Datenschutz in einer grenzenlosen Welt: Internationale Regelungsansätze

Marita Körner

I. Hintergrund

Seit wenigen Jahren ist Datenschutz wieder in aller Munde. Nachdem 1970 im Bundesland Hessen das erste Datenschutzgesetz der Welt in Kraft gesetzt worden war und im Jahr 1983 das Bundesverfassungsgericht sein für die weitere Entwicklung des Datenschutzes wegweisendes Volkszählungsurteil gefällt hatte, in dem das Gericht das Recht auf informationelle Selbstbestimmung in Art. 2 und Art 1 GG verankerte,[1] war es um das Thema langsam wieder still geworden und Fragen nach der Zulässigkeit von Erhebung und Weiterverarbeitung von personenbezogenen Daten wurden vorwiegend in Expertenzirkeln gestellt.

Zwar haben nach und nach alle Bundesländer Landesdatenschutzgesetze erlassen und das seit 1978 geltende Bundesdatenschutzgesetz (BDSG) ist mehrfach angepasst worden. Auch sind in etlichen Bereichen bereichsspezifische Datenschutzregeln geschaffen worden. Dennoch haben die Reaktionen des Gesetzgebers nicht annähernd mit der technischen und wirtschaftlichen Entwicklung Schritt gehalten. Die geltenden Regeln spiegeln im Wesentlichen die Lage der siebziger und achtziger Jahre wider, in denen im Vergleich zu heute relativ wenige Daten aus beschränkten Lebensausschnitten formularmäßig erfasst und in Rechenzentren mit Großrechnern vor allem für die Verwaltung verarbeitet wurden. Dagegen haben wir es heute mit dem durch das seit 1993 für die Öffentlichkeit zugänglichen Internet mit völlig veränderten Kommunikationsmustern zu tun. Stand 1983 zur Zeit des Volkszählungsurteils die Angst vor Durchleuchtung und Verlust der Privatsphäre durch den Daten sammelnden Staat im Zentrum der Debatte einer kritischen Öffentlichkeit, geben heute Millionen von Menschen täglich Millionen an personenbezogenen Daten freiwillig für vermeintlich kostenlose, schnelle und einfache Kommunikation in sozialen Netzwerken preis und zögern nicht, umfassende Informationen über sich selbst beim Einkaufen und Surfen im Internet zu hinterlassen.

Personenbezogene Daten sind zu einem erheblichen Wirtschaftsfaktor geworden. Der Handel mit der Ware „personenbezogene Information" gilt als Zukunfts-

1 BVerfGE 65, 1.

markt. In den USA sollen bereits Millionen von Arbeitsplätzen direkt davon abhängen. Vor diesem Hintergrund werden die Defizite der bisherigen Datenschutzregelungen besonders deutlich, haben sie doch vor allem datensammelnde öffentliche Stellen im Blick. Die Regelungen des BDSG zur Kontrolle privater Stellen, d.h. vor allem privater Wirtschaftsunternehmen sind schwach, die Kontrollmechanismen gar europarechtswidrig.[2]

Erst große Datenpannen und -skandale in einigen deutschen Unternehmen haben das Bewusstsein der Öffentlichkeit für das Thema Datenschutz wieder geschärft, zumal der Datenmissbrauch bei Telekom, Deutscher Bahn oder Lidl Arbeitnehmerdaten betraf und somit potentiell einen großen Teil der Bevölkerung. Da es trotz jahrzehntelanger Diskussion in Deutschland für Arbeitnehmerdaten noch immer keine bereichsspezifischen Schutzregeln gibt, hat der Gesetzgeber als eilige Reaktion auf die Skandale im Jahr 2010 § 32 ins BDSG eingefügt, der aber kaum über die zuvor auf Arbeitnehmerdaten angewendete allgemeine Regel in § 28 I BDSG hinausgeht. Da das auch dem Gesetzgeber klar war, hat er einen Entwurf zu weiteren, das BDSG ergänzenden Arbeitnehmerdatenschutzregeln vorgelegt, dessen Zukunft allerdings angesichts der europäischen und internationalen Entwicklung ungewiss ist.[3] Seit März 2011 im Gesetzgebungsverfahren und mehrfach kurz vor der Verabschiedung, ist der Entwurf nach massiver Kritik u.a. des DGB[4] im Januar 2013 vorläufig gescheitert.

Neben dem Paradigmenwechsel vom datensammelnden Staat zum datensammelnden Wirtschaftsunternehmen ist der Gesetzgeber mit einem weiteren ebenso bedeutsamen Phänomen konfrontiert, das wesentlich schwerer zu fassen und effizienten Regelungen zuzuführen ist: die Globalisierung der Datenströme. Nicht nur große Teile der wirtschaftlichen Betätigung machen an Ländergrenzen nicht mehr halt, sondern vor allem auch die Datenverarbeitung, die schon aus der Natur der Sache heraus grundsätzlich nicht ortsgebunden ist. Will man in Zukunft das Freiheitsrecht „informationelle Selbstbestimmung“ schützen, wird man mit nationalen Regelungen – so wichtig die auch sein mögen und sei es zur Bewusstseinsbildung – nicht weit kommen. Datenschutzregeln für die eigenen staatlichen Stellen, die sich auf dem Territorium des jeweiligen Landes befinden, mögen noch wirksam durchgesetzt werden können. Geht es aber um den Datenschutz im privaten Bereich, müssen die Datenschutzregeln der grenzüberschreitenden Tätigkeit der Unternehmen folgen. Internationale Regeln sind also unerlässlich.

2 EuGH, Urt. v. 9.3.2010 – C-518/07.
3 Zu den Details des Entwurfs kritisch Körner, M., Gutachten für das HSI Frankfurt, Nov. 2010 (abrufbar unter: www.hugo-sinzheimer-institut.de).
4 DGB Info Recht 25.1.2013: Kein sogen. „Beschäftigtendatenschutz“ auf „Biegen und Brechen“.

II. BDSG-Regeln zum grenzüberschreitenden Datentransfer

Die Regeln des BDSG zum grenzüberschreitenden Datentransfer sind allerdings eher symbolischer Natur. § 4b BDSG knüpft für die Zulässigkeit der Datenübermittlung ans Ausland an ein dort gewährleistetes ausreichendes Datenschutzniveau an. Dabei können aber in Ländern, die keine Datenschutzgesetzgebung haben, auch privatrechtliche Zusicherungen des Datenempfängers ausreichen. Darüber hinaus sieht § 4c BDSG weite Ausnahmen vor. So muss ein ausreichendes Datenschutzniveau etwa dann nicht vorliegen, wenn der Betroffene in die Datenübertragung eingewilligt hat oder diese zur Erfüllung eines Vertrages dient.

Allerdings kann eine nationale Regelung wie das BDSG die Datenweitergabe letztlich nur an ein angemessenes Datenschutzniveau im Zielland knüpfen und müsste, wenn dort der Standard nicht ausreicht – wie in den meisten Ländern der Welt – den Transfer verbieten, ein wirtschaftsweltfremder Ansatz. Umso mehr kommt es auf wirksame europäische und internationale Regelungen an.

III. EU-Datenschutz

1. Datenschutzrichtlinie

Erst 1995 wurde der grenzüberschreitenden Dimension der Datenverarbeitung mit der EG-Datenschutzrichtlinie begegnet[5]. Die Richtlinie war nicht die erste Datenschutzregelung in Europa. Bereits 1981 hatte der Europarat mit dem Übereinkommen Nr. 108 Mindeststandards für den europäischen Datenschutz geschaffen, die auch in der EU gelten, aber später durch die eigenen EU-Regelungen z.T. überlagert wurden. Die Richtlinie von 1995 ist derzeit noch die Grundlage für den Datenschutz in den EU-Mitgliedstaaten, gilt aber nicht für den Polizei- und Justizbereich. Aus diesem Grund, so der EuGH, sei die Übermittlung von Fluggastdaten durch Fluggesellschaften an die USA nicht von der Richtlinie erfasst[6], denn hierbei handele es sich um Daten, die im Rahmen polizeilicher Zusammenarbeit erhoben würden. Ansonsten allerdings legt der EuGH den Anwendungsbereich der Datenschutzrichtlinie weit aus. Um ein einheitliches Schutzniveau innerhalb der EU zu gewährleisten, sieht die Richtlinie die sogen. „Art. 29-Gruppe“ vor, ein Koordinierungs- und Beratungsgremium für die Kommission, das von den Datenschutzbehörden der Mitgliedstaaten beschickt wird. Für den Bereich der Telekommunika-

5 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995.

6 EuGH, Urt. v. 30.5.2006 – C-317/04 und C-318/04.

tion sind 2002/2009[7] eigene Richtlinien erlassen worden. Auch wenn die Datenschutzrichtlinie von 1995 neben der Gewährleistung des freien Datenverkehrs im gemeinsamen Binnenmarkt vor allem den Grundrechtsschutz im Auge hat, ist nicht alles, was die EU nach 1995 in Sachen Datenschutz auf den Weg gebracht hat, von diesem Grundrechtsansatz inspiriert. So spricht die Richtlinie zur Vorratsdatenspeicherung von 2006 eine andere Sprache. Sie erlaubt eine umfassende Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten und wurde daher in vielen Mitgliedstaaten heftig kritisiert. Nicht nur in Deutschland wurde in der Folge das Gesetz zur Umsetzung der umstrittenen Richtlinie von den jeweiligen Verfassungsgerichten verworfen[8].

2. Entwurf einer Datenschutzgrundverordnung

Auch wenn die Datenschutzrichtlinie von 1995 die Schaffung eines einheitlich (hohen) Datenschutzniveaus in allen 27 Mitgliedstaaten zum Ziel hatte, so stößt sie doch aus zwei Gründen an ihre Grenzen. Zum einen ist die Richtlinie fast zwanzig Jahre alt und damit in der schnelllebigen Welt der Informationstechnologie nicht mehr auf der Höhe der technischen Datenverarbeitungsmöglichkeiten. Zum anderen ist das Ziel eines einheitlichen Datenschutzniveaus längst nicht überall erreicht worden, da die Richtlinie nicht nur einen Umsetzungskorridor erlaubt, sondern manche Mitgliedstaaten diesen deutlich unterschreiten. Das muss nicht unbedingt auf der Ebene des materiellen Rechts der Fall sein, findet sich aber häufig bei der Kontrolle.

Vor diesem Hintergrund ist eine Reform des EU-Datenschutzrechts dringend geboten. Hierauf hat die Kommission mit dem Entwurf zu einer Datenschutzgrundverordnung vom 15.1.2012[9] reagiert und damit allerdings in zentralen Bereichen das Kind mit dem Bade ausgeschüttet[10]. Um Ausweichreaktionen einzelner Mitgliedstaaten zu vermeiden, schlägt die Kommission keine Richtlinie, sondern eine Verordnung vor. Die dient zwar unzweifelhaft ab dem Tag ihres Inkrafttretens der Vereinheitlichung des Datenschutzniveaus in allen Mitgliedstaaten. Allerdings kann sie trotzdem kontraproduktiv wirken, da gerade wegen der rasanten technischen Veränderungen ein flexibles Regelungsinstrument nötig wäre. Daher ist immer wieder vorgeschlagen worden, Datenschutzregelungen grundsätzlich zu be-

7 Richtlinie 2002/58/EG und Richtlinie 2009/136/EG.
8 Für Deutschland siehe BVerfGE 125, 260, 324f.
9 KOM (2012) 11 endg. Neben der Grundverordnung schlägt die Kommission auch eine Richtlinie zum Schutz personenbezogener Daten vor, die im Rahmen der Strafverfolgung und -vollstreckung erhoben werden (KOM (2012) 10 endg.
10 Dazu genauer Körner, Die Reform des EU-Datenschutzes: der Entwurf einer EU-Datenschutz-Grundverordnung, in ZESAR 2013, Heft 3 und 4.

fristen.[11] Regulierungsflexibilität kann auch mit anderen Mechanismen erreicht werden, vor allem durch bereichsspezifische Regelungsbefugnisse für die Mitgliedstaaten. Genau die soll es aber in der neuen Verordnung kaum geben. Zwar sieht der Verordnungsentwurf eine bereichsspezifische Öffnung für den wichtigen Bereich des Arbeitnehmerdatenschutzes vor. Der einzelstaatliche Handlungsspielraum wird aber im gleichen Atemzug wieder stark beschnitten, da sich eine einzelstaatliche bereichsspezifische Regulierung zum Arbeitnehmerdatenschutz „im Rahmen der Verordnung" halten müsste.

Dieser Rahmen ist aber alles andere als klar. Die Verordnung arbeitet mit vielen unbestimmten Rechtsbegriffen. Deren Ausfüllung wie auch die Regelung ganzer Bereiche soll im Wesentlichen der Kommission in Gestalt sogenannter delegierter Rechtsakte obliegen. Daneben wird die Bedeutung der nationalen Aufsichtsbehörden stark beschnitten, werden die nationalen Verfassungsgerichte marginalisiert und wird die Kontrolle bei der Kommission konzentriert.

Sind diese Gründe schon ausreichend, den Verordnungsentwurf in dieser Form nicht zu verabschieden, wird die Skepsis trotz der an sich nötigen Neuregelung des europäischen Datenschutzes noch größer mit Blick auf die offensichtliche Motivation der Kommission für den Entwurf. Schon im ersten Abschnitt zur Begründung des Entwurfs heißt es, dass Datenschutz als „Voraussetzung dafür angesehen wird, dass die digitale Wirtschaft im Binnenmarkt weiter Fuß fasst"[12]. Dazu passt die Aussage der zuständigen Kommissarin, dass persönliche Daten „die Währung des heutigen digitalen Marktes" seien[13]. Es drängt sich also der Eindruck auf, dass die Neuregelung des EU-Datenschutzes nicht vorwiegend das Ziel eines besseren Persönlichkeitsschutz des Einzelnen anstrebt als vielmehr bessere Verarbeitungsbedingungen für Unternehmen.

IV. Völkerrechtliche Datenschutzregelungen

So wichtig EU-Regelungen zum Datenschutz sind, können auch sie das Problem der die EU-Grenzen überschreitenden Datenverarbeitung nicht lösen, zumal der Entwurf für eine EU-Datenschutzgrundverordnung keine weitergehenden Konzepte bereit hält als das veraltete BDSG.

Angesichts weltumspannender Datenströme könnten international gültige Datenschutzstandards das Recht auf informationelle Selbstbestimmung am besten schützen. Allerdings liegt wie bei anderen sinnvoll nur global zu regelnden Pro-

11 Simitis, S., in: Simitis, S. (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011, Einl., Rn 122.
12 KOM (2012) 11 endg., S. 2.
13 Reding, V., DLD-Konferenz München, 22.1.2012.

blemen – man denke nur an den Umweltschutz und die Regulierung der Finanzmärkte – hier auch das Problem, mit dem völkerrechtliche Regelungen immer konfrontiert sind: aus langwierigen Verhandlungen folgende vage Bestimmungen im materiellen Recht und Umsetzungsdefizite angesichts souveräner Staaten, die die Kontrollmechanismen der verschiedenen internationalen Organisationen nicht immer ernst nehmen.

Bedenkt man weiterhin, dass der Schutz personenbezogener Daten ein junges Rechtsgebiet ist, verwundert es nicht, dass der Bestand an völkerrechtlichen Datenschutzregeln noch sehr lückenhaft ist. Wie im nationalen Datenschutz waren auch im internationalen Datenschutz vor allem die 1980er Jahre die hohe Zeit der Regulierung. Die Europaratskonvention zum Datenschutz oder die UNO-Datenschutzrichtlinien stammen aus diesen Jahren. Erst die rasante Entwicklung der Informationstechnologie und das wieder wachsende Bewusstsein der damit verbundenen Persönlichkeitsrechtsprobleme haben den Datenschutz auch international zum Thema gemacht, allerdings vor dem Hintergrund eines Paradigmenwechsels. Nicht mehr nur der Datenhunger des Staates – wenn der auch durch neues Sicherheitsdenken seit 2001 keineswegs gestillt ist -, sondern vor allem der rasant wachsende ökonomische Wert personenbezogener Informationen machen persönlichkeitsrechtsorientierte Regulierung viel schwerer durchsetzbar als in den 1980er Jahren, zumal auf internationaler Ebene, wo wesentlich mehr „Spieler" involviert sind als im einzelnen Staat. Paradebeispiel dafür ist der Entwurf der o.a. EU-Datenschutzverordnung, die nicht mehr, wie noch die EG-Datenschutzrichtlinie von 1995, primär den Persönlichkeitsschutz des Einzelnen im Auge hat, sondern mindestens ebenso, wenn nicht vorrangig, das wirtschaftliche Verwertungsinteresse der Datenverarbeitungsindustrie bedient. Vor diesem Hintergrund fallen die Defizite der derzeitigen völkerrechtlichen Datenschutzregeln besonders auf.

1. Verbindliche Regelungen

Nur der Europarat hat bislang auf völkerrechtlicher Ebene mit dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten von 1981[14] rechtsverbindliche Datenschutzregeln verabschiedet, die 44 Staaten binden. Ganz neue Datenschutzgrundsätze wurden vom Europarat nicht entwickelt, sondern auf zu diesem Zeitpunkt schon existierende nationale Datenschutzgesetze zurückgegriffen (Art. 5 ff.) und damit zentrale Prinzipien wie die Zweckbindung, die Datensparsamkeit oder die Unabhängigkeit der Datenschutzkontrolle (Art. 1 Nr. 3) internationalisiert. Den grenzüberschreitenden Datenschutz

14 Übereinkommen Nr. 108 vom 28.1.1981.

spricht die Konvention in Art. 12 an, konnte aber zunächst den zentralen Problemen nicht gerecht werden, da sich die Regelung nur auf die Länder bezog, in denen die Konvention galt. Seit 2001 regelt ein Zusatzprotokoll, dass personenbezogene Daten an Drittstaaten nur übermittelt werden dürfen, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Allerdings sind im Zusatzprotokoll von diesem Grundsatz weite Abweichungen erlaubt. Es darf eben nicht vergessen werden, dass auch die Konvention des Europarates nicht nur den Schutz des Einzelnen anstrebt, sondern auch den freien Datentransfer gewährleisten will. Nichtsdestoweniger ist die Datenschutzkonvention des Europarates das stärkste völkerrechtliche Menschenrechtsinstrument in Sachen Datenschutz. Allerdings verliert die Konvention seit der Regulierung auf EU-Ebene, aber auch angesichts der beschleunigten technischen Entwicklung an praktischer Bedeutung. Dieser Bedeutungsrückgang wird jedoch z.T. durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte kompensiert, der insbesondere in Auslegung von Art. 8 EMRK, der das Recht auf Achtung des Privatlebens gewährleistet, die Erhebung und Verarbeitung von personenbezogenen Daten einschränkt.

2. Empfehlungen

a) OECD

Hat der Europarat primär einen menschenrechtlichen Blick auf den Datenschutz, so ist die Perspektive der OECD eine ganz andere. Auch schon früh, im Jahre 1980, hat sie Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten verabschiedet, dabei aber vor allem die Gefahr von Handelshemmnissen durch nationale Datenschutzregelungen gesehen und vor allem von den Mitgliedstaaten Maßnahmen zum freien grenzüberschreitenden Datenverkehr angemahnt (Nr. 15-18). Dazu passt es, dass die OECD für die Umsetzung ihrer Datenschutzrichtlinien, die durchaus auch die gängigen Verarbeitungsgrundsätze enthalten (Nr. 7-14), nicht allein auf staatliche Gesetzgebung baut, sondern auch Selbstregulierung durch die Unternehmen zulässt (Nr. 19b).

b) UNO

Auch die UNO hat bereits in den 1980er Jahren in unkontrollierter Datenverarbeitung eine Gefahr für die Menschenrechte gesehen. Daher legte die Menschenrechtskommission 1988 Vorschläge für Richtlinien zur Verarbeitung personenbe-

zogener Daten vor, die 1990 von der Generalversammlung verabschiedet wurden. Diese Richtlinien haben zwar nur Empfehlungscharakter, gelten aber nicht nur für die Mitgliedstaaten (Teil A), sondern auch für die internationalen Organisationen selbst (Teil B). Für Daten, die im Rahmen der „humanitären Hilfe" oder zum „Schutz der Menschenrechte" erhoben und verarbeitet werden, gelten Ausnahmen, da z.B. bei der Erhebung von Opferdaten nicht zuvor deren Einwilligung eingeholt werden kann. Die Verarbeitungsgrundsätze in den UNO-Richtlinien entsprechen im Wesentlichen denen der Datenschutzkonvention des Europarates. Für grenzüberschreitenden Datenaustausch wird eine gleichwertige Datenschutzregelung im Empfängerstaat verlangt (Nr. 9). Über diese Aussage hinaus wird aber nicht weiter spezifiziert, was das genau heißt. Es kann also aus Nr. 9 nicht abgeleitet werden, dass es sich bei den Datenschutzregeln im Empfängerstaat um gesetzliche Regelungen handeln muss.

c) Internationale Arbeitsorganisation

Für die ILO steht der Arbeitnehmerdatenschutz im Mittelpunkt. Anders als bei den ansonsten langwierigen Abstimmungs- und Kompromissprozeduren um Übereinkommen hat die ILO beim Datenschutz einen anderen Weg gewählt: den schnelleren, inhaltlich weiter gehenden Weg eines Verhaltenskodex, der 1997 verabschiedet wurde. Anders als das deutsche BDSG sieht der Datenschutz-Verhaltenskodex die Einwilligung des Arbeitsnehmers in Datenerhebung und -verarbeitung kritisch, da der Arbeitnehmer wegen seiner Abhängigkeit Einwilligungen selten wirklich freiwillig erteilen wird. Jedenfalls muss nach dem Kodex bei sensiblen Daten ein Gesetz die Datenverarbeitung gestatten. Den Besonderheiten des Arbeitsrechts trägt auch der Umstand Rechnung, dass zum Arbeitnehmerdatenschutz möglichst kollektivrechtliche Regelungen abgeschlossen werden sollen (Nr. 12.2).

V. Ausblick

Die internationale datenschutzrechtliche Reaktion hält bei weitem nicht Schritt mit der technischen Entwicklung und der heute großen wirtschaftlichen Bedeutung von personenbezogenen Daten. Weitgehend auf den Ideen des Datenschutzaufbruchs der 1980er Jahre fußend, sind die Schutzkonzepte lückenhaft, zumal auf völkerrechtlicher Ebene außer dem Europarat keine Organisation verbindliche Regeln hat schaffen können. Eine Sonderrolle spielt die EU mit dem Entwurf einer alle Mitgliedstaaten sowie den öffentlichen wie den privaten Bereich umfassenden Datenschutzregelung in einer nicht umsetzungsbedürftigen Verordnung. Auch diese

Verordnung löst allerdings das Problem des Datentransfers in Drittstaaten nicht und will das wohl auch nicht, um einem ihrer Ziele näher zu kommen, dem freien Datenverkehr. Dieses Ziel, das aus dem hohen ökonomischen Potential personenbezogener Informationen folgt, ist der Hauptgrund, warum trotz der Erkenntnis, dass alle existierenden Datenschutzregelungen veraltet sind, bislang vor allem international keine wirksamen, dem heutigen Stand der Technik entsprechenden Datenschutzvorschläge vorgelegt wurden, die sich vorwiegend am Interesse des zu schützenden Individuums orientieren.

Aus dem Süden Europas: Überlegungen zur Bürgerschaft in Krisenzeiten[1]

Antonio Baylos

I. Politische Bürgerschaft und Soziale Bürgerschaft

Heutzutage haben die beiden Konzepte Staatsangehörigkeit und Bürgerschaft als zwei eng mit der Souveränität des Staates in Verbindung stehende Elemente eine komplexe Bedeutung erlangt. Unter Staatsangehörigkeit versteht man „die rechtliche Beziehung, die einen Menschen mit dem Staat verbindet" oder „den maximalen juristischen Ausdruck der Integration eines Menschen in eine staatliche Gemeinschaft". Bürgerschaft bezeichnet Mitbestimmungs- und Beteiligungsrechte im öffentlichen Raum, die aufgrund der Zugehörigkeit zu einer organisierten Gemeinschaft, normalerweise zu einem Nationalstaat, bestehen. Bürgerschaft umfasst Rechte und Pflichten, die in der Verfassung des Staates verbrieft sind, zu dem sich der Bürger – normalerweise aufgrund seiner Staatsangehörigkeit – zugehörig erklärt. Für gewöhnlich wird der Begriff der Bürgerschaft auf die politischen Rechte beschränkt. Selbst das Wörterbuch der *Real Academia Española* definiert einen „Bürger" als Träger politischer Rechte, der durch deren Ausübung an der Regierung eines Landes beteiligt ist.

Doch die Beteiligung am öffentlichen Raum als Träger von Rechten steht erst am Ende eines historischen Prozesses, in dessen Verlauf der Bürgerbegriff durch die Entwicklung der subjektiven politischen Rechte, der institutionellen Garantien und der Leistungsansprüche an den Staat angereichert wurde. Daher umfasst der Begriff Bürgerschaft für gewöhnlich zwei charakteristische Eigenschaften: Politische Bürgerschaft und soziale Bürgerschaft. Beide sind eng miteinander verbunden.

Während die politische Bürgerschaft denjenigen vorbehalten ist, die im Besitz der Staatsangehörigkeit des Staates sind, in dem sie ihre Rechte auf politische Teilhabe ausüben, eröffnet sich die soziale Bürgerschaft den anderen mit Hilfe eines Verfahrens der Transformation bzw. Wiederherstellung des Begriffs der Bürgerschaft. Dies geschieht durch ein zentrales Element in den Verfassungen, die von der Erklärung des Sozialstaates und dem Wert der Arbeit für die Erlangung von Rechten im öffentlichen Raum ausgehen.

1 Beitrag zu den Studien zu Ehren von Klaus Lörcher. Mein Dank gilt meiner guten Freundin Reingard Zimmer für ihren Vorschlag, mich daran zu beteiligen.