F. Digitaler Grundrechtsschutz auf europäischer Ebene

I. Einführung: Digitaler Grundrechtsschutz in der EU-Grundrechte-Charta (EU-GRCh)

"Gerade im Hinblick auf grundlegende Wertentscheidungen des Grundgesetzes wie den Schutz der Würde des Menschen, aber auch Gewährleistungen im Hinblick auf die konstitutive Bedeutung der freien öffentlichen Meinungsbildung besteht eine Pflicht zur aktiven regulatorischen Gestaltung auch unter den Bedingungen des **europäischen Mehrebenensystems**."
Di Fabio, Grundrechtsgeltung in digitalen Systemen, 2016, S. 90.

Was ist die EU-Grundrechtecharta?

- kein Grundrechtskatalog in den Verträgen
  - gem. Art. 6 Abs. 1 EUV kommt der EU-GRCh der Rang rechtsverbindlichen Primärrechts zu
    - allerdings nicht für alle Mitgliedstaaten bindend
    - Vereinigtes Königreich und Polen: keine einklagbaren Rechte aus der Charta, soweit sie nicht im nationalen Recht vorgesehen sind
  - zudem sind über Art. 6 Abs. 3 EUV die Grundrechte der EMRK und Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze weiterhin Teil des Unionsrechts
- Anwendungsbereich Art. 51 EU-GRCh
  - verpflichtet sind Organe, Einrichtungen und sonstige Stellen der Union, wenn sie Unionsrecht erlassen oder vollziehen
  - auch mitgliedsstaatliche Stellen, wenn sie Unionsrecht vollziehen
- Schranken der Unionsgrundrechte
  - Eingriffe in die Bestimmungen der EU-GRCh müssen gesetzlich vorgesehen sein und den Wesensgehalt des Grundrechts beachten
  - dürfen i.S.d. Verhältnismäßigkeitsprinzips nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten/dem Gemeinwohl dienenden Zielsetzungen und Erfordernissen des Schutzes der Rechte und Freiheiten anderer entsprechen, Art. 52 Abs. 1 S. 2 EU-GRCh

- ausnahmsweise Bindung der Mitgliedsstaaten
  - grds. sind Mitgliedsstaaten bei Erlass nationalen Rechts nicht an Unionsgrundrechte gebunden
  - aber: mitgliedsstaatliche Regelungen sind dann an Unionsrecht zu messen, wenn sie im Anwendungsbereich der AEUV erlassen werden oder ansonsten Beurteilung nach unionsrechtlichen Maßstäben erforderlich ist
    - wenn nationale Rechtsvorschriften in Ausfüllung der Vorbehalte (durch AEUV ausdrücklich oder nach EuGH Cassis de Dijon[1]) die Grundfreiheiten einschränken
    - beim unmittelbaren mitgliedsstaatlichen Vollzug des Unionsrecht (etwa einer Unionsverordnung Art. 288 Abs. 2 AEUV)
- digitale Aspekte umfasst der Grundrechtsschutz der Charta in Art. 7 und Art. 8 EU-GRCh

Was schützt Art. 7 EU-GRCh?

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation
Art. 7 EU-GRCh

- schützt u.a. das „Privatleben“
  - Begriff wird umfassend verstanden und ist einer abschließenden Definition nicht zugänglich
  - zentraler Inhalt: Autonomie des Menschen
    - damit ein Recht auf Selbstbestimmung
    - Inhalt kann sich im Zuge sich verändernder gesellschaftlicher Anschauungen weiterentwickeln
- Gewährleistungsinhalt
  - Recht auf Identität und Entwicklung der Person
    - gemeint ist eine geschützte Sphäre, in der eine Person ihr Leben nach ihrer Wahl lebt und ihre Persönlichkeit entwickeln kann
    - wesentliche Elemente: Name, geschlechtliche Ausrichtung, Sexualleben, Identifizierung mit dem Geschlecht, aber auch körperliche Integrität und geistige Gesundheit
  - Möglichkeit, Beziehungen zu anderen Menschen, auch sexueller Art, aufzunehmen, auch geschäftliche und berufliche Aktivitäten
- EuGH greift bei Auslegung auf die vom EGMR zu Art. 8 Abs. 1 EMRK entwickelten Grundsätze zurück[2]

[1] Vgl. EuGH, Rs. 120/78 – *Cassis de Dijon.*
[2] Vgl. EuGH, Rs. C-450/06, ECLI:EU:C:2008:91, Rn. 48 – *Varec.*

Wann liegt ein Eingriff in Art. 7 EU-GRCh vor?

- in Rechte des Art. 7 EU-GRCh wird eingegriffen, wenn Grundrechtsverpflichteter belastende Regelungen zu den geschützten Bereichen erlässt
- Gleiches gilt, wenn er darauf faktisch in einer Weise einwirkt, die einer Regelung vergleichbar ist
    - im Bereich **Achtung des Privatlebens** liegt Eingriff regelmäßig im Eindringen in Privatsphäre; (im Einzelnen stellt etwa Durchsuchung von Personen Eingriff dar, desgleichen eine GPS-Überwachung, weiter die Abnahme von Fingerabdrücken oder die Blutentnahme sowie die Einbehaltung des Personalausweises
    - im Bereich **Achtung des Familienlebens** liegt Eingriff etwa in Entziehung des Sorge- oder Erziehungsrechts
    - im Bereich der **Wohnung** liegt Eingriff bei optischer oder akustischer Überwachung vor
    - im Bereich **Achtung der Kommunikation** stellt jede Maßnahme eines Grundrechtsverpflichteten einen Eingriff dar, die den Kommunikationsvorgang betrifft und zur Kenntnis der Kommunikationsinhalte oder Kommunikationsdaten (etwa Zeitpunkt, Absender, Adressat etc.) führt
    - typische Fälle sind Briefkontrolle oder das Abhören von Telefon oder die Beobachtung der Internetnutzung
- zur Rechtfertigung von Eingriffen in Art. 7 EU-GRCh siehe unten (Fall: Vorratsdatenspeicherung)

Was schützt Art. 8 EU-GRCh?

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) [1]Diese 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. [2]Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Art. 8 EU-GRCh

- Art. 8 EU-GRCh schützt personenbezogene Daten
  - als personenbezogene Daten werden alle Informationen über eine bestimmte oder bestimmbare natürliche Person eingestuft
  - bestimmbar ist eine Person, die direkt oder indirekt identifiziert werden kann
  - Daten müssen eine natürliche Person betreffen
  - erfasst werden Informationen, die die Privatsphäre i.e.S. einschließlich der Intimsphäre betreffen
  - Daten ohne Personenbezug werden hingegen nicht erfasst
- keine Rolle spielt Art der Speicherung der Daten und ob sie allgemein zugänglich sind

Wann liegt ein Eingriff in den Schutzbereich des Art. 8 EU-GRCh?

- Eingriff liegt vor, wenn personenbezogene Daten „verarbeitet" werden
  - „Verarbeiten" ist als Oberbegriff für alle datenbezogenen Vorgänge zu verstehen, nämlich das:
    - Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten
    - dabei kommt es nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben
  - Beispiele für typische Eingriffe:
    - Arbeitgeber leitet Daten über die Einkünfte eines Arbeitnehmers oder eines Ruhegehaltsempfängers an einen Dritten weiter
    - persönliche Daten von Empfängern von Agrarbeihilfen werden veröffentlicht
    - biometrische Daten werden im Reisepass gespeichert und Kommunikationsdaten werden gespeichert
    - Nutzerdaten werden an Drittstaaten (hier: USA) weitergegeben, in denen staatliche Behörden ggfs. unbegrenzten Zugriff auf diese Daten haben
    - Vorratsdatenspeicherung (siehe dazu Fall unten)
- kein Eingriff ist bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber ohne Weitergabe an Dritte
- zur Rechtfertigung von Eingriffen in Art. 8 EU-GRCh siehe unten (Fall: Vorratsdatenspeicherung)

II. Übungsfall zur Art. 7 und Art 8 EU-GRCh: Vorratsdatenspeicherung

Sachverhalt[3]

Der schwedische Gesetzgeber erließ Vorschriften, mit denen er in Schweden ansässige Betreiber elektronischer Kommunikationsdienste verpflichtete, sämtlich Verkehrs- und Standortdaten der Telekommunikation anlass- und unterschiedslos auf Vorrat zu speichern (sog. Vorratsdatenspeicherung), um den Behörden des Landes Zugriff auf die gespeicherten Daten einzuräumen. Damit setzte der schwedische Gesetzgeber die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung sowie die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation um. Bei den erfassten Daten handelt es sich u.a. um Angaben, die zur Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie zur Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte erforderlich sind. Dazu gehören Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden Anschlusses und des angerufenen Anschlusses sowie bei Internetdiensten die IP-Adresse.

Sowohl die Richtlinien- als auch die Gesetzesbegründung geben an, dass die erhobenen Daten ein wichtiges Mittel bei der Terrorbekämpfung und insbesondere der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten darstellen sollten. Zudem enthält das schwedische Gesetz Vorschriften zum Datenschutz und zur Datensicherheit.

Verletzt das schwedische Gesetz die EU-GRCh?

[3] Nach EuGH, Urt. v. 21.12.2016 – C 203/15 u.a.

OS: Das schwedische Gesetz stellt eine Verletzung der EU-GRCh dar, wenn sie anwendbar ist, das Gesetz in den Schutzbereich der Grundrechte eingreift und dieser Eingriff nicht gerechtfertigt ist

I. Anwendbarkeit der EU-GRCh

- da das schwedische Gesetz europäische Richtlinien umsetzt, handelt es sich um Durchführung von Recht der Union i.S.d. Art. 51 Abs. 1 S. 1 EU-GRCh
- Folge: EU-GRCh ist anwendbar

II. Schutzbereich

- in Betracht kommt eine Verletzung der Grundrechte aus Art. 7 Abs. 1 EU-GRCh, Art. 8 Abs. 1 EU-GRCh sowie Art. 11 Abs. 1 EU-GRCh
  - **Art. 7 EU-GRCh** gewährleistet Schutz des Privat- und Familienlebens inklusive dazugehörigen Kommunikation
    - aus Gesamtheit, der von der gesetzlichen Regelung erfassten Daten, können **sehr genaue Schlüsse auf Privatleben** der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden (z.B. Gewohnheiten, ständige oder vorübergehende Ortsveränderungen)
    - Daten ermöglichen darüber hinaus **Erstellung des Profils** der betroffenen Personen
    - Schutzbereich von Art. 7 EU-GRCh folglich betroffen
  - **Art. 8** Abs. 1 **EU-GRCh** gewährleistet den Schutz personenbezogener Daten
    - Daten, die von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert werden, ermöglichen Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte
    - zu diesen Daten gehören Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden und des angerufenen Anschlusses sowie bei Internetdiensten der IP-Adresse
    - Schutzbereich von Art. 8 EU-GRCh ist eröffnet
  - **Art. 11 EU-GRCh** erfasst alle Aspekte und Formen kommunikativen Verhaltens, von der inhaltbezogenen Freiheit, eine bestimmte Meinung zu bilden, haben und äußern zu dürfen bis zu den medialen Verbreitungsformen
    - vorliegend kann nicht ausgeschlossen werden, dass das Wissen um eine Vorratsdatenspeicherung Auswirkungen auf Kommunikationsverhalten der Betroffenen hat
    - Schutzbereich des Art. 11 EU-GRCh ist ebenfalls eröffnet

III. Eingriff

- Eingriff ist jede Verkürzung des grundrechtlichen Schutzbereichs durch ein grundrechtsgebundenes Organ
  - Speicherung der entsprechenden Daten hat nachteilige Auswirkung auf geschützten Freiheiten, insbesondere vor dem Hintergrund, dass sie **systematisch, kontinuierlich und anlasslos** erfolgt
  - weitere Benachteiligungen der schwedischen Bürger liegen in Verarbeitung gespeicherter Daten sowie in Gestattung des Zugriffs durch zuständige Behörde
  - Eingriff kann schwedischem Staat auch **zugerechnet** werden, da Speicherung durch Privatunternehmen aufgrund einer gesetzlichen Verpflichtung
- ein Eingriff liegt damit vor

IV. Rechtfertigung

- Eingriff könnte gem. Art. 52 Abs. 1 EU-GRCh gerechtfertigt sein, wenn muss jede Einschränkung der Ausübung der Rechte und Freiheiten der EU-GRCh gesetzlich vorgesehen sein, den **Wesensgehalt** der Rechte und Freiheiten achten sowie **verhältnismäßig** sein
- erfolgen Eingriffe durch Mitgliedstaat der Union, ist nach Art. 52 Abs. 1 S. 1 Hs. 1 EU-GRCh nationales Gesetz erforderlich, dass Eingriffe gestattet bzw. regelt.
  - ein solches Gesetz liegt in Umsetzung der europäischen Richtlinie vor
- ferner müsste schwedische Gesetzgeber Voraussetzungen gewahrt haben, die EU-GRCh an Eingriffe an Grundrechte stellt
  - deshalb sind nur solche Eingriffe gerechtfertigt, die **Wesensgehalt** der Grundrechte nicht antasten, Art. 52 Abs. 1 S. 1 Hs. 2 EU-GRCh
    - der mit der schwedischen Regelung über Vorratsdatenspeicherung einhergehende Eingriff in die Art. 7, 8 EU-GRCh ist von großem Ausmaß und als besonders schwerwiegend anzusehen
    - ferner ist Umstand, dass Vorratsdatenspeicherung vorgenommen wird, ohne dass Nutzer der elektronischen Kommunikation darüber informiert werden, geeignet, bei Betroffenen Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist
    - allerdings erstreckt sich Vorratsdatenspeicherung **nicht auf Inhalt** der Kommunikation
    - zudem enthält schwedische Gesetz Vorschriften zum Datenschutz und zur Datensicherheit
    - Wesensgehalt der betroffenen Grundrechte nicht betroffen

- gem. Art. 52 Abs. 1 S. 2 EU-GRCh dürfen Eingriffe in Grundrechte nur unter Wahrung des **Grundsatzes der Verhältnismäßigkeit** erfolgen
  - legitime Ziele
    - Vorratsdatenspeicherung erfolgt zum Zweck, **terroristische Anschläge** zu verhindern und die Bekämpfung schwerer Kriminalität zu fördern
  - Geeignetheit
    - angesichts Bedeutung elektronischer Kommunikationsmittel – gerade bei Begehung schwerer Straftaten – stellen Vorratsdatenspeicherung und die Möglichkeit, Daten abzurufen für Gefahrenabwehr bzw. Strafverfolgungsbehörde **nützliches und effektives Mittel** dar
  - Erforderlichkeit
    - angesichts der Bedeutung moderner Kommunikationsmittel bei Planung und Durchführung schwerer Straftaten stoßen bisherigen Ermittlungsmethoden der Sicherheitsbehörden an ihre Grenzen, sodass **mildere Maßnahmen nicht gleich effektiv sind**
    - ***Hinweis:*** *Gerichtshof belässt es bei Prüfung der Erforderlichkeit nicht bei der Auseinandersetzung mit milderen Mitteln, sondern nimmt zugleich Abwägung zwischen verfolgten Ziel und betroffenen Grundrechten vor; „**damit entfällt Prüfung der Angemessenheit!“***
  - bei zusätzlich vorzunehmenden Abwägung ist zunächst zu berücksichtigen, dass Bekämpfung schwerer Kriminalität und des Terrorismus von größter Bedeutung für Gewährleistung der öffentlichen Sicherheit ist und dass Wirksamkeit in hohem Maß von Nutzung moderner Ermittlungstechnik abhängt; diesem gewichtigen Interesse stehen auch schwerwiegende Grundrechtseingriffe gegenüber:
    - aufgrund Schwere der Grundrechtseingriffe kann Vorratsdatenspeicherung nur erfolgen, wenn sie auf **absolut Notwendige** beschränkt wird
    - nationale Regelung ist daher nur dann erforderlich, wenn sie klare und präzise Regeln über Tragweite und Anwendung der Vorratsdatenspeicherung enthält
    - gesetzliche Regelung muss insbesondere Aussage darüber treffen, **unter welchen Umständen und unter welchen Voraussetzungen** Daten auf Vorrat gespeichert werden dürfen
    - schwedische Gesetz ordnet Vorratsdatenspeicherung anlasslos und allumfassend an; **keine Differenzierung**, Einschränkung oder Ausnahme
    - gilt auch für Personen, bei denen keinerlei Anhaltspunkte dafür bestehen, dass ihr Verhalten in einem Zusammenhang mit schweren Straftaten stehen
    - zudem sieht schwedische Gesetz **keine Ausnahme** vor, sodass Regelungen auch für Personen gelten, deren Kommunikation nach nationalen Rechtsvorschriften dem Berufsgeheimnis unter-

liegen
- Vorratsdatenspeicherung ist weiterhin nur zulässig, wenn sie nach objektiven Kriterien erfolgt, die **Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel** herstellen; nur auf diese Weise kann Maßnahme und infolgedessen auch der betroffene Personenkreis begrenzt werden
- objektive Anknüpfungspunkte müssen deshalb geeignet sein, zumindest mittelbaren Zusammenhang der betroffenen Personen oder Daten mit schweren Straftaten sichtbar zu machen
- eine solche Begrenzung lässt sich ggf. auch durch geografisches Kriterium gewährleisten, wenn zuständige Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden
- diesen Vorgaben wird schwedische Regierung nicht gerecht
- sie verlangt keinen Zusammenhang zwischen Daten, deren Vorratsdatenspeicherung vorgesehen ist und einer Bedrohung der öffentlichen Sicherheit
- insb. beschränkt sie Vorratsdatenspeicherung weder auf Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten oder des Terrorismus beantragen könnten

▪ folglich ist Regelung nicht erforderlich und **verletzt damit Grundsatz der Verhältnismäßigkeit**

V. Ergebnis: das schwedische Gesetz über die Vorratsdatenspeicherung verletzt die Artt. 7, 8 Abs. 1 und 11 Abs. 1 EU-GRCh

Hinweis

Mit einer vergleichbaren Argumentation hat der Gerichtshof auch die Verletzung der EU-GRCh durch die Vorratsdatenspeicherungsrichtlinie (RL 2006/24/EG) festgestellt und diese für unionsrechtswidrig erklärt.[4] Die den schwedischen Regelungen entsprechende deutsche Vorschrift über die Vorratsdatenspeicherung wurde vom BVerfG für verfassungswidrig erklärt und aufgehoben.[5] Eine neue eingeführte Verpflichtung deutscher Telekommunikationsunternehmen halten erste Gerichte ebenfalls für unionsrechtswidrig.[6]

[4] EuGH ZD 2014, 296 (Digital Rights Ireland [2014]).
[5] BVerfGE 125, 260 (Verfassungswidrige Vorratsdatenspeicherung von Telekommunikationsdaten [2014]); dazu auch *Roßnagel* NJW 2016, 533, 539.
[6] OVG Münster NVwZ-RR 2018, 43 (Stopp der Vorratsdatenspeicherung [2017]).

III. Erweiterung des digitalen Grundrechtsschutzes auf europäischer Ebene – die Digitalcharta?

Wieso ist es sinnvoll, über Digitalgrundrechte auf europäischer Ebene nachzudenken?

- für viele Bürger ist Hergabe ihrer personenbezogenen Daten für die im Gegenzug ihnen „for free" angebotenen Dienste der US-amerikanischen Internetgiganten nebensächlich: rechtsgeschäftlich relevante Vorstellungen verbinden sie damit in aller Regel nicht
- jetzt aber legt Skandal um Facebook und Cambridge Analytica den Verdacht nahe, dass 50 Millionen User – ohne dass sie es wussten – in ihrer freien Wahlentscheidung nachhaltig durch einseitige Beeinflussung manipuliert worden sein könnten
- das Ergebnis der amerikanischen Wahlen wäre dann, wenn sich denn dieser Verdacht erhärtet, kaum noch als demokratisch zu bezeichnen.
- unter dem Eindruck dieser Ereignisse erscheint es dringend, den Blick auf eine europarechtlich zu verankernde „Digitalcharta" zu werfen

Was ist die Digitalcharta?

- die Charta der Digitalen Grundrechte der Europäischen Union („Digitalcharta") ist eine Bürgerinitiative der Zeit-Stiftung, die eine allgemeine und rechtlich verbindliche schriftliche Niederlegung von Grundrechten in der digitalen Welt auf europäischer Ebene fordert
  - wurde am 30. November 2016 auf Deutsch, Englisch, Französisch und Spanisch veröffentlich
  - Entwicklung der Digitalcharta dauerte 14 Monate
- mit der Digitalcharta wurden die von den Initiatoren erwünschten digitalen Grundrechte in der Europäischen Union umfassend schriftlich niedergelegt
  - Urhebern ging es nicht darum einen verfassungsgebenden Text, sondern Grundlage für gesellschaftliche Diskussion über Grundrechte im digitalen Zeitalter auf europäischer Ebene vorzulegen
  - Digitalcharta soll im Ausschuss für bürgerliche Freiheit, Justiz und Inneres des Europäischen Parlaments vorgestellt werden
  - sie beginnt mit Präambel, in der Anerkennung der Allgemeinen Erklärung der Menschenrechte, der EMRK und der Grundrechts- und Datenschutzstandards der Europäischen Union und ihrer Mitgliedstaaten ausgedrückt wird, und setzt sich fort in 18 Artikeln

Braucht Europa eine Digitalcharta?

e.A.: Digitalcharta ist notwendig	e.A.: Digitalcharta ist nicht notwendig
- durch Anspruch einer EU-weit gültigen, einheitlichen Digitalcharta wird Handlungs- und Abwehrbereich des Einzelnen auf größeres Gebiet ausgeweitet; dadurch werden nicht nur Rechte gegenüber dem eigenen Staat, sondern auch auf höherer Instanz gegen die EU gestärkt - Wortlaut der Digitalcharta ist noch nicht vollständig ausgereift; es soll zunächst lediglich eine Debatte über die Zukunft der digitalen Gesellschaft und wie man sie politisch gestalten kann entstehen	- handelt sich nur um eine deutsche Aktion: Diskussion über eine Digitalcharta müsste aber europaweit geführt werden - keine Notwendigkeit für Digitalcharta, da bereits europäischer Grundrechtsschutz für digitale Sachverhalte besteht o EU-GRCh ist umfassend und lässt Raum für Neuentwicklung und Neuinterpretationen; gilt insbesondere für Art. 7 und Art. 8 EU-GRCh o Verfasser richten starren Blick auf tatsächliche und vermeintliche Gefahren der Vernetzung: Das Internet als Hochrisikozone, in der die „normalen“ Grundrechte zum Schutz der Bürger nicht mehr ausreichen - kein umfassender Grundrechtekatalog: wichtige Grundrechte wie Versammlungsfreiheit und Vereinigungsfreiheit kommen in der Digitalcharta nicht vor

Soll die Digitalcharta eine unmittelbare Wirkung der Grundrechte begründen?

- Hintergrund: Art. 23 Abs. 3 der Digitalcharta in der Fassung von 2016 lautete:

(3) [1]Rechte und Pflichten aus dieser Charta gelten für alle Unternehmen, die auf dem Gebiet der EU tätig sind. [2]Die Festlegung eines Gerichtsstands außerhalb der EU ist unzulässig.
Art. 23 Abs. 3 Digitalcharta

- Art. 23 Abs. 3 Digitalcharta wurde in der Fassung von 2018 gestrichen
- eine unmittelbare Wirkung der Grundrechte wird folglich auch auf EU-Ebene diskutiert
- fraglich ist, welche Argumente dafür und dagegen sprechen

Bedarf es einer unmittelbaren Grundrechtsbindung Privater auf europäischer Ebene?	
e.A.: es bedarf einer unmb. Grundrechtsbindung Privater	**a.A.: keine unmb. Grundrechtsbindung Privater notwendig**
- insbesondere die Vertreter von Big Data (Google, facebook etc.) nehmen gegenüber dem Bürger eine dem Staat vergleichbare Stellung ein - EuGH hat in Urteil Google Spain[7] bereits ein „Recht auf Vergessenwerden“ von Privaten gegenüber den Betreibern einer Suchmaschine anerkannt und dieses auf Art. 7 und 8 EU-GRCh gestützt	- Grundrechte sind Abwehrrechte des Bürgers gegen den Staat - Überlastung des Gerichtshofs - Privatrecht würde an Komplexität gewinnen, weil seine Auslegung wie Anwendung dann auch im Rahmen der Konformität zum Primärrecht der Union im Rahmen der Auslegungshoheit des EuGH durchzuführen ist

Literaturempfehlungen
- *Priebe*, Vorratsdatenspeicherung und kein Ende, EuZW 2017, 136 - *Graf von Westphalen*, Digitale Charta – Erweiterung der europäischen Grundrechte für das digitale Zeitalter - *Graf von Westphalen*, Digitale Grundrechte für Europa – eine Initiative der Zivilgesellschaft, BB 2018, Heft 31, Umschlagteil I - *Härting*, „Digitale Grundrechte“ – warum eigentlich?, LTO v. 01.12.2016

[7] EuGH NJW 2014, 2257 (Anspruch auf Datenlöschung gegenüber Google – „Recht auf Vergessenwerden“ [2014]).