EBS Law School

Skript
Öffentliches Recht als Steuerungsinstrument für die Digitalisierung

Emanuel V. Towfigh

Spring Term 2019

C. Das Allgemeine Persönlichkeitsrecht

I. Einführung: A Brave New World? Chinas Sozialkreditsystem

Wie funktioniert das Sozialkreditsystem?

- viele Details noch unbekannt, daher nur kursorischer Überblick
- jeder Chinese, aber auch Firmen und Behörden erhalten ein Punktekonto, das ihre Vertrauenswürdigkeit ausweist
- „Wohlverhalten“ – etwa wohltätige Arbeit leisten, Familienangehörige pflegen oder keine Schulden haben und die Regierung in sozialen Netzwerken loben – führt zum Aufstieg im Sozialkreditsystem
- „Fehlverhalten“ – etwa durch Betrug in Online-Spielen, seine Eltern nicht regelmäßig besuchen, bei „Rot“ über die Ampel gehen, aber auch bei regierungskritischen Posts in sozialen Medien oder der Teilnahme an religiösen Versammlungen, die von der Regierung nicht genehmigt wurden – führt zum Punktabzog

Welchen Einfluss hat der Kontostand auf das persönliche Leben?

- großer Einfluss auf das tägliche Leben
- hoher Kontostand ermöglicht beispielsweise
  - Vorrang bei Schulzulassungen oder der Vergabe von Arbeitsplätzen
  - leichterer Zugang zu Krediten
  - günstigere Tickets für den öffentlichen Nahverkehr
  - kürzere Wartezeiten im Krankenhaus
- geringer Kontostand führt dagegen beispielsweise zu
  - Ausschluss von der Buchung von Flügen oder Schnellzügen
  - erschwertem Zugang zu Krediten
  - eingeschränkter Zugang zu öffentlichen Dienstleistungen
  - Sperre für Jobs im öffentlichen Raum

Woher stammen die Daten?

- alle Quellen, die der Regierung zur Verfügung stehen
- etwa Meldedaten, Strafregister, Kreditbewertungen und Schulzeugnisse
- Daten aus der umfassenden Videoüberwachung in China (inkl. Gesichtserkennung)
- darüber hinaus aber auch Daten aus digitalen Quellen, wie Suchbegriffe bei Online-Suchmaschinen, Kommentare in sozialen Medien, usw.
- Daten werden von einer künstlichen Intelligenz erhoben und ausgewertet (laut eigenen Angaben wurden bisher 16,5 Milliarden personenbezogene Daten gesammelt)[1]

Fiktion oder Realität?

- Sozialkreditsystem soll 2020 flächendeckend eingeführt werden
- bereits Testläufe in einigen Städten Chinas durchgeführt
- Folge der Testläufe: Veröffentlichung einer „Schwarzen Liste“ durch chinesische Gerichte
  - 10.360.000 chinesische Bürger umfasst
  - Einschränkungen bei Flugreisen oder Fahrten mit Hochgeschwindigkeitszügen
  - erprobt wurden auch Restriktionen wie Einschränkungen bei Immobilienkäufen, der Schulanmeldung und der Nutzung von Autobahnen

Literaturempfehlungen

- *Oganesian/Heermann*, China: Der durchleuchtete Mensch – Das chinesische Social-Credit-System, ZD-Aktuell 2018, 06124
- *Wissenschaftliche Dienste des Deutschen Bundestages,* Big Data unter Berücksichtigung der Situation in der Volksrepublik China, Az. WD 10-3000 -068/17, vom 12.01.21018
- Einführungsvideo aus der Vorlesung: http://www.daserste.de/information/wissen-kultur/wissen-vor-acht-zukunft/videos/sozialkreditsystem-wissen-vor-acht-zukunft-video-100.html

[1] *Siemons*, Die totale Kontrolle, F.A.Z.-Net vom 11.05.2018 (abrufbar unter: https://www.faz.net/aktuell/feuilleton/debatten/chinas-sozialkreditsystem-die-totale-kontrolle-15575861.html?printPagedArticle=true#pageIndex_0)

II. Recht auf informationelle Selbstbestimmung

Wiederholungsfrage: Was schützt das Recht auf informationelle Selbstbestimmung?

- Bürger*innen sollen die Kontrolle über ihre Daten behalten und selbst über deren Preisgabe und Verwendung entscheiden können
- mit dem Recht auf informationelle Selbstbestimmung wäre eine Rechtsordnung nicht vereinbar,

„in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“
BVerfGE 65, 1, 43 (Volkszählung [1983])

Wiederholungsfrage: Welche Bedeutung hat das Recht auf informationelle Selbstbestimmung?

- systematische Erfassung von Daten über Bürger*innen könnte ein Gefühl der ständigen Überwachung hervorrufen
- Bürger*innen würden gegebenenfalls davon abgehalten, ihre staatsbürgerlichen Rechte wahrzunehmen

„möglicherweise [wird der Bürger] auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist.“
BVerfGE 65, 1, 43 (Volkszählung [1983])

Gibt es ein Grundrecht auf Datenschutz auf europäischer Ebene?

- Verankert in Art. 8 EU-GRCh, als *lex specialis* zu Art. 7 (Achtung des Privat- und Familienlebens)
- Datenschutz als Aspekt der Achtung der Privatsphäre ist ein besonders wichtiger Teil des Schutzes des Privatlebens, sodass dieser in einer gesonderten Bestimmung behandelt wird
- Grundrechtsverpflichtete
  - die Organe und Einrichtungen der Union
  - die Mitgliedstaaten, aber nur bei der Durchführung von EU-Recht
  - nicht: Privatpersonen; aber Normen des Privatrechts sind grundrechtskonform auszulegen, sodass sich hierüber ggf. eine Bindung Privater ergeben kann
- Gewährleistungsinhalt
  - *klassisches Abwehrrecht* gegen staatliches Handeln
  - darüber hinaus auch die Funktion des *status positivus*
    - staatliche Schutzpflichten
    - insbesondere müssen die Grundrechtsverpflichteten Schutz auch gegenüber privatem Handeln gewährleisten
    - Eingriffe können danach auch durch ein Unterlassen erfolgen
    - aber: großer Entscheidungsspielraum bei der Entscheidung über entsprechende Schutzregelungen für Grundrechtsverpflichtete

Gibt es ein Grundrecht auf Datenschutz in Hessen?

- neu in der Hessischen Verfassung Art. 12a
  - umfasst ein hessisches Datenschutz-Grundrecht und hessisches Computer-Grundrecht
  - inhaltlich gleicht das Computer-Grundrecht dem entsprechenden Unterfall des APR
  - das Recht auf Datenschutz könnte indessen spezieller sein als das allgemeine Recht auf informationelle Selbstbestimmung und ähnelt der Gewährleistung in Art. 8 EU-GRCh

- Verhältnis von Landesverfassungsrecht zur Bestimmung im Grundgesetz
  - grundsätzlich Art. 31 GG: „Bundesrecht bricht Landesrecht“
  - anders bei Grundrechten
    - es gilt nicht die Faustformel „Bundesrecht bricht Landesrecht“ aus Art. 31 GG, sondern als *lex specialis* Art. 142 GG
    - danach bleiben Grundrechte der Landesverfassungen insoweit in Kraft, „als sie in Übereinstimmung“ mit Artt. 1-18 GG stehen
    - dies gilt auch für „ungeschriebene“ Grundrechte wie das APR
    - BVerfG: auch weiterreichende Gewährleistungen können gem. Art. 142 GG „in Übereinstimmung“ mit den Artt. 1-18 GG sein

„Art. 142 GG sieht die Geltung der Grundrechte der Landesverfassungen nur vor, soweit sie mit den entsprechenden Rechten des Grundgesetzes übereinstimmen. Das ist der Fall, wenn der Gewährleistungsbereich der jeweiligen Grundrechte und ihre Schranken einander nicht widersprechen. Diese Widerspruchsfreiheit besteht bei Grundrechten, die inhaltsgleich sind, weil sie "den gleichen Gegenstand in gleichem Sinne, mit gleichem Inhalt und in gleichem Umfang" regeln […]. Aber auch soweit Landesgrundrechte gegenüber dem Grundgesetz einen weitergehenden Schutz oder auch einen geringeren Schutz verbürgen, widersprechen sie den entsprechenden Bundesgrundrechten als solchen nicht, wenn das jeweils engere Grundrecht als Mindestgarantie zu verstehen ist und daher nicht den Normbefehl enthält, einen weitergehenden Schutz zu unterlassen […].“

BVerfGE 96, 345, 365 (Landesverfassungsgerichte [1997])

- Folge: Übereinstimmung bei Computer-Grundrecht, hinausgehender Regelungsinhalt beim Datenschutzgrundrecht
  - spezifische landesverfassungsrechtliche Regelungen, die über das Grundgesetz hinausgehen, gelten jeweils in den betreffenden Ländern
  - nur hessische Sachverhalte lassen sich unter das hessische Grundrecht subsumieren, ohne dass sich Bürger anderer Länder auf entsprechende Auslegungen der Bestimmung berufen könnten
  - gleichwohl mag eine eigenständige hessische Rechtsprechung des Staatsgerichtshofs einen Beitrag zur Entwicklung der bundesdeutschen Dogmatik liefern

Betreffen diese Rechte auch den Umgang mit personenbezogenen Daten durch soziale Netzwerke?

- grundsätzlich keine Bindung von Privaten an Grundrechte
- Grundrechte können allenfalls mittelbar über Generalklauseln auch im Verhältnis von Privaten zueinander wirken[2]
- aber informationeller Selbstbestimmung kann auch eine **Schutzfunktion des Staates** entnommen werden
    - Verpflichtung des Staates, Regelungen zu schaffen, die auch in Privatrechtsverhältnissen die personenbezogenen Daten der Bürger schützen
- privatrechtliches Rechtsverhältnis zwischen Nutzer des sozialen Netzwerks und dessen Anbieter
    - als solches nichtgeregelter Vertragstyp: der Anbieter stellt IT-Leistungen – meist unentgeltlich – zur Verfügung, während der Nutzer in die Nutzung und Verarbeitung seiner Daten – insb. zu Werbezwecken – einwilligt
    - hierdurch erhalten soziale Netzwerke Zugang zu einer enormen Menge an personenbezogenen Daten, was aber auch Missbrauch Tür und Tor öffnen kann, Bsp. der Fall *Cambridge-Analytica*
        - der Entwickler einer Umfrage-App hatte Informationen von Facebook-Nutzern unrechtmäßig an *Cambridge Analytica* weitergereicht, welche die Daten als Beauftragte des Wahlkampfteams von US-Präsident Donald Trump analysierte
        - betroffen waren nicht nur die Daten der rund 300.000 Umfrage-Teilnehmer, sondern auch die ihrer Facebook-Freunde
        - ein solcher, weitreichender Zugang zu Nutzerdaten war App-Entwicklern zwischen 2007 und 2014 möglich
    - Folge: das Handeln privater Unternehmen ist für den einzelnen Nutzer mitunter genauso einschneidend, wie eine massenhafte Datensammlung durch den Staat
    - es ergibt sich mithin aus der Schutzpflicht des Staates ein Auftrag die Interessen der Netzwerkbetreiber und –nutzer zu einem Ausgleich zu bringen

[2] Beachte hierzu die neueren Entwicklungen in der Rechtsprechung des BVerfG, insb. BVerfG, NJW 2018, 1667 (Stadionverbot [2018]); dazu auch unten im Rahmen der Meinungsfreiheit, S. 21 f.

III. Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

Wiederholungsfrage: Was umfasst der Schutzbereich des IT-Grundrechts?

Hintergrund

- dem Verfassungsschutz des Landes NRW sollte die Möglichkeit eingeräumt werden, Computer zu überwachen, beispielsweise durch unbemerkt installierte Überwachungssoftware
- in seiner Entscheidung dazu begründete das BVerfG eine neue Ausprägung des APR, um eine Lücke im grundrechtlichen Schutz zu schließen

„Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist.“
BVerfGE 120, 274, 308 (Computer-GR [2008])

Voraussetzungen

- informationstechnisches System (PC, Navigationsgerät, Telefon, etc.)
- das nur vom Betroffenen und gegebenenfalls anderen Berechtigten als eigenes genutzt wird
- muss einen aussagekräftigen Bestand an personenbezogenen Daten beinhalten, der Rückschlüsse auf die Eigenschaften und das Verhalten der Nutzer zulässt

Abgrenzung

- Art. 10 GG: schützt keine Daten, die sich nach Ende des Kommunikationsvorgangs bei einem Kommunikationsteilnehmer befinden
- Art. 13 GG: Eindringen in informationstechnisches System setzt nicht die Überwindung eines raumspezifischen Schutzes voraus, insbesondere nicht körperliches Eindringen in die Wohnung
- Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (informationelle Selbstbestimmung): geht über den Schutzbereich (Erhebung einzelner Daten) weit hinaus

Wie sind Online-Durchsuchungen nun nach der Rechtsprechung des BVerfG im Lichte des Computer-Grundrechts zu beurteilen?

Umfang und Gegenstand von Online-Durchsuchungen

- Infiltration eines informationstechnischen Systems eines Bürgers durch staatliche Stellen, zumeist unbemerkt (heimliche Überwachung)
- Daten-, Informationsbeschaffungs- und Überwachungsmöglichkeiten durch eine Online-Durchsuchung
  - Erstellen von *Screenshots*
  - Raumüberwachung mittels *Web-Cam*
  - Ausspähung der Festplatte
- daher: Schutz vor Online-Durchsuchungen notwendig, denn:

„[e]in Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein“
BVerfGE 120, 247, 313 (Online-Durchsuchungen [2008])

kein generelles Verbot von Online-Durchsuchungen durch das Computer-Grundrecht

- Eingriffe könnten sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein
- um verhältnismäßig zu sein, bedarf es – jedenfalls für heimliche Online-Durchsuchungen eines Geheimdienstes – einer im Einzelfall drohenden Gefahr für ein überragend wichtiges Rechtsgut
- BVerfG fordert geeignete Verfahrensvorkehrungen für heimliche Zugriffe auf informationstechnische Systeme:

„Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.[…] Ein solcher Vorbehalt ermöglicht die vorbeugende Kontrolle einer geplanten heimlichen Ermittlungsmaßnahme durch eine unabhängige und neutrale Instanz.[…] Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil der Betroffene sonst ungeschützt bliebe. Dem Gesetzgeber ist allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, grundsätzlich ein Regelungsspielraum eingeräumt.“
BVerfGE 120, 247, 331 f. (Online-Durchsuchungen [2008])

- vor diesem Hintergrund kann bezweifelt werden, ob § 100b StPO, welcher Online-Durchsuchungen im Ermittlungsverfahren regelt, verfassungsmäßig ist, denn er sieht keinen Richtervorbehalt vor

Vermittelt das Computer-Grundrecht auch eine Schutzpflicht des Staates?

- die wenigsten Bürger sind von einer Online-Durchsuchung betroffen sein
- durch vernetzte Geräte und die Nutzung verschiedener Programme und Applikationen gewähren Nutzer aber privaten Dritten oft Zugang zu ihren informationstechnischen Systemen
  - ein Video-Chat-Programm etwa funktioniert nur, wenn das Programm Zugriff auf die Web-Cam hat
  - eine Navigationssoftware funktioniert nur, wenn Standortdaten mitgeteilt werden
  - das Betriebssystem kann nur aktualisiert werden, wenn die Hersteller-Software in die bereits installierte eingreifen und diese verändern darf (gleiches gilt für Anti-Viren-Programme)
- hier zeigen sich auch die überlappenden Schutzbereiche der Fallgruppen informationelle Selbstbestimmung und Computer-Grundrecht
- der Staat muss hier auch den gesetzlichen Rahmen für einen gerechten Interessenausgleich zwischen Nutzer und Anwendungsanbieter schaffen, ähnlich wie bei der Nutzung sozialer Netzwerke

IV. Recht am eigenen Bild und am eigenen Wort und Schutz der persönlichen Ehre

Wiederholungsfrage: Was umfasst der Schutzbereich der Fallgruppe Darstellung der Person in der Öffentlichkeit?

- der Einzelne soll vor entstellenden und verfälschenden Darstellungen seiner Person bewahrt werden
- dies umfasst mehrere Rechte

Recht am eigenen Bild und Recht am eigenen Wort

„Dieses Grundrecht schützt auch Rechtspositionen, die für die Entfaltung der Persönlichkeit notwendig sind. Dazu gehört in bestimmten Grenzen, ebenso wie das Recht am eigenen Bild, das Recht am gesprochenen Wort. Deshalb darf grundsätzlich jedermann selbst und allein bestimmen, wer sein Wort aufnehmen soll sowie ob und vor wem seine auf einen Tonträger aufgenommene Stimme abgespielt wird.“
BVerfGE 34, 238, 246 (Tonband [1973])

Welche Gefahren für das eigene Bild sind aktuell besonders relevant?

Analyse abweichenden Verhaltens im öffentlichen Raum: Ausbau der flächendeckenden Videoüberwachung

- Kombination von Videoüberwachung mit einer automatischen Auswertung der Bilder durch eine Software zu Verhaltenserkennung
  - System soll Verhaltensmuster erkennen, die von „normalem Verhalten“ abweichen und so eine Möglichkeit bieten bei „abnormalem Verhalten“ zu intervenieren
  - Pilotversuche in Berlin und Mannheim
- hierdurch sollen Gefahren für die öffentliche Sicherheit und Ordnung vermieden werden können

- mögliche grundrechtliche Probleme dieser Überwachung
  - Mustererkennung erzeugt Anpassungsdruck, sodass sich Menschen eher „konform“ verhalten und kein gesellschaftlich nicht toleriertes Verhalten an den Tag legen, aus Sorge um Sanktionen
  - möglicherweise können davon neben dem APR in seiner Ausprägung des Rechts am eigenen Bild und der informationellen Selbstbestimmung auch andere Grundrechte betroffen sein, etwa die Meinungsfreiheit, die Religionsfreiheit, die Versammlungsfreiheit, in jedem Falle aber die allg. Handlungsfreiheit
- Folge der enormen Grundrechtsrelevanz dieser Überwachungsmaßnahmen
  - gesetzliche Ermächtigungsgrundlagen erforderlich
  - diese müssen dann umfassend auch die Verhaltenserkennung erlauben, anders als bisherige Regelungen, vgl. § 14 Abs. 3 und 4 HSOG

Gesichtserkennung durch soziale Netzwerke und anderer Applikationen

- teilweise automatische Gesichtserkennung in sozialen Netzwerken (Bsp. *Facebook*[3]) ermöglicht das leichtere „*taggen*“, also verlinken einer Person mit einem Foto, indem dem Hochladenden gleich passende Vorschläge der auf dem Bild erkannten „Freunde“ unterbreitet werden
- andere Anwendungsbereiche denkbar, etwa
  - Entsperren von Geräten
  - Authentifizierung bei der Anmeldung zu Benutzerkonten oder dem Online-Banking
- wiederum Überlappung der Schutzbereiche der einzelnen Fallgruppen des APR: eigenes Bild in digitaler Form ist ein personenbezogenes Datum und unterfällt auch dem Schutz der informationellen Selbstbestimmung
- wiederum muss zur Sicherung der Interessen des Nutzers ein Interessenausglich mit dem privaten Verwender des Bildes hergestellt werden, sodass auch hier der Schutzfunktion des Staates neben der Abwehrfunktion des Grundrechts eine besondere Bedeutung zukommt

[3] Dazu kurz Schütze, Art. 29-Datenschutzgruppe: Stellungnahme zu automatischer Gesichtserkennung, ZD-Aktuell 2012, 02890; ausführlich *Art. 29-Datenschutzgruppe*, WP 192; Facebook hat in Folge der scharfen Kritik europäischer Datenschützer die automatische Gesichtserkennung wieder deaktiviert.

Wiederholungsfrage: Was ist vom Schutz der persönlichen Ehre erfasst?

„Die […] gegen den Beschwerdeführer gerichteten Angriffe waren geeignet, das verfassungsrechtlich gewährleistete allgemeine Persönlichkeitsrecht des Beschwerdeführers zu beeinträchtigen. Dieses umfaßt unter anderem die persönliche Ehre und das Recht am eigenen Wort; es schützt den Grundrechtsträger auch dagegen, daß ihm Äußerungen in den Mund gelegt werde, die er nicht getan hat und die seinen von ihm selbst definierten sozialen Geltungsanspruch beeinträchtigen […] Insofern kann sich der Betroffene auch bei einer unrichtigen, verfälschten oder entstellten Wiedergabe seiner Äußerungen auf das allgemeine Persönlichkeitsrecht berufen.“
BVerfGE 54, 208, 217 (Böll [1980])

Greift der Ehrschutz aus dem APR bei Cybermobbing?

Cybermobbing umfasst…

- Beleidigungen, Verleumdungen und Stalking im Internet
- also Straftaten gegen die persönliche Ehre, die insb. bei Beleidigungsdelikten auch nicht mehr vom Schutzbereich des Art. 5 Abs. 1 S. 1 Alt. 1 GG erfasst sind
- diese ehrverletzenden Äußerungen treten zumeist in Form von Kommentare und Bilder im Internet auf
- für den Betroffenen ist dies angesichts der nahezu unbegrenzten Dauerhaftigkeit der Äußerungen im Internet – was durch einfache Verbreitung etwa durch Verlinkung mit anderen Seiten noch verstärkt wird – besonders belastend
- Anonymität im Internet senkt die Hürden für ehrverletzendes Verhalten

Schutzpflicht des Staates

- hierbei wird wiederum deutlich, dass die Schutzfunktion der Grundrechte den Staat zur Regelung dieser Fälle verpflichtet
- beispielsweise indem der Staat Rechtschutzmöglichkeiten für betroffene schafft oder Straftatbestände entsprechend anpasst

Rechtschutzmöglichkeiten oft aber nur mangelhaft: Ein Ende der Anonymität im Internet notwendig?

- Anonymität im Internet verhindert privatrechtlichen Ehrschutz gegen die Täter
  - oft lässt sich nicht oder nur schwer nachweisen, wer hinter einem im Internet gebrauchten Pseudonym steckt
  - kein Auskunftsanspruch auf Nennung des Klarnamens durch den Plattformbetreiber ggü. dem Betroffenen[4]

„Der Schutz der Anonymität im Internet endet de lege lata somit auch erst dann, wenn durch die Äußerungen des Nutzers ein Straftatbestand erfüllt ist und die eingeschalteten Strafverfolgungsbehörden Auskunft bei dem Diensteanbieter über die Identität des Nutzers verlangen. Grds. muss der Verletzte also Strafanzeige gegen Unbekannt stellen, anschließend (im Falle der Eröffnung des Strafverfahrens) über die Akteneinsicht (§ 147 StPO) die Identität des Nutzers ermitteln und sodann ein separates Zivilverfahren einleiten.“
***Krupna*, Anm. zu BGH: Kein Anspruch auf Herausgabe von Nutzerdaten bei Persönlichkeitsrechtsverletzung, ZD 2014, 520, 523**

- einige Lösungsvorschläge der Literatur
  - Pflicht zur Verwendung von Klarnamen, was aber zu einem Ende der Anonymität im Internet führte und damit ein besonderes Spezifikum des Internets gerade aufheben würde[5]
  - Konzept des Anonymitätsfolgenausgleichs:[6] ähnlich wie beim strafprozessualen Opferschutz oder der gesetzlichen Haftpflichtversicherung im Straßenverkehr soll danach die Folgen der Anonymität im Internet von der Solidargemeinschaft getragen werden[7]
  - private Cyber-Courts:[8] hiernach sollen Betreiber von Plattformen mit Betroffenem und dem vermeintlichen Täter den Sachverhalt aufklären und auf dieser Grundlage über eine Löschung entscheiden – dabei kann dann auch über die Offenlegung des Klarnamens gegenüber dem Betroffenen entschieden werden

[4] Vgl. BGH, NJW 2014, 2651 ff. (Ärztebewertungsportal [2014]).
[5] Zu dieser Kritik *Glaser*, NVwZ 2012, 1432,1437.
[6] Dazu *Heckrnann*, NJW 2012, 2631, 2632 f..
[7] Ein Überblick der davon umfassten Teilmaßnahmen bei *Hoffmann et al*., Die digitale Dimension der Grundrechte, 2015, S. 93.
[8] *Ladeur/Gostomzyk*, NJW 2012, 710, 714 f.

V. Zusammenfassung: Vom Allgemeinen Persönlichkeitsrecht zum Schutz der digitalen Persönlichkeit

- viele Fallgruppen des APR bieten Schutz für den Bürger auch und gerade im digitalen Raum
- neben der Abwehrfunktion der Grundrechte rückt dabei die Schutzfunktion in den Vordergrund: der Staat ist aufgefordert durch entsprechende Rechtssetzung seine Bürger auch gegen Private zu schützen
- eine unmittelbare Drittwirkung von Grundrechten insb. für große Internetkonzerne besteht hingegen (noch?) nicht

Ein deutsches Sozialkreditsystem?

- nach dem Vorstehenden ist das eingangs dargestellte chinesische Sozialkreditsystem in Deutschland nicht vorstellbar
- weder dürfte der Staat sich aus allen – insb. nicht-staatlichen – Quellen Informationen über seine Bürger zusammensuchen, noch diese unbegrenzt speichern
- die Veröffentlichung von „schwarzen Listen“ ist dem Staat durch den im APR festgeschriebenen Ehrschutz verboten
- eine flächendeckende Videoüberwachung, die das Verhalten der Bürger analysiert, gibt es zumindest in Modellversuchen auch in Deutschland, bedarf aber einer gesetzlichen Ermächtigung, die selbst hohe Hürden erfüllen muss, um verhältnismäßig und damit verfassungsmäßig zu sein

Vertiefende Literaturempfehlungen für einzelne Aspekte der Veranstaltung
- *Kahl/Ohlendorf*, Grundfälle zu Art. 2 I i.V. mit 1 I GG, JuS 2008, 682 ff. - *Siegel*, Grundlagen und Grenzen polizeilicher Videoüberwachung, NVwZ 2012, 738 ff. - *Glaser*, Grundrechtlicher Schutz der Ehre im Internetzeitalter, NVwZ 2012, 1432 ff. - *Giebel,* Zivilrechtlicher Rechtsschutz gegen Cybermobbing in sozialen Netzwerken, NJW 2017, 977 ff. - *Heckmann*, Persönlichkeitsschutz im Internet, NJW 2012, 2631 ff.