1. Die europäische Grundrechtecharta als internetvertrauensbildende Maßnahme in Bremen und Europa

Auch wenn es beim Umgang mit den flüchtenden Menschen leider nicht immer den Anschein hat, ist der eingebaute Antriebsmechanismus der Europäischen Union das Einreißen von Grenzen. Bei dem Ziel, Verkehrshemmnisse abzubauen, geht es nicht nur darum, dass sich Personen von nationalstaatlichen Grenzen ungehindert in Europa bewegen können. Auch Waren, Dienstleistungen und Beschäftigte sollen Grenzen überschreiten können, ohne dass hierfür Nachteile erwartet werden müssen. Der von der Europäischen Union eingeschlagene Weg ist dabei regelmäßig der, in allen Staaten durch den Erlass von Rechtsnormen einheitliche Verhältnisse herzustellen. Dadurch, dass überall in der Europäischen Union dasselbe Recht gilt, soll verhindert werden, dass Menschen, aber vor allem auch Unternehmen aus anderen Staaten der Europäischen Union schlechter oder besser behandelt werden als inländische Personen oder Unternehmen. Auch bei der Diskussion um den Datenschutz in Europa geht es um den Abbau von Verkehrshindernissen. Die Datenschutzgrundverordnung ist daher in Wirklichkeit keine "Datenschutz"-Grundverordnung, wie es die auch hier verwendete amtliche Abkürzung nahelegt. Der korrekte Titel lautet: "Verordnung (…) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten **und zum freien Datenverkehr**".

Sofern die betreffenden Grundrechtsbereiche wirtschaftliche Reflexe aufwiesen, konnte die primäre Wirtschaftsgetriebenheit der Europäischen Union in der Vergangenheit positive Nebeneffekte für Grundrechte erzeugen. So hängt das Außerkrafttreten von deutschen Gesetzen, die Frauen bezüglich ihres Arbeitsentgeltes diskriminierten, eng damit zusammen, dass Frankreich bereits auf die Frauendiskriminierung in diesem Bereich verzichtet hatte. Dies wurde jedoch als wirtschaftlicher Nachteil im Vergleich zu der Situation in anderen Staaten erlebt. Deshalb wirkte Frankreich darauf hin, dass die damalige Europäische Wirtschaftsgemeinschaft in Artikel 119 des Vertrages über die Europäischen Gemeinschaften den Grundsatz des gleichen Entgelts für Männer und Frauen bei gleicher Arbeit formulierte. Das ökonomische Ziel, in der Europäischen Gemeinschaft einen einheitlichen Frauendiskriminierungsgrad beziehungsweise Frauengleichstellungsgrad beim Entgelt zu erreichen, hätte auch erreicht werden können, indem Frankreich auf die Regelungen verzichtet hätte, die die Entgeltdiskriminierung von Frauen sanktionierten. Dass dieser Weg nicht beschritten wurde, sondern die anderen europäischen Länder verpflichtet wurden, Regelungen wie in Frankreich zu erlassen, zeigt, dass es zwei Voraussetzungen für grundrechtserweiternde Effekte von Entwicklungen auf europäischer Ebene gibt: Ein grundrechtsfreundlicher europäischer Konsens muss auf rechtliche Verpflichtungen treffen. In den 1970er Jahren sorgte der europäische Konsens, Frauendiskriminierungen in allen

Lebensbereichen abbauen zu wollen, dafür, dass europäische Regelungsverpflichtungen dafür genutzt wurden, das Niveau der Frauengleichstellung überall in Europa anzuheben.

Die Lage beim Datenschutz ist vergleichbar: Unternehmen, die die als besonders streng geltenden deutschen Datenschutzgesetze beachten müssen, betrachten dies als wirtschaftlichen Nachteil. Die Datenschutzgrundverordnung hat daher in der europäischen Logik vor allem das Ziel, alle Unternehmen, die in Europa agieren, gleich (aus Sicht der Lobby des freien Datenverkehrs: gleich schlecht) zu behandeln. Die wirtschaftsgetriebene europäische Diskussion um den Datenschutz, die im Frühjahr 2016 mit der Verabschiedung der Datenschutzgrundverordnung ihren vorläufigen Höhepunkt erreichen wird, wird also dann positive Nebeneffekte für die Datenschutzgrundrechte haben, wenn die beiden Voraussetzungen des flankierenden grundrechtsfreundlichen Diskurses und der bindenden rechtlichen Verpflichtung für die Verabschiedung von Regelungen mit einem hohen Datenschutzniveau gegeben sind.

1.1 Das gestiegene Bedürfnis nach internetvertrauensbildenden Maßnahmen

Die Menschen in Europa schätzen ihr Grundrecht auf informationelle Selbstbestimmung und beklagen den mangelnden Schutz personenbezogener Daten im Internet. 2015 ergab eine Umfrage des Deutschen Instituts für Vertrauen und Sicherheit im Internet, dass zwar fast alle Internetnutzerinnen und Internetnutzer in Deutschland zumindest gelegentlich im Netz einkaufen. Doch die Mehrheit von ihnen (54 Prozent) hat solche Einkäufe bereits aufgrund von Sicherheitsbedenken abgebrochen. Die meisten Befragten nennen die mangelnde Sicherheit persönlicher Daten sowie den unsicheren Online-Zahlungsverkehr als größte Probleme. Dabei liegt es am Fehlen alternativer Angebote, dass trotz der vorhandenen Sicherheitsbedenken online bestellt wird. Nach einer im November 2015 veröffentlichten Umfrage des Bundesverbandes der Verbraucherzentralen ist die Bereitschaft der Verbraucherinnen und Verbraucher, für Datenschutz zu zahlen, dabei von 35 Prozent im Jahr 2013 auf 51 Prozent gestiegen. Von ihnen würden 87 Prozent bis zu fünf Euro im Monat oder mehr zahlen. Der Mangel an Vertrauen der Menschen in die Sicherheit wirtschaftlicher Interaktionen im Internet kann nicht im Interesse der digitalen Wirtschaft Europas liegen und war nach Aussage der Europäischen Kommission sogar Motivation für den Entwurf für die Datenschutzgrundverordnung.

Die dem Grundrecht auf Datenschutz gewogene Stimmung in der europäischen Öffentlichkeit wurde durch die Enthüllungen von Edward Snowden über die anlasslosen und umfassenden Überwachungsmaßnahmen US-amerikanischer Geheimdienste seit Juni 2013 noch verstärkt. So kritisierten 47 Prozent der Befragten ein Jahr nach den ersten Enthüllungen in einer repräsentativen Umfrage des Deutschen Instituts für Vertrauen und

Sicherheit im Internet, dass zu wenig für den Datenschutz in Deutschland unternommen werde. 52 Prozent hielten ein starkes, gemeinsames Auftreten der Europäischen Union (EU) beim Thema Datenschutz gegenüber den Vereinigten Staaten von Amerika (USA) für wichtig. Die große Mehrheit lehnte den Zugriff auf private Daten im Netz durch Außenstehende ab, wobei 56 Prozent glaubten, jeder werde abgehört. In Bezug auf Datenzugriffe von Nachrichtendiensten meinten 48 Prozent, dass dadurch unsere Grundrechte verletzt werden. 83 Prozent wollten einen Datenzugriff ausländischer Sicherheitsbehörden nicht erlauben. Nur 39 Prozent der Befragten wollten dies deutschen Sicherheitsorganen erlauben. 23 Prozent der Befragten gaben an, wegen der Snowden-Enthüllungen beim Telefonieren, Mailen und Surfen im Internet vorsichtiger geworden zu sein. Auch wenn hier möglicherweise das tatsächliche Handeln dem Wollen hinterherhinkt, ist soziologisch gesehen eine Verhaltensänderung bei fast einem Viertel der Menschen eine beachtliche Größe.

Von einem dem Grundrecht auf informationelle Selbstbestimmung gewogenen Klima in Europa kann also ausgegangen werden. Wie aber sieht es mit der bindenden rechtlichen Verpflichtung für die Verabschiedung von Regelungen mit einem hohen Datenschutzniveau aus? Im Januar 2012 legte die Europäische Kommission den genannten Entwurf der "Verordnung (…) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" vor. Nach Auffassung von Datenschützerinnen und Datenschützern erreichte dieser Entwurf das von der Europäischen Kommission selbst formulierte Ziel nicht, das Vertrauen der Menschen in die Sicherheit ihrer Daten durch die Schaffung eines hohen Datenschutzniveaus nicht nur zu erschleichen, sondern zu rechtfertigen. Siehe hierzu die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutzgrundverordnung[1] sowie mein Gutachten für den Innenausschuss des Deutschen Bundestages zur EU-Datenschutzgrundverordnung[2]. Obwohl es im Interesse der Wirtschaft gelegen hätte, das Vertrauen der Menschen in wirtschaftliche Aktionen im Internet durch die Gewährleistung eines hohen Datenschutzniveaus zu begründen, gab es im Zusammenhang mit der Diskussion über die europäischen Datenschutzregelungen von Seiten der Wirtschaft massive Versuche, darauf hinzuwirken, das Datenschutzniveau der von der Europäischen Kommission vorgeschlagenen Regelungen abzusenken, die ja ihrerseits bereits der Kritik von Seiten der Datenschützerinnen und Datenschützern ausgesetzt waren. Der Erfolg der Einflussnahmeversuche der Lobby des freien Datenverkehrs (siehe hierzu 36. Jahresbericht, Ziffer 1.) zeigt sich beim Vergleich des vom federführenden Berichterstatter verfassten Entwurfes der Fassung des Europäischen Parlamentes mit der letztlich im Oktober 2013

[1] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/DSK_Stellungnahme_Grundverordnung.pdf
[2] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Datenschutzverordnung%20Kommissionsentwurf.pdf

vorgelegten Version des Europäischen Parlamentes. Vor allem aber findet sich der Einfluss datenschutzkritischer Argumente in den Vorschlägen des Rates der Europäischen Union zur Datenschutzgrundverordnung, die erst im Juni 2015 veröffentlicht wurden. Die datenschutzrechtlichen Kernpunkte der Datenschutzkonferenz für die Trilogverhandlungen[3] bestanden daher im Wesentlichen darin, die Forderungen des Rates zurückzuweisen.

Insgesamt ist zu konstatieren, dass die Versuche von Datenschützerinnen und Datenschützern, auf die Formulierungen der Datenschutzgrundverordnung Einfluss zu nehmen, trotz des genannten datenschutzfreundlichen Klimas und trotz des Umstandes, dass es eigentlich im Interesse der Internetwirtschaft gelegen hätte, durch die Formulierung eines verbindlichen und hohen Datenschutzniveaus das Vertrauen der Menschen in Internettransaktionen zu erhöhen, deutlich weniger erfolgreich blieben als das auf Absenkung des Datenschutzniveaus gerichtete Lobbying. Insofern wird die Datenschutzgrundverordnung ihrer Funktion als internetvertrauensbildende Maßnahme nicht allein gerecht werden können.

1.2 Der Europäische Gerichtshof als oberster Internetvertrauensbildner in Europa

Dies alles könnte Anlass zu Pessimismus bezüglich des Datenschutzniveaus in Europa sein. Ein solcher Pessimismus würde aber die Bedeutung der Europäischen Grundrechtecharta, die für alle Staaten, ausgenommen das Vereinigte Königreich und Polen, seit Dezember 2009 bindend ist, und die Rolle des vierten Akteurs auf europäischer Ebene verkennen. Neben den drei Trilogpartnern Europäische Kommission, Europäisches Parlament und Rat der Europäischen Union gibt es im Europäischen Gerichtshof einen Akteur, der uns in der letzten Zeit mit starken grundrechtlichen Pflöcken erfreut hat, die er gestützt auf die Europäische Grundrechtecharta einrammte. Das europäische internetvertrauensbildende Regelwerk ist also nicht erst die Datenschutzgrundverordnung, sondern schon die Europäische Grundrechtecharta. In ihrem Artikel 8 ist festgelegt, dass jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten zusteht. Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Artikel 7 der Europäischen Grundrechtecharta gewährt jeder Person das Recht auf Achtung ihres Privatlebens und ihrer Kommunikation.

Diese starke grundrechtliche Verankerung von Sachverhalten mit Internetbezug hat der Europäische Gerichtshof vor allem in den drei wegweisenden Entscheidungen zur Nichtigkeit der europäischen Vorratsdatenspeicherungsrichtlinie, zu Google Spain und zur Nichtigkeit der Safe-Harbor-Entscheidung der Europäischen Kommission noch einmal gestärkt. Mit

[3] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Kernpunktepapier+DE.pdf

Urteil vom 8. April 2014 erklärte der Europäische Gerichtshof die Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten für ungültig und erteilte der undifferenzierten und automatischen Totalerfassung dieser Daten unter Hinweis auf die in der Europäischen Grundrechtecharta garantierten Rechte auf Privatleben und Datenschutz eine Absage (siehe hierzu 37. Jahresbericht, Ziffer 19.6). In seinem "Google Spain"-Urteil vom 13. Mai 2014 entwickelte der Europäische Gerichtshof das gegen die Betreiber von Suchmaschinen gerichtete Recht, nicht in jedem Fall leicht im Internet gefunden zu werden. Das Urteil stellt klar, dass Anbieter von Suchmaschinen keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen sind, die die Grundrechte der Betroffenen zu berücksichtigen haben (siehe hierzu 37. Jahresbericht, Ziffer 19.10). Am 6. Oktober 2015 erklärte der Europäische Gerichtshof die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig, die als Rechtsgrundlage für die Übermittlung personenbezogener Daten von Bürgerinnen und Bürgern der Europäischen Union in die USA auch über das Internet gedient hatte (siehe hierzu Ziffer 15.2 und Ziffer 17.8 dieses Berichts). Der Gerichtshof verweist dabei darauf, dass die Kommissionsentscheidung den Wesensgehalt des durch Artikel 7 der Europäischen Grundrechtecharta garantierten Grundrechts auf Achtung des Privatlebens verletze.

1.3 Profiling als besonders internetvertrauensbedürftiger Bereich

Die Datenschutzgrundverordung wird aller Voraussicht nach im Frühjahr 2016 verabschiedet werden, nachdem der Trilog im Dezember 2015 abgeschlossen worden war. Soweit die Datenschutzgrundverordnung die starken Hinweise des Europäischen Gerichthofes nicht beachtet, ist es nicht unwahrscheinlich, dass der Gerichtshof, der durch die genannte Rechtsprechung zum unverzichtbaren Garanten eines hohen Datenschutzniveaus in Europa geworden ist, bestimmte Regelungen der Datenschutzgrundverordnung wegen Verstoßes gegen die Europäische Grundrechtecharta zurückweisen, beziehungsweise die Rechtsanwendenden zur Grundrechtcharta-konformen Auslegung der Datenschutzgrundverordnung verpflichten wird.

Einer dieser Fälle könnte das Profiling sein. Von keinem der Trilogpartner wurde hierzu ein aus Sicht des Datenschutzgrundrechtes akzeptabler Regelungsvorschlag gemacht, der eine wirksame Begrenzung von Profilbildungen ermöglicht. Im zum Redaktionsschluss vorliegenden Text der Datenschutzgrundverordnung hat sich der Rat der Europäischen Union durchgesetzt. Nicht bereits die Profilbildung selbst, sondern erst die Nutzung von Profilen wird rechtlichen Beschränkungen unterworfen, wenn es in Artikel 20 heißt, die Menschen sollten das Recht haben, keiner Entscheidung ausgesetzt zu sein, die allein auf automatischer Datenverarbeitung inklusive Profilbildung beruhe und rechtliche Auswirkungen habe oder sie in ähnlich bedeutsamer Weise beträfe. ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling,

which produces legal effects concerning him or her or similarly significantly affects him or her.") Dieses bereits sehr schmale Recht der Menschen auf Schutz vor Entscheidungen, die nur auf Profilbildungen beruhen, soll zusätzlich dann nicht bestehen, wenn die Profilbildung auf der ausdrücklichen Einwilligung der oder des Betroffenen beruht, erforderlich für den Abschluss oder die Durchführung eines Vertrages mit dem Datennutzer ist oder durch nationalstaatliche Gesetze erlaubt ist, die ausreichend die Rechte und Freiheiten und legitimen Interessen der Grundrechtsträgerinnen und Grundrechtsträger beachten.

Alle genannten Urteile des Europäischen Gerichtshofes enthalten wichtige Aussagen, die darauf hindeuten, dass schon die Profilbildungen selbst grundrechtlichen Beschränkungen unterworfen werden müssten. Im Urteil zu Google Spain stellt der Europäische Gerichtshof grundlegende Erwägungen zur Rolle des Internets, von Suchmaschinen und mit ihnen möglichen Profilbildungen in der modernen Gesellschaft an. Allen, die diese Möglichkeiten nutzten, sei ein strukturierter Überblick über die zu Personen im Internet zu findenden Informationen möglich, die potenziell zahlreiche Aspekte von deren Privatleben betreffen könnten und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden könnten. Hieraus schließt der Europäische Gerichtshof, wegen seiner potenziellen Schwere könne ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse an der Datenverarbeitung gerechtfertigt werden. Im Urteil zur Ungültigkeit der Vorratsdatenspeicherungsrichtlinie wird deutlich, dass der Europäische Gerichtshof dem Grundsatz der Erforderlichkeit eine hohe Bedeutung beimisst. Auch die Aussagen zu technischen Anforderungen können auf Profilbildungen übertragen werden. Es sei entscheidend, dass es hinreichende Garantien gebe, dass die Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt seien. Im Urteil zur Ungültigkeit der Safe-Harbor-Entscheidung formuliert der Europäische Gerichtshof eine strikte Zweckbindung von Datenverarbeitungen, die verletzt sei, wenn eine Regelung generell die Speicherung aller personenbezogenen Daten sämtlicher Personen gestatte. In Randnummer 91 bringt der Europäische Gerichtshofs seine ständige Rechtsprechung folgendermaßen auf den Punkt: Eine Unionsregelung, die einen Eingriff in die durch die Artikel 7 und 8 der Charta garantierten Grundrechte enthalte, müsse klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren personenbezogene Daten betroffen seien, über ausreichende Garantien verfügten, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichten.

Die Anforderungen des Europäischen Gerichtshofes sprechen also dafür, auch die Profilbildungen selbst rechtlichen Beschränkungen zu unterwerfen. Es hätte daher nahe gelegen, in der Datenschutzgrundverordnung eng begrenzte klare Erlaubnistatbestände für Profilbildungen zu formulieren, Transparenz und Informiertheit der Betroffenen ausdrücklich

zu gewährleisten und etwa eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und Auswertung verwendeten Daten festzuschreiben. Die Formulierung eines solchen verbindlichen und hohen Datenschutzniveaus hätte auch im Interesse der Internetwirtschaft gelegen, weil sie das Vertrauen der Menschen in Internettransaktionen erhöht hätte. Insofern werden sich die Lobbyisten der Datenschutzrechte gemeinsam mit den Lobbyistinnen des freien Datenverkehres über die zu erwartenden Entscheidungen des Europäischen Gerichtshofes freuen!

1.4 Da kommt was auf uns zu. Oder: Was der Landesgesetzgeber nach Erlass der Datenschutzgrundverordnung entscheiden muss

Eines steht fest: Nach Verabschiedung der Datenschutzgrundverordnung werden auf die nationalstaatlichen Gesetzgeber sehr viele Entscheidungen über die Beurteilung des jetzt geltenden Rechts zukommen. Auch der bremische Landesgesetzgeber muss für alle Normen, die gegenwärtig Datenverarbeitungsregelungen enthalten, prüfen, ob das Landesrecht durch die Datenschutzgrundverordnung **ersetzt** wird, die Datenschutzgrundverordnung also direkt gilt, ob das Landesrecht **beibehalten** bleiben kann und soll, oder ob das Landesrecht unter Beachtung der Datenschutzgrundverordnung **geändert** werden soll. Das gilt beispielsweise für das Bremisches Datenschutzgesetz, das Bremische Schuldatenschutzgesetz, das Bremische Krankenhausdatenschutzgesetz, das Bremische Archivgesetz, das bremische Pressegesetz, das Bremische Polizeigesetz, das Bremische Hilfeleistungsgesetz, das Gesetz über das Krebsregister der Freien Hansestadt Bremen, das Bremische Naturschutzgesetz, das bremische Vergabegesetz, das Bremische Beamtengesetz und das Bremische Hafenbetriebsgesetz. Über den Bundesrat ist Bremen daneben auch an der Bundesgesetzgebung beteiligt, die ebenfalls weitreichende Aufgaben bei der Konkretisierung der Datenschutzgrundverordnung zu erfüllen hat.

Dies alles gibt dem bremischen Gesetzgeber die Chance, den durch die Datenschutzgrundverordnung eröffneten gesetzgeberischen Spielraum im Sinne des durch die Europäische Grundrechtecharta geforderten höchstmöglichen Grundrechtsschutzes zu nutzen. Das Pochen auf die demokratisierende Funktion von Grundrechtsschutz wäre jetzt genau die richtige Reaktion auf die im Berichtsjahr verübten offenbar zutiefst antidemokratisch motivierten Attentate.

Dr. Imke Sommer