage, in welchem Umfang personenbezogene Daten auf europäischer Ebene veröffentlicht werden dürfen. Gerade die zuletzt genannte Differenz zwischen den einzelnen Mitgliedstaaten wurde deutlich, als der Datenschutzausschuss ein Register der bisher gefällten Entscheidungen der nationalen Aufsichtsbehörden im One-Stop-Shop-Verfahren veröffentlichte.[29] Während darin aufgrund von innerstaatlichem Recht Entscheidungen einzelner Aufsichtsbehörden (darunter auch der Landesdatenschutzbeauftragten von Mecklenburg-Vorpommern, Niedersachsen und Nordrhein-Westfalen) entweder in Teilen oder überhaupt nicht (nicht einmal anonymisiert) veröffentlicht werden dürfen, werden andererseits die Entscheidungen der kroatischen Datenschutzbehörde mit vollem Personenbezug veröffentlicht, was mit dem Datensparsamkeitsgrundsatz der Grundverordnung nicht vereinbar sein dürfte.

Konkrete Änderungsvorschläge für die Grundverordnung hat die Kommission bei dieser ersten Evaluation nicht gemacht, obwohl etwa die deutschen Datenschutzbehörden solche durchaus vorgeschlagen hatten. Für die Zurückhaltung der Kommission spricht zum einen, dass der Zeitraum seit dem Inkrafttreten des neuen Rechtsrahmens noch relativ kurz war, zum anderen bei dessen Novellierung immer auch damit zu rechnen ist, dass dies von interessierter Seite etwa der Wirtschaft, aber auch von

den Mitgliedstaaten, dazu genutzt wird, um das einmal erreichte Datenschutzniveau wieder abzusenken.

Fazit

Die Verabschiedung der Datenschutz-Grundverordnung bedeutete zweifellos einen wesentlichen Fortschritt bei der Stärkung der informationellen Selbstbestimmung in der Europäischen Union, der auch auf außereuropäische Länder ausstrahlte, wie etwa der neue kalifornische *Consumer Privacy Act* verdeutlicht. Die Bedeutung dieses europäischen Datenschutzgesetzes im Zeitalter des Überwachungskapitalismus (Shoshana Zuboff) steht und fällt aber mit seiner koordinierten und sichtbaren Durchsetzung. Dafür ist die Kooperation zwischen den Datenschutzbehörden in Europa von entscheidender Bedeutung. Wenn es nicht gelingt, die Verzögerungen im Umgang mit großen außereuropäischen Unternehmen, die den europäischen Markt mit ihren Angeboten beherrschen, zu beseitigen und schneller abgestimmt auf Rechtsverstöße zu reagieren (z.B. durch Eilmaßnahmen einzelner Aufsichtsbehörden), dann muss die Europäische Kommission schon vor der nächsten Evaluation 2024 Änderungen der Grundverordnung (z.B. durch Fristen für die federführende Behörde oder eine zentralisierte Federführung auf Unionsebene) einleiten, um das Verfahren effektiver zu gestalten. Auch müssen die nationalen Verwaltungsverfahren stärker harmonisiert und dem Vorrang der Vorschriften der Grundverordnung zur Geltung verholfen werden.

Die Europäische Kommission hat im Sommer 2020 erstmals auch die Möglichkeit von Vertragsverletzungsverfahren gegen Mitgliedstaaten angedeutet, die ihre Aufsichtsbehörden unzureichend ausstatten. Es ist außerdem zu hoffen, dass der Europäische Datenschutzausschuss seine Rolle als Motor der europäischen Datenschutzkontrolle noch stärker als bisher wahrnimmt. Schließlich hat die Auseinandersetzung zwischen Max Schrems und der irischen Datenschutzbehörde verdeutlicht, welche wichtige Funktion engagierte Betroffene und zivilgesellschaftliche Organisationen bei der Durchsetzung des Datenschutzrechts in Europa haben.

DR. ALEXANDER DIX ist stellv. Vorsitzender des Vorstandes der Europäischen Akademie für Informationsfreiheit und Datenschutz in Berlin; war von 2005 bis 2016 Berliner Beauftragter für Datenschutz und Informationsfreiheit und bis 2015 Vertreter der Bundesländer in der Art. 29-Gruppe.

Anmerkungen:

1 Art. 30 Abs. 1 lit. a Richtlinie 95/46/EG
2 § 38 Abs. 5 BDSG aF
3 Art, 56, 60 DS-GVO
4 Art. 77 DS-GVO
5 Art. 79 Abs. 2 S. 2 DS-GVO
6 Art. 68, 69 DS-GVO
7 Art. 75 DS-GVO
8 Art 65, 66 DS-GVO
9 S. https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf (zuletzt abgerufen am 3.7.2020)
10 EuGH, Urt. v. 6.10.2015, Rechtssache C-362/13 (Schrems I)
11 Vgl den Offenen Brief von noyb v. 25.5.2020, https://noyb.eu/sites/default/files/2020-05/Open%20Letter_noyb_GDPR.pdf (zuletzt abgerufen am 6.7.2020)
12 EuGH, Urt. v. 16.7.2020, Rechtssache C-311/18 (Schrems II)
13 S.https://www.dataprotection.ie/en/irish-dpc-submits-article-60-draft-decision-inquiry-twitter-international-companys-compliance (zuletzt abgerufen am 6.7.2020)
14 Die Entscheidungen sind auf der Webseite des Europäischen Datenschutzausschusses veröffentlicht: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en (zuletzt aufgerufen am 7.7.2020)
15 S. https://www.independent.ie/business/technology/data-protection-commissioner-signals-block buster-fines-for-multinationals-on-the-way-38972780.html (zuletzt aufgerufen am 8.7.2020)
16 Evaluationsbericht der Europäischen Kommission v. 24.6.2020, Data protection as a pillar of citizen's empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, COM (2020) 264 final, 6
17 Art. 78 Abs. 2 DS-GVO
18 Art 60 Abs. 3 DS-GVO
19 Art. 64 Abs. 2 DS-GVO
20 Art. 60 Abs. 11, Art. 66 DS-GVO
21 Art. 65 DS-GVO
22 Art. 56 i.V.m. Art. 4 Nr. 16 DS-GVO
23 Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment, 9.7.2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201908_changeofmainorsingleestablishment_en.pdf (zuletzt aufgerufen am 10.7.2020)
24 Svantesson, European Data Protection Law Review 2020, 98, 100 f.
25 Art. 70 DS-GVO
26 Beschluss v 23.6.2020, KVR 69/19
27 Communication from the Commission to the European Parliament and the Council, Data Protection as a pillar of citizens' empowerment and the EU's approach to digital transition – two years of application of the General Data Protection Regulation, COM (2020) 264 final
28 Vgl. die von der Art. 29-Gruppe veröffentlichten Arbeitspapiere (Working Papers) 137 (2007), 172 (2010) und 229 (2015)
29 S. https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en (zuletzt aufgerufen am 10.7.2020).