Datenschutz in Hessen und Europa

Prof. Dr. Dr. h.c. Thomas von Danwitz, D.I.A.P. (ENA, Paris)
Richter am Gerichtshof der Europäischen Union, Luxemburg

Sehr geehrte Frau Landtagspräsidentin,
sehr geehrte Frau Ministerin,
sehr geehrter Herr Datenschutzbeauftragter,
sehr geehrte Damen, meine Herren,

gerne bin ich Ihrer freundlichen Einladung, sehr geehrter Herr Roßnagel, gefolgt und freue mich, an dieser Festveranstaltung zu „50 Jahre Datenschutz: in Hessen und Europa“ teilnehmen zu dürfen. Es ist eine große Ehre und Freude, mit diesem Festvortrag an der Würdigung des bedeutsamen Anteils, den das Land Hessen an der Entwicklung des Datenschutzrechts in Deutschland und Europa hat, mitwirken zu können. Wie von meinen Vorrednerinnen schon zu Recht hervorgehoben wurde, hat das Land Hessen am 7.10.1970 das erste Datenschutzgesetz der Welt erlassen und kann daher mit Fug und Recht seine Urheberschaft und Vorreiterrolle in einem Rechtsgebiet beanspruchen[1], das sich über die vergangenen 50 Jahre von einer eher exotischen Nischenmaterie zu einer zentralen Fragestellung der Abgrenzung hoheitlicher Eingriffsbefugnisse von privater Freiheit und gesellschaftlicher Autonomie sowie und vielleicht sogar zuvörderst zwischen Wirtschaftsteilnehmern und Verbrauchern entwickelt hat. Zugleich ist diese Veranstaltung eine willkommene Gelegenheit, die Entwicklung des Datenschutzes von seinem mitgliedstaatlichen Ursprung bis zu seiner aktuellen europäischen Ausgestaltung beleuchten zu können. Dem Anlass dieser Festveranstaltung gemäß bietet sie sich vor allem an, um über Wert und Wertungen des Datenschutzrechts nachzudenken, seinem inneren Kompass nachzuspüren und die Ausrichtung des Datenschutzrechts angesichts der aktuellen Herausforderungen zu würdigen.

I.

Nimmt man den Text des Datenschutzgesetzes vom 7.10.1970 sowie die über seine Genese Auskunft gebenden Berichte der Lesungen des Hessischen Landtags vom 8. Juli und vom 30. September 1970 und den Ersten Tätigkeitsbericht des Datenschutzbeauftragen vom 29. März 1972 zur Hand, so ist man selbst als mit der Materie vertrauter Leser erstaunt über die bis heute unveränderte Aktualität der damaligen Ausführungen, vor allem aber über die Deutlichkeit des politischen Willens, der seinerzeit im Landtag artikuliert wurde und sich auf eine breite überparteiliche Übereinstimmung stützen konnte. Die von der Landesregierung 1970 mit der Vorlage des Gesetzentwurfs verfolgten Ziele *erstens* die Privatsphäre des Bürgers zu schützen, *zweitens* die Datenbestände vor unberechtigten Zugriffen zu schützen und *drittens*

den Parlamenten trotz dieses Schutzes Zugang zu den gespeicherten Informationen zu gewähren[2], erscheinen heute noch so aktuell wie vor 52 Jahren. Gleiches gilt insbesondere für die Aussage des damaligen Ministerpräsidenten *Osswald*, dass die hessische Landesregierung den Einzug der elektronischen Datenverarbeitung in die öffentliche Verwaltung seit Jahren intensiv gefördert, aber es zugleich als Ihre Aufgabe angesehen habe, „alles zu tun, damit die wachsende Technisierung das Verhältnis des Bürgers zu seiner Verwaltung nicht stört und die Fortentwicklung der Demokratie nicht beeinträchtigt". Er fuhr fort: „Die Befürchtungen hinsichtlich des ‚Großen Bruders Computer', vor allem mit dem Blick auf die Überwachung der Privatsphäre des Bürgers, sind bekannt. Wir können heute nicht mit Bestimmtheit sagen, solche Befürchtungen seien grundlos. Wir müssen aber alles Mögliche tun und unternehmen, um vermeidbare Gefahren, die die elektronische Datenverarbeitung für Bürger, Regierung und Verwaltung mit sich bringt, von vornherein auszuschließen"[3].

Der damalige Vorsitzende des Rechtsausschusses, der Abgeordnete und spätere Vorsitzende seiner Fraktion *Milde*, begründete deren Zustimmung zur Vorlage des Datenschutzgesetzes unter Bezugnahme auf die Befürchtung, „ […] dass [eines Tages] jedermann karteimäßig erfasst wird und dass der Kunde einer zentralen Auskunftsstelle auf Anhieb die Wesensmerkmale, frühere und gegenwärtige Betätigungen, Geschmacksrichtungen und Wünsche eines jeden erfahren kann" und führte dazu aus: „[W]ir müssen bei den Dingen, die hier auf uns zukommen, sehr vorsichtig sein. Der Hinweis auf den Großen Bruder George Orwells darf nicht ein etwas ironischer Hinweis sein, sondern wir müssen ihn außerordentlich ernst nehmen. Ein Informationssystem unterliegt nämlich wie jede technische Neuerung dem Gesetz einer autonomen Entwicklung"[4].

1.

Im ersten Tätigkeitsbericht des hessischen Datenschutzbeauftragten vom März 1972 wird die Aufgabe des Datenschutzes mit einer für diese Zeit außergewöhnlichen Klarsichtigkeit einerseits dahingehend umschreiben: „Es liegt im Interesse des einzelnen Bürgers wie der Gemeinschaft, dass der Verwaltung für ihre Entscheidungen möglichst umfassende Informationen zur Verfügung stehen[5]. Andererseits bedroht diese Technik die freie und unkontrollierte Entfaltungsmöglichkeit des Menschen durch Einblicke in seine Privatsphäre und durch die Möglichkeiten der Manipulation mit den so gewonnenen Informationen. Wenn auch […] ein Wunderglaube an den Computer verfehlt wäre, so dürfen doch die Missbrauchsmöglichkeiten eines derartigen technischen Systems nicht unterschätzt werden. Es ist auch ein Instrument staatlicher Machtausübung und birgt die Verlockung in sich, es so umfassend, wie die Technik es ermöglicht, zu gebrauchen. Dabei können leicht die Schranken überschritten werden, welche die Grundrechte und die demokratischen Prinzipien des Staates ziehen"[6]. Mit dieser Orientierung entsprach das hessische Datenschutzrecht den Grundsätzen, die das BVerfG in seinem Beschluss zum Mikrozensus von 1969 bereits vorgezeichnet hatte[7].

2.

Angesichts der so umrissenen Aufgabenstellung sah das hessische Datenschutzgesetz von 1970 eine Reihe von Bestimmungen vor, die bis heute zum Kernbestand des Datenschutzes gehören. Zu nennen sind namentlich das Datengeheimnis und ein Individualanspruch auf Datenschutz, der situationsabhängig auf Berichtung, Restitution oder Unterlassung gerichtet sein kann[8]. Ebenso vorbildhaft in diesem Gesetz sind das Recht eines Jedermann auf Anrufung des Datenschutzbeauftragten, dessen Weisungsfreiheit sowie seine jährliche Berichterstattung gewesen[9]. Vor allem aber hat sich das Datenschutzgesetz Hessens als Katalysator für andere Bundesländer, namentlich in Rheinland-Pfalz, Nordrhein-Westfalen und Hamburg, erwiesen sowie für das Bundesdatenschutzgesetz und die noch in den 70er Jahren erlassenen Datenschutzgesetze in Schweden und Frankreich[10]. Dennoch war den Beteiligten 1970 bei Verabschiedung des hessischen Datenschutzgesetzes bereits bewusst, dass die „weitere Entwicklung möglicherweise zur Überarbeitung dieser Vorschriften zwingen wird“[11].

Wie wir heute wissen hat die im Jahre 1970 nicht vorhersehbare Revolutionierung der technologischen Möglichkeiten und namentlich die Digitalisierung ganzer Lebensbereiche, die seither stattgefunden hat, die Notwendigkeit des Datenschutzes allgemein im Bewusstsein der Öffentlichkeit verankert und weitreichende Entwicklungen ausgelöst. Aus heutiger Perspektive ist es jedoch überaus interessant anhand der Gesetze vom 31. Januar 1978 und vom 11. November 1986[12] festzustellen, dass Hessen seine Vorreiterrolle im Datenschutz auch in der Folgezeit nicht vernachlässigt hat. So enthielt bereits das Datenschutzgesetz von 1978 eine spezifische Regelung, nach der eine solche Verarbeitung „nur“ zulässig ist, wenn das Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat[13]. Ebenso wegweisend war die weitere Ausgestaltung der Rechte von Betroffenen, denen ein Recht auf Auskunft und Berichtigung, auf Sperrung und Löschung der zu seiner Person gespeicherten Daten sowie auf Anrufung des Datenschutzbeauftragten zuerkannt wurde[14]. Zudem sind – um es in der heute üblichen Terminologie zu sagen – Datenverarbeitungen seit dem Datenschutzgesetz von 1978 in Hessen nur zulässig, wenn diese zur rechtmäßigen Aufgabenerfüllung erforderlich sind[15]. Zu nennen sind sodann die Bestimmungen über die Zulässigkeit der Datenübermittlung innerhalb des öffentlichen Bereichs und an Stellen außerhalb der öffentlichen Verwaltung[16].

Entsprechend seiner Vorreiterrolle hat Hessen den Quantensprung, den der Datenschutz mit dem Urteil des BVerfG zum Volkszählungsgesetz von 1983[17] vollzogen hatte, als erstes Bundesland legislatorisch nachvollzogen, während vor allem der Bundesgesetzgeber auf diese Entwicklung ausgesprochen zögerlich reagierte und das novellierte BDSG erst 1990 verabschiedete[18]. Zu den wichtigsten Neuerungen des Hessischen Datenschutzgesetzes vom 11. November 1986 gehört aus heutiger Sicht fraglos der Grundsatz der Bindung der Datenverarbeitung an den Zweck, für den sie erhoben oder gespeichert wurden, die Bestimmung über automatisierte Abrufverfahren und das Recht Betroffener auf Schadensersatz sowie schließlich

die ins Detail gehenden Regelungen über die Rechtsstellung und die Befugnisse des Hessischen Datenschutzbeauftragten – bis hin zu seiner Personal- und Sachausstattung[19].

Zusammenfassend lässt sich diese frühe Ausformung des hessischen Datenschutzrechts aus heutiger Sicht nicht anders bezeichnen als die einer wegweisenden Rechtsentwicklung, die auf dem notwendigen Gleichlauf von technologischer und rechtlicher Innovation, der Notwendigkeit eines effektiven Grundrechtsschutzes und der Gewährleistung eines ausgewogenen Gleichgewichts der sich im Datenschutz gegenüberstehenden Interessen beruht; denn diese Orientierung ist zum Schutz der Funktionsbedingungen einer freiheitlichen Demokratie geboten. Sicherlich ist diese Entwicklung auch und vielleicht vor allem der glücklichen Fügung geschuldet, dass Regierung, Parlament und Verwaltung in Hessen den Datenschutz nicht zum symbolträchtigen Gegenstand politischer Auseinandersetzung gemacht haben und die hessischen Datenschutzbeauftragten ihr Amt mit besonderer Sachkunde, großer Umsicht und nachhaltigem Engagement wahrgenommen haben. Auf diese Weise war in Hessen bereits vor der „Europäisierung" des Datenschutzrechts durch die Datenschutzrichtlinie 95/46[20] ein modernes Datenschutzrecht entstanden, das als Inspiration und sogar als „benchmark" für den Unionsgesetzgeber dienen konnte.

II.

Mit der Vollendung des europäischen Binnenmarktes wurde eine europäische Regelung des Datenschutzes zu einer praktischen Notwendigkeit, zumal die in den 90er Jahren einsetzende Digitalisierung der Wirtschaft den Datenschutz aus einer primär hoheitlichen Regelungsperspektive löste und seine Beachtung zu einem auch und vor allem im Wirtschaftsverkehr unter Privaten zu beachtenden Anliegen machte. Wie bereits der zweite Erwägungsgrund der Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr betonte, stehen „die Datenverarbeitungssysteme im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundreche und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialem Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen". Weiter heißt es in den Erwägungsgründen dieser Richtlinie, dass – angesichts der Fortschritte der Informationstechnik – die Verarbeitung und der Austausch dieser Daten beträchtlich erleichtert werde[21]. Insbesondere angesichts der großen Unterschiede, die zwischen den einzelstaatlichen Rechtsverschriften zum Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere in Bezug auf die Privatsphäre bestehen, sei ein gleichwertiges Schutzniveau für die Gewährleistung dieser Rechte und Freiheiten bei der Verarbeitung solcher Daten unerlässlich[22]. Die von der Datenschutzrichtlinie bezweckte Rechtsangleichung „darf" – wie der Unionsgesetzgeber programmatisch formulierte – nicht zu einer Verringerung des bereits garantierten Schutzes führen, „sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen"[23].

Im Anschluss an diese Richtlinie von 1995 erließ die Union – um nur die wichtigsten Rechtsakte zu nennen – die Richtlinie über den elektronischen Geschäftsverkehr 2000/31[24], die Richtlinie 2002/58 über den Schutz der Privatsphäre in der elektronischen Kommunikation[25] sowie die Richtlinie 2006/24 über die Vorratsdatenspeicherung[26], die der Gerichtshof 2014 für nichtig erklärte[27]. In einem zweiten Regulierungspaket folgten 2016 sodann die Datenschutzgrundverordnung 2016/679[28], durch die die Datenschutzrichtlinie 95/46 aufgehoben wurde, die sog. Polizei-Richtlinie 2016/680 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten[29] und die sog. PNR-Richtlinie 2016/681 über die Verwendung von Fluggastdatensätzen[30].

1.

Vor diesem Hintergrund wird man dem Unionsgesetzgeber wohl kaum Karenz auf dem Gebiet des Datenschutzes vorwerfen können. Dass die unionsrechtlichen Regelungen dieser Rechtsakte mitunter über viele Jahre dennoch oftmals nur eine geringe Wirkung auf das mitgliedstaatliche Recht und namentlich auf die Geschäftspraktiken der in voller Expansion befindlichen Internetbranche nehmen konnten, hat vielfältige Ursachen. Die im Schrifttum für die Digitalisierung bis 2015 auf den Begriff des „Kontrollverlusts“[31] gebrachte Entwicklung erklärt sich nur unzureichend mit der zunächst gleichsam fehlenden Wettbewerbsaufsicht über die innovativen Geschäftspraktiken der neuen Technologie. Vielmehr wurde die Richtlinie 95/46 mancherorts nur zögerlich in nationales Recht[32] umgesetzt, was auch aktuell für die sog. Polizeirichtlinie zu beobachten ist[33]. Zudem wird auf unzureichende Sanktionsrisiken für Verstöße gegen Datenschutzbestimmungen unter der Richtlinie 95/46 und eine unzureichende Ausstattung[34] bzw. Unabhängigkeit[35] der Datenschutzbeauftragten in bestimmten Mitgliedstaaten hingewiesen. Auch marktmächtige Unternehmen, deren Geschäftsmodell auf einer ebenso weitreichenden wie nachhaltigen Verarbeitung personenbezogener Daten beruht, dürften wenig Eigeninteresse an einer strikten Einhaltung der europäischen Datenschutzvorschriften gehabt haben. Ohne Beweis über diese Erklärungsversuche erheben zu wollen, kann jedoch festgehalten werden, dass die Bedeutung der Datenschutzrichtlinie 95/46 trotz interessanter Ansätze in der Rechtsprechung[36] über weite Strecken eher als „law in the books“ denn als „law in action“ zu sehen ist. So hat es bspw. bis in das Jahr 2017[37] – also 22 Jahre nach dem Erlass der Richtlinie im Jahr 1995 – gedauert, bevor der Gerichtshof erstmals zu einer so grundlegenden Frage wie den Anforderungen befragt wurde, die an das Vorliegen einer rechtswirksamen Einwilligung zu stellen sind.

Daher vermag es nicht zu verwundern, dass das Urteil des Gerichtshofs vom 8. April 2014 in der causa *Digital Rights Ireland* von Manchem in der juristischen Fachöffentlichkeit nicht nur als Weckruf verstanden worden ist, das europäische Datenschutzrecht nicht zu vernachlässigen, sondern als veritable Zeitenwende für die Bedeutung und Verbindlichkeit des europäischen Datenschutzrechts und darüber hinaus für die institutionelle Rolle des Gerichtshofes als Verfassungsgericht der Europäischen Union im Allgemeinen[38]. In der Tat hat der Gerichtshof

seit 2014 in den Rechtssachen *Schrems I* und *II* sowie zum PNR-Abkommen mit Kanada bzw. jüngst zur PNR-Richtlinie 2016/681 der Europäischen Union[39], vor allem aber zur Vertraulichkeit der elektronischen Kommunikation nach der E-Privacy-Richtlinie 2002/58 in den Rechtssachen *Tele2 Sverige*, *Ministerio Fiscal, La Quadrature du Net e.a.*, *Privacy International*, *Prokuratuur* und *Commissioner of An Garda Síochána* sowie jüngst in *SpaceNet* und *VD*[40] in dichter Abfolge ebenso grundlegende wie weitreichende Entscheidungen zum europäischen Grundrechtsschutz auf dem Gebiet der Datenverarbeitung treffen können. Als Berichterstatter in den meisten dieser Rechtssachen bin ich vielleicht nicht der objektivste Beobachter, kann aber einige Erläuterungen zu dieser Rechtsentwicklung geben, die sich aus der Außenperspektive nicht sogleich erschließen, und zwar ohne das Beratungsgeheimnis zu strapazieren.

2.

Jenseits aller mitunter erheblichen Unterschiede, welche die Sach- und Rechtsfragen kennzeichnen, die in diesen Verfahren gegenständlich waren, zieht sich die Notwendigkeit einer wirksamen Achtung der betroffenen Grundrechte, namentlich durch eine Abwägung der gegenläufigen Belange, wie ein roter Faden durch diese Urteile. Wie in diesen dokumentiert ist, hat sich der Gerichtshof dieser Aufgabe nicht aus eigenem Gutdünken gewidmet, sondern auf der Grundlage der einschlägigen Vorschriften des Primär- und des Sekundärrechts der Union, aus denen sich ergibt, dass die Union ein hohes Schutzniveau für alle Personen auf Achtung des Privat- und Familienlebens einschließlich ihrer Kommunikation nach Artikel 7 und allgemein auf Schutz personenbezogener Daten nach Artikel 8 der mit dem Vertrag von Lissabon in Kraft getretenen Charta der Grundrechte gewährleistet. Die Charta der Grundrechte, die nach jahrzehntelangem Drängen des Europäischen Parlaments – und Anmahnung durch das BVerfG[41] – unter deutscher Präsidentschaft vom Europäischen Rat in Köln 1999 mit dem Ziel ins Werk gesetzt wurde, „die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern“[42], betont in diesem Zusammenhang in ihrer Präambel die Notwendigkeit, „angesichts der Weiterentwicklung der Gesellschaft, des sozialen Fortschritts und der wissenschaftlichen und technologischen Entwicklungen den Schutz der Grundrechte zu stärken“.

Indem das Recht auf Achtung des Privat- und Familienlebens nach Artikel 7 der Charta ausdrücklich die Kommunikation einer jeden Person schützt und der Schutz personenbezogener Daten nach Artikel 8 Abs. 1 unabhängig vom privaten oder gar sensiblen Charakter der Daten gewährleistet ist, Abs. 2 dieser Bestimmung die Datenverwendung beschränkt und ein Auskunftsrecht garantiert sowie Abs. 3 die Einhaltung dieser Vorschriften der Überwachung einer unabhängigen Stelle überantwortet, geht die Charta nach Inhalt und Präzision deutlich über die textlichen Vorgaben des Grundgesetzes und anderer nationalen Verfassungen hinaus. Ins-

besondere der Gewährleistungsgehalt von Artikel 8 beruht maßgeblich auf der Datenschutzrichtlinie 95/46, deren Grundsätze in Artikel 8 auf die Ebene des Primärrechts gehoben worden sind[43].

Dieser primärrechtliche Ausgangsbefund, der deutlich über die textlichen Vorgaben des Grundgesetzes hinausgeht, erfährt durch das einschlägige Sekundärrecht eine weitere Bestätigung. So ergibt sich aus der Entstehungsgeschichte der E-Privacy-Richtlinie 2002/58, dass der Unionsgesetzgeber einen hochgradigen Schutz personenbezogener Daten und der Privatsphäre erstrebt hat[44]. Der Erwägungsgrund 11 dieser Richtlinie sieht dementsprechend vor, dass Maßnahmen zum Schutz der öffentlichen Sicherheit in einem „strikt" angemessenen Verhältnis zum verfolgten Zweck stehen müssen[45]. Vor allem aber sieht Artikel 5 Abs. 1 dieser Richtlinie das grundsätzliche Verbot für jede andere Person als den Nutzer vor, Verkehrs- und Standortdaten elektronischer Kommunikation ohne dessen Einwilligung auf Vorrat zu speichern[46]. Angesichts der besonderen Bedeutung, die diesen Daten für den Schutz des Rechts auf Vertraulichkeit der Kommunikation und der Meinungsfreiheit zukommt, die wiederum für eine demokratische Gesellschaft konstitutiv ist[47], erscheint die vom Gerichtshof vorgenommene enge Auslegung der in Art. 15 Abs. 1 dieser Richtlinie vorgesehenen Befugnis zur Speicherung solcher Daten auf Vorrat keineswegs überraschend.

Denn im Unterschied zu den Daten über die zivile Identität der Kommunikationsteilnehmer liegt es in der Natur der Verkehrs- und Standortdaten elektronischer Kommunikation, dass selbst die Speicherung einer begrenzten Menge dieser Daten geeignet ist, präzise Informationen über das Privatleben eines Nutzers elektronischer Kommunikationsmittel zu verschaffen[48]. Angesichts der Auswirkungen einer solchen Maßnahme für die Wahrnehmung der Kommunikationsfreiheiten („chilling effects") und ihre Rückwirkungen auf die Funktionsbedingungen demokratischer Gesellschaften[49] bleibt für diese Rechtsprechung der vom Gerichtshof immer wieder betonte Umstand maßgeblich, dass die bisherigen Vorratsspeicherungen ohne Differenzierung, Einschränkung oder Ausnahme erfolgt sind und pauschal alle Nutzer elektronischer Kommunikationsmittel erfassten – also die Quasi-Gesamtheit der Bevölkerung – ohne dass diese Personen sich auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte[50]. In diesem Zusammenhang ist aber auch zu betonen, dass eine solche allgemeine und unterschiedslose Vorratsspeicherung allein derjenigen IP Adressen, die nur der Quelle einer Verbindung zugewiesen sind, insbesondere zur Bekämpfung von Kinderpornografie im Internet unter engen Voraussetzungen zulässig sein kann[51].

3.

Die Rechtsprechung zur Beurteilung des sog. „EU-US Datenschutzschildes", des PNR-Abkommens mit Kanada und der PNR-Richtlinie beruht auf normativen Grundlagen, die zu vergleichbaren Wertungen führen. So betont Erwägungsgrund 101 der DSGVO für Datenübertragungen in Drittländer – wie bereits im Kern aus der Richtlinie 95/46 folgte[52] –, dass das durch diese

Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen bei der Übermittlung personenbezogener Daten in Drittländer nicht untergraben werden sollte und Erwägungsgrund 104, dass das Drittland Garantien für ein angemessenes Schutzniveau bieten sollte, das dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist; das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und den betroffenen Personen sollten nach Artikel 45 Abs. 2 lit. a) DSGVO wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden. Angesichts des Vorbringens der Parteien und insbesondere der schriftlichen und mündlichen Erläuterungen der Regierung der USA zum amerikanischen Recht ist der Gerichtshof in der Rechtssache *Schrems II* zum Schluss gelangt, dass diese Vorschriften den Mindestvorgaben nicht genügen, die im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit einzuhalten sind und das amerikanische Recht in diesem Bereich zudem keine Garantien bietet, die der nach Artikel 47 der Charta erforderlichen Gewährleistung eines effektiven Rechtsschutzes der Sache nach gleichwertig wären[53].

In seiner jüngst verkündeten Entscheidung zur Gültigkeit und Auslegung der sog. PNR-Richtlinie 2016/681 hat der Gerichtshof angesichts der wiederholten Bezugnahmen der Erwägungsgründe der Richtlinie auf die vollständige Wahrung der Grundrechte, des Rechts auf Privatsphäre und den Grundsatz der Verhältnismäßigkeit[54] die operativen Bestimmungen dieser Richtlinie einer grundrechtskonformen Auslegung unterzogen, die erhebliche Beschränkungen der hoheitlichen Befugnisse zur Folge hat, die die Richtlinie vorsieht. Insbesondere kann das PNR-System nur im Hinblick auf terroristische Straftaten und auf schwere Kriminalität angewandt werden, die – zumindest mittelbar – in objektivem Zusammenhang mit der Beförderung von Fluggästen steht[55]. Daher können EU-interne Flüge dem PNR-System nur unterworfen werden, sofern es in dem betroffenen Mitgliedstaat hinreichend konkrete Umstände für die Annahme gibt, dass er mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist; ansonsten überschreitet die Anwendung dieses Systems das Maß des unbedingt Erforderlichen[56]. Des Weiteren hat der Gerichtshof die Auswertung der PNR-Daten in Bezug auf den Abgleich mit anderen Datenbanken strikten Beschränkungen unterworfen und insbesondere die kriterienbasierte Auswertung auf vorab festgelegte Kriterien beschränkt, unter Ausschluss selbstlernender Systeme[57]. Zudem müssen die Mitgliedstaaten präzise Regelungen treffen, um eine nichtdiskriminierende Anwendung des Systems und insbesondere die Kohärenz der individuellen Nachprüfungen zu gewährleisten[58]. Betroffene müssen zudem über angemessene Rechtsschutzmöglichkeiten verfügen, auch in Bezug auf die im Voraus festgelegten Prüfkriterien und im Hinblick auf die Funktionsweise der Programme, mit denen diese Kriterien angewandt werden[59]. Um die Angemessenheit des Systems zu gewährleisten, hat der Gerichtshof – anknüpfend an die Regelungen der Richtlinie – die Aufbewahrung der PNR-Daten aller Flugpassagiere auf prinzipiell 6 Monate beschränkt, es sei denn, dass objektive Anhaltspunkte im Einzelfall für das Fortbestehen einer von bestimmten Fluggästen in Bezug auf die Begehung terroristischer Straftaten und schwerer

Kriminalität ausgehenden Gefahr vorliegen, die eine Speicherung für einen Zeitraum von maximal fünf Jahre rechtfertigen können[60].

III.

Dass solche Erwägungen keineswegs revolutionär sind, sondern vielmehr ganz auf der Linie dessen liegen, was bereits vor 50 Jahren in Hessen als Anliegen des Datenschutzes formuliert wurde, zeigt ein Blick in den ersten Tätigkeitsbericht des hessischen Datenschutzbeauftragten von 1972. Im Hinblick auf das für 1973 in der ersten Ausbaustufe vorgesehene polizeiliche Informationssystem des Landeskriminalamtes, in dem auch Angaben über den bestehenden Verdacht der Begehung einer Straftat sowie Hinweise zur Charakterisierung der Persönlichkeit solcher Personen aufgenommen werden sollten, befand der Datenschutzbeauftragte, dass „[…] die sachliche Notwendigkeit, für die kriminalistische Tätigkeit auch Informationen über Fälle bloßen Verdachts, vermutete Eigenschaften und Verhaltensweisen bereitzustellen, […] nicht bestritten werden (soll). […] Andererseits greift dieses Informationssystem vom Inhalt der Daten her tief in das Persönlichkeitsrecht des Betroffenen ein, und zwar auch in den grundsätzlich unantastbaren Intimbereich. Der Aufbau und die Unterhaltung eines solchen Systems ist aus höherwertigen Interessen des Gemeinwohls nur dann zu rechtfertigen, wenn Weitergabe und Verwendung der Informationen so eng wie möglich geregelt sind und optimal wirksame Sicherungen gegen unberechtigte Kenntnisnahme und Verwendung bestehen“[61].

Die Rechtsprechung des Gerichtshofes stellt sich bei Lichte besehen als konsequente Fortschreibung der Wertungsgrundlagen dar, die bereits das hessische Datenschutzgesetz von 1970 geprägt hatten und dieser Rechtsmaterie seither Ausrichtung und Gestalt verliehen haben. Die moderne Ausprägung des Datenschutzrechts erklären indes drei weitere Faktoren. Mit der sog. Europäisierung des Datenschutzrechts geht naturgemäß einher, dass die Wertungsgesichtspunkte und -zusammenhänge, die in das europäische Datenschutzrecht Eingang gefunden haben, den gesamteuropäischen Kontext und die besonderen Funktionsbedingungen der Europäischen Union widerspiegeln. Der Unionsgesetzgeber ist dieser genuin europäischen Perspektive bei der Normsetzung ebenso verpflichtet wie der Gerichtshof bei der Auslegung dieser Vorschriften. Damit geht keineswegs eine Absage an nationale Besonderheiten einher, wohl aber die Notwendigkeit, bspw. das Maß des erforderlichen Schutzes, etwaige Missbrauchsrisiken und Unabhängigkeitserfordernisse sowie allgemein das Bestehen von Gefahrenlagen für die demokratische Gesellschaft in übergreifenden europäischen Zusammenhängen zu beurteilen.

Ganz in diesem Sinne sieht etwa die DSGVO vor, dass die unabhängigen Datenschutzbehörden der Mitgliedstaaten in die Arbeit des Europäischen Datenschutzausschusses (EDSA) eingebunden sind, der insbesondere zur Gewährleistung einer einheitlichen Anwendung der unionsrechtlichen Datenschutzvorschriften über eigene Entscheidungsbefugnisse verfügt. Hinzu

kommt, dass die erhobenen Datenmengen und ihre Verarbeitung in den vergangenen Jahrzehnten exponentiell gewachsen sind und Möglichkeiten der Datenverknüpfung und des Data-mining entstanden sind, die vor wenigen Jahren noch als bloße Science-Fiction erschienen. Solche Möglichkeiten, wie selbstlernende Systeme künstlicher Intelligenz sie bspw. darstellen, mögen heute für die effektive Erfüllung hoheitlicher Aufgaben zwar oftmals sinnvoll sein, sie lösen indes gleichsam spiegelbildlich elementare Bedürfnisse nach dem Schutz der Menschenwürde, der Kommunikationsfreiheiten in einer demokratischen Gesellschaft und eines effektiven Rechtsschutzes aus. Die Suche nach dem richtigen Weg zeugt daher von der ernsthaften Verantwortung des Gerichtshofes für die Einhaltung der in Artikel 2 EUV statuierten Werte und keineswegs für ein hypertrophes Grundrechtsverlangen derer, die vielleicht keine wirklichen Sorgen haben.

Ein weiterer grundlegender Unterschied gegenüber der Datenschutzperspektive der frühen 70er Jahren folgt schließlich aus der ökonomischen Entwicklung, die dazu geführt hat, dass personenbezogene Daten in großem Stil zur Handelsware geworden sind und dass kaum ein Unternehmen – auch der sog. Realwirtschaft – ohne nachhaltige Auswertung personenbezogener Daten arbeitet. Zudem ist schon seit geraumer Zeit eine Neujustierung von Angebot und Nachfrage zu beobachten, eine Entwicklung, die die US-amerikanische Wirtschaftswissenschaftlerin *Shoshana Zuboff* auf den Begriff des „surveillance capitalism“ also Überwachungskapitalismus[62] gebracht hat. Unter diesen Vorzeichen und angesichts der damit einhergehenden Schwierigkeiten, in Gesetzgebungsverfahren und Einzelfallentscheidungen jeweils zu einer Abwägung der konfligierenden Interessen im Sinne praktischer Konkordanz zu gelangen, die den grundrechtlich geschützten Interessen hinreichend Rechnung trägt, wächst der jeweils zuständigen Gerichtsbarkeit auf mitgliedstaatlicher wie auf europäischer Ebene eine besondere Verantwortung zu. Eine Gesamtschau dieser Entwicklungslinien hat den Gerichtshof daher veranlasst, das europäische Datenschutzrecht anknüpfend an die normtextlichen Vorgaben ganz in der Traditionslinie eines hochwertigen Datenschutzes auszulegen, die dieses Rechtsgebiet seit seinen Anfängen in Hessen geprägt hat.

Infolge der von der Europäischen Kommission aktuell vorgeschlagenen Neureglungen[63] in einer ganzen Reihe von spezifischen Bereichen des Datenschutzes und der Datenwirtschaft wird es in Zukunft fraglos zu einer stärkeren Ausdifferenzierung von Schutzbedürfnissen und Verarbeitungsmöglichkeiten kommen, wie bspw. die vorgeschlagenen Regelungen über künstliche Intelligenz einerseits und für Verarbeitung von Gesundheitsdaten andererseits erkennen lassen. Daher lässt sich die Diskussion der Zukunft nicht auf die allzu vereinfachende Gleichung von „mehr“ oder „weniger“ Datenschutz bringen. In Rechtsbereichen, in denen der Schutz personenbezogener Daten nennenswerte Auswirkungen auf die Ausübung hoheitlicher Befugnisse hat und erst recht in der Frage von wirtschaftlichen Nutzungsmöglichkeiten solcher Daten, auf denen ganze Geschäftsmodelle basieren, ist der sehr gemessene und nüchtern-abwä-

gende Tonfall der parlamentarischen Debatte des hessischen Landtags um das erste Datenschutzgesetz vor 50 Jahre leider mancherorts einer allzu aufgeregt-interessengeleiteten Diskussion gewichen. Natürlich haben auch solche Auseinandersetzungen ihre Berechtigung, obwohl sie leicht Gefahr laufen, die grundlegende Bedeutung des Datenschutzes für den notwendigen Schutz der Grundrechte und der Funktionsbedingungen einer pluralistischen Gesellschaft aus dem Auge zu verlieren, wie bereits ein Blick auf den Umgang mit persönlichen Daten zeigt, der in nichtdemokratischen Staaten in anderen Regionen der Welt vorherrscht.

Daher sollten wir uns auf der ständig neuen Suche nach praktischer Konkordanz der konfligierenden Interessen zwischen Datenschutz und Datennutzung nicht beirren lassen. Eine demokratische Gesellschaft, die den Bürger als *citoyen* ernst nimmt und – wie die Charta der Grundrechte es ausweislich ihrer Präambel tut – „den Menschen in den Mittelpunkt ihres Handelns (stellt)", verwirklicht sich im Zeitalter der Digitalisierung auch und vor allem durch einen hochwertigen Datenschutz, der es dem Bürger ermöglicht, Institutionen des Staates und Wirtschaftsunternehmen gleichermaßen in freier Selbstbestimmung auf Augenhöhe zu begegnen.

---

1 Hessisches Datenschutzgesetz vom 7.10.1970, Hess. GVBl. I 1970, S. 625. Im Ersten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vom 29.3.1972, LT-Drs. 7/1495, S. 11 heißt es dazu: „Mit der Verabschiedung des Datenschutzgesetzes und der Einrichtung der Institutionen des Datenschutzbeauftragten betrat Hessen juristisches ‚Neuland'. Es gibt keine vergleichbare Einrichtung."

2 Siehe die Begründung zum Entwurf der Landesregierung für ein Datenschutzgesetz, LT-Drs. Nr. 3065, S. 7 sub. 1.1.

3 So die die Ausführungen von Ministerpräsident *Osswald* (SPD), Stenographischer Bericht der 77. Sitzung des Hessischen Landtags, 6. Wahlperiode vom 8.7.1970, S. 4057.

4 So der Abg. *Milde* (CDU), Stenographischer Bericht der 77. Sitzung des Hessischen Landtags, 6. Wahlperiode vom 8.7.1970, S. 4058. Zustimmend äußerte sich auch der Abg. Stein (F.D.P.), ebenda, S. 4060 f.

5 Erster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vom 29.3.1972, LT-Drs. 7/1495, S. 7.

6 Ebenda, S. 8.

7 So BVerfGE 27, 1 (6) - Mikrozensus.

8 Siehe §§ 3 und 4 des Hess. Datenschutzgesetz vom 7.10.1970.

9 Vgl. dazu in der o.g. Reihenfolge §§ 11, 8 und 14 des Hess. Datenschutzgesetzes vom 7.10.1970.

10 *Dammann/Mallmann/Simitis*, Gesetzgebung zum Datenschutz, 1977, S. 54 ff.

11 So die Begründung zum Entwurf der Landesregierung für ein Datenschutzgesetz, LT-Drs. Nr. 3065, S. 8 sub. 1.7; dazu auch *Stephan Schindler*, 50 Jahre Datenschutz in Hessen, ZD-Aktuell 2020, 07388.

12 Hess. Datenschutzgesetz vom 31.1.1978, Hess. GVBl. I 1978, S. 96; Hess. Datenschutzgesetz vom 11.11.1986, Hess. GVBl. I 1986, S. 309.

13 Jeweils § 7 des Hess. Datenschutzgesetzes vom 31.1.1978 und des Hess. Datenschutzgesetzes vom 11.11.1986.

14 §§ 18, 19 und 27 des Hess. Datenschutzgesetzes vom 31.1.1978 sowie §§ 18, 19 und 28 des Hess. Datenschutzgesetzes vom 11.11.1986.

15 Jeweils § 11 des Hess. Datenschutzgesetzes vom 31.1.1978 und des Hess. Datenschutzgesetzes vom 11.11.1986.

16 §§ 12 und 16 des Hess. Datenschutzgesetzes vom 31.1.1978 sowie §§ 14 und 16 des Hess. Datenschutzgesetzes vom 11.11.1986.

[17] BVerfGE 65, 1 - Volkszählung.

[18] Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990, BGBl. I 2000, S. 2954.

[19] §§ 13, 20 sowie §§ 21 bis 31 des Hess. Datenschutzgesetzes vom 11.11.1986.

[20] Richtlinie 95/46 vom24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23.11.1995, S. 31.

[21] Erwägungsgründe 4 und 6 der Richtlinie 95/46.

[22] Ebenda, Erwägungsgründe 7 und 8 der Richtlinie 95/46.

[23] Erwägungsgrund 11, Satz 2 der Richtlinie 95/46.

[24] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17.7.2000, S. 1.

[25] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

[26] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54.

[27] EuGH, 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238.

[28] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

[29] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89.

[30] Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119 vom 4.5.2016, S. 132.

[31] Siehe *Seemann*, Die Geschichte der Digitalisierung in fünf Phasen – mit der narratologischen Rampe in die Digitalisierung, in: Stiftung Genshagen „Virtuell, vernetzt, analog. Beiträge und Ausblicke“ (2020), S. 26 (28).

[32] Siehe dazu die Angaben zu den Umsetzungsfristen für die Richtlinie 95/46 und den in den einzelnen Mitgliedstaaten erlassenen Umsetzungsakten auf der Internetseite https://eur-lex.europa.eu/legal-content/DE/NIM/?uri=celex:31995L0046 (zuletzt eingesehen am 9.9.2022). In Deutschland erfolgte die Umsetzung unter Überschreitung der dreijährigen Umsetzungsfrist erst nach Erhebung eines Vertragsverletzungsverfahrens im Jahre 2001 durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.5.2001 (BGBl. I 2001, S. 904), vgl. dazu Gola/Klug, NJW 2001, 3747 (3748).

[33] Siehe dazu die Angaben zu den Umsetzungsfristen für die Richtlinie 2016/680 und den in den einzelnen Mitgliedstaaten erlassenen Umsetzungsakten auf der Internetseite https://eur-lex.europa.eu/legal-content/DE/NIM/?uri=CELEX:32016L0680&qid=1662732344440 (zuletzt eingesehen am 9.9.2022). Siehe auch EuGH, 25. Februar 2021, Kommission/Spanien (Richtlinie über personenbezogene Daten – Strafrechtlicher Bereich), C-658/19, EU:C:2021:138.

[34] Siehe zum Sanktionsregime: *Martini/Wagner/Wenzel*, Das neue Sanktionsregime der DSGVO – ein scharfes Schwert ohne legislativen Feinschliff, Teil 1, Verwaltungsarchiv, 2018, S. 163 (164), und zur Ausstattung der Datenschutzbeauftragten: *Selmayr,* in: *Ehmann/ders.*, DSGVO, 2. Aufl. 2018, Art. 52 Rn. 24 m.w.N. Siehe zudem

[35] Siehe dazu EuGH, 9. März 2010, Kommission/Deutschland, C-518/07, EU:C:2010:125; 16. Oktober 2012, Kommission/Österreich (C-614/10, EU:C:2012:631), sowie 8. April 2014, Kommission/Ungarn, C-288/12, EU:C:2014:237.

[36] Vgl. etwa EuGH, 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294; 6. November 2003, Lindqvist, C-101/01, EU:C:2003:596, sowie 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662.

[37] Siehe dazu EuGH, 1. Oktober 2019, Planet49, C-673/17, EU:C:2019:801, sowie 11. November 2020, Orange Romania, C-61/19, EU:C:2020:901.

[38] Siehe dazu *Kühling*, Der Fall der Vorratsdatenspeicherungs-RL und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, S. 681; *von Danwitz*, in: Grabenwarter (Hrsg.), Europäischer Grundrechtsschutz (EnzEuR Bd. 2), 2. Aufl. 2022, § 27 Rn. 17 (m.w.N. in Fn. 107), sowie *Benecke/ Spiecker genannt Döhmann*, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2. Aufl. 2022, § 23, Rn. 75 f. Eingehend dazu auch *Hijmans*, The European Union as Constitutional Guardian of Internet Privacy and Data Protection : The Story of Art 16 TFEU, 2016, S. 165 ff.

[39] EuGH, 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650; Gutachten 1/15 vom 26. Juli 2017, EU:C:2017:592; 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559 sowie 21. Juni 2022, Ligue des droits humains, C-817/19, EU:C:2022:491.

[40] EuGH, 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 und C-698/15, EU:C:2016:970; 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788; 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791; 6. Oktober 2020, Privacy International, C-623/17, EU:C:2020:790; 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation), C-746/18, EU:C:2021:152; 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258; 20. September 2022, SpaceNet und Telekom Deutschland, C-793/19 und C-794/19, EU:C:2022:702; 20. September 2022, VD, C-339/20, EU:C:2022:703.

[41] BVerfGE 37, 271 (285 und Leits.) – Solange I.

[42] Europäischer Rat in Köln, 3./4.6.1999, Schlussfolgerungen des Vorsitzes, Anhang IV, https://www.consilium.europa.eu/media/21062/57872.pdf (letzter Abruf am 12.9.2022).

[43] Siehe dazu die Erläuterungen zur Charta der Grundrechte, ABl. C 303 vom 14.12.2007, S. 17 (20); *Bernsdorff*, in: *Meyer/Hölscheidt* (Hrsg.), Charta der Grundrechte, 5. Aufl. 2019, Art. 8, Rn. 17.

[44] Siehe dazu EuGH, 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 36 m.w.N.

[45] EuGH, 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 51.

[46] Siehe dazu EuGH, 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 35, 39 und 47 sowie die dortigen Hinweise auf EuGH, 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791.

[47] EuGH, 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 42 und 43, unter Bezugnahme auf EuGH, 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 113 und 114.

[48] EuGH, 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation), C-746/18, EU:C:2021:152, Rn. 39, 40; SpaceNet Rn. 90, 91.

[49] EuGH, 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 141 und 142, 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 65.

[50] EuGH, 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 143 und 144, sowie 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 66.

[51] EuGH, 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 72 bis 74, unter Bezugnahme auf die in Rn. 154 und 155 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, genannten prozeduralen und materiellen Voraussetzungen.

[52] Siehe dazu EuGH, 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 68 bis 78.

[53] EuGH, 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 184 und 197.

[54] Siehe v.a. Erwägungsgründe 15, 20, 22, 25, 36 und 37 der PNR-Richtlinie 2016/681.

[55] EuGH, 21. Juni 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, Rn. 157.

[56] Ebenda, Rn. 171 bis 174.

[57] Ebenda, Rn. 194.

[58] Ebenda, Rn. 203 bis 205.

[59] Ebenda, Rn. 209, 210.

[60] Ebenda, Rn. 255 bis 260.

[61] Erster Tätigkeitsbericht des hessischen Datenschutzbeauftragten, LT-Drs. 7/1495 vom 29.3.1972, sub 4.1.1.3. c), S. 24.

[62] *Shoshana Zuboff,* Big other: Surveillance Capitalism and the Prospects of an Information Civilization, Journal of Information Technology, (2015) 30, S. 75, und *dies*., The Age of Surveillance Capitalism, 2019.

[63] Siehe dazu Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM(2020) 842 final; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz festgelegt werden (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.4.2021, COM(2021) 206 final; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) vom 23.2.2022, COM (202)68 final; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten vom 3.5.2022, COM(2022) 197 final. Siehe auch die auf Vorschlag der Kommission erlassene Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) (Text von Bedeutung für den EWR), ABl. L 152 vom 3.6.2022, S. 1, und die Verordnung (EU) 2022/991 des Europäischen Parlaments und des Rates vom 8. Juni 2022 zur Änderung der Verordnung (EU) 2016/794 in Bezug auf die Zusammenarbeit von Europol mit privaten Parteien, die Verarbeitung personenbezogener Daten durch Europol zur Unterstützung strafrechtlicher Ermittlungen und die Rolle von Europol in Forschung und Innovation, ABl. L 169 vom 27.6.2022, S. 1.