Humanistische Union

Digitale Grundrechte

aus: vorgänge Nr. 209 (Heft 1/2015), S. 99-101

(Red.) Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/Kim Corinna Borchers, Die digitale Dimension der Grundrechte. Das Grundgesetz im digitalen Zeitalter. [DIVSI-Perspektiven Bd. 2, hrsg. vom Deutschen Institut für Vertrauen und Sicherheit im Internet], Baden-Baden 2015 (Nomos), 221 S., 57.- €.

Die vorliegende Studie entstand im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), einer von der Deutschen Post finanzierten, gemeinnützigen Gesellschaft. Diese will eine „Plattform für einen offenen und transparenten Dialog zu Vertrauen und Sicherheit im Internet“(1) sein.

Die Autor_innen stellen zunächst in kurzen Worten das Konzept der „digitalen Dimension der Grundrechte“ vor, die „keine eigenständige Grundrechtsfunktion [darstelle], wie es bspw. die Abwehrfunktion, die Schutzpflicht- bzw. Gewährleistungsdimension, originäre Leistungsansprüche sowie die Drittwirkung sind. Es handelt sich um eine zusammenfassende Beschreibung eines Teilbereichs des jeweiligen Schutzgehalts, der sich durch den besonderen Bezug zur Informationstechnik bzw. zum Internet auszeichnet.“ (S. 20) Das für die digitale Sphäre eine eigene Kategorie bzw. Dimension des Grundrechtsschutzes eingeführt werde, rechtfertige sich schon dadurch, dass es sich bei der Informationstechnologie um „die entscheidende Infrastruktur der nächsten Jahrzehnte“ (S. 21) handle. Die Weiterentwicklung der Grundrechte folge dabei dem Grundsatz, dass die freiheitlichen Schutzgarantien unabhängig davon gelten, ob sich das betreffende Verhalten der Bürger_innen in der analogen oder digitalen Welt abspielt. Entsprechend finden sich in der Studie immer wieder Analogien, in denen digitale Streitfragen in die analoge Welt übersetzt und mit den dortigen Rechtsständen verglichen werden; eine Methode, die manche interessante Anregung bietet, aber nicht besonders innovativ ist, wird so doch lediglich der Status quo der Rechtsentwicklung auf neue Bereiche übertragen.

Die eigentliche Untersuchung beginnt (S. 25 ff.) mit der digitalen Dimension der Menschenwürde (Art. 1 Abs. 1 GG), um sich anschließend allen speziellen Grundrechten und deren digitaler Bedeutung zu widmen. Unter den einzelnen Artikeln wird i.d.R. die herrschende Meinung der Rechtsprechung zu den Inhalten und der Reichweite der jeweiligen Schutzbereiche erläutert und anschließend an zahlreichen Anwendungsbeispiele erläutert. Dazu gehören etwa die sog. Online-Streifen von Sicherheitsbehörden im Netz (als möglicher Eingriff in die allgemeine Handlungsfreiheit) und das Recht auf Vergessen (Allgemeines Persönlichkeitsrecht), der Umgang mit personenbezogenen Daten in sozialen Netzwerken (Recht auf informationelle Selbstbestimmung), die teils unkontrollierbaren Zugriffe von Programmen und Apps auf Benutzersysteme und deren Daten (IT-Grundrecht), von Cybermobbing über die Netzneutralität (deren Herleitung aus dem Diskriminierungsverbot verneint wird) bis zum „Recht auf Internet“ (Gewährleistung eines menschenwürdigen Existenzminimus).

An den Fallbeispielen wird erkennbar, wie sich der Wandel der Lebens- und Kommunikationsformen in der juristischen Debatte niederschlägt. Ein zentrales Moment, auf das die Autor_innen immer wieder zu sprechen kommen, ist der Umstand, dass sich im Internet hauptsächlich private Nutzer_innen und Anbieterfirmen gegenüber stehen. „Der Eingriff in das Recht auf informationelle Selbstbestimmung ist nicht staatlich initiiert, sondern kommt von privater Seite. Überdies ist er – selbst wenn die hohen Anforderungen des deutschen (…) Datenschutzrechts an eine Einwilligung nicht eingehalten werden – freiwillig.“ (S. 68) Entsprechend wird diskutiert, ob die kostenlosen Angebote sozialer Dienste im Internet nicht als Austauschverhältnis verstanden werden müssen, bei dem die Benutzung des Dienstes mit der Verwertung der anfallenden privaten Daten durch die Anbieter „verrechnet“ werden können, dass also grundrechtliche

Ansprüche (zumindest teilweise) veräußert und monetarisiert werden können: „Für eine solche Sichtweise spricht auch der Umstand, dass personenbezogenen Daten, insbesondere in sozialen Netzwerken [wie Facebook], ein erheblicher monetärer Wert zugeordnet wird … Branchenintern wird der Wert eines registrierten Online-Kunden mit 50 bis 100 US-Dollar beziffert. Der Wert eines Facebook-Fans liegt für das Unternehmen bei 136 US-Dollar.“ (S. 52, vgl. a. S. 53). Ob aus solchen brancheninternen Kalkulationen, die in der Selbstdarstellung der Anbieter tunlichst verborgen werden, abgeleitet werden kann, dass die Benutzer_innen etwa mit der Anmeldung bei Facebook dem Geschäftsmodell dieser Firma bewusst zustimmen, muss ernsthaft bezweifelt werden.

Ob sich aus der Vielzahl privater Anbieter im Internet zudem der Schluss ziehen lässt, dass die klassische Schutzfunktion der Grundrechte als Abwehrrechte gegenüber dem Staat ausgedient habe, darf auch bezweifelt werden. Dass die Autor_innen zu dieser Einschätzung gelangen, hat auch mit ihrer Bewertung staatlicher Eingriffe in die digitale Kommunikationswelt zu tun: Hier sei nur auf das Anwendungsbeispiel der sog. Online-Streifen verwiesen, bei denen Polizeibehörden oder Geheimdienste offene Daten auf Webseiten erheben oder verdeckt in soziale Netzwerke eindringen und dort persönliche Statusnachrichten, Bilder und dergleichen mehr abgreifen (s. 38ff.). Einerseits bestätigen die Autor_innen, dass viele Nutzer_innen selbst dann, wenn sie den Adressatenkreis ihrer Nachrichten nicht mehr überschauen können, diese Informationen dennoch nicht in staatliche Hände geben wollen – und stimmen dennoch der herrschenden Rechtsprechung zu, die einfach unterstellt, dass soziale Netzwerke von Firmen und Institutionen (und somit auch von Sicherheitsbehörden) genutzt werden, die Benutzer ihre Einwilligung in die staatliche Kenntnisnahme der dort geposteten Inhalte erteilt hätten, selbst wenn diese nur an Freundeskreise gerichtet seien und selbst dann, wenn sich die Behörden dabei verdeckter (also nicht als behördliche Nutzer erkennbarer) oder gekaperter Accounts (z.B. von vermeintlichen Freund_innen) bedienen. Derart verschleierte Benutzeranmeldungen verstoßen nicht nur gegen die Regeln vieler Anbieter wie Facebook, die eine Anmeldung mit Klarnamen verlangen, sondern konterkarieren auch die Erwartungshaltung der Nutzer_ innen, denen seitens der Anbieterfirmen eine Authentizität der Benutzer_innen suggeriert wird (vgl. S. 42 f.).

Leider ist die Studie nicht immer in sich schlüssig – was vermutlich der umfangreichen Autor_innenschaft geschuldet ist: So wird beispielsweise bei der eben genannten Online-Streife die staatliche Kenntnisnahme von Nachrichten, Bildern etc. in abgeschlossenen Netzwerken wie Facebook als zulässig angesehen, da sich diese Äußerungen an einen „nicht weiter abgegrenzten Personenkreis richten“ (BVerfG, zit. n. S. 42), die damit als öffentliche Informationen behandelt werden dürfen. Ihre Kenntnisnahme durch staatliche Stellen wird nicht einmal als Grundrechtseingriff bewertet (ebd.) – es sei denn, diese Informationen würden massenhaft erhoben und ausgewertet. Wenige Seiten später wird hingegen betont, dass in der digitalen Welt (im Gegensatz zur Realwelt) keine wirklichen öffentlichen Räume existierten, mithin alles Handeln dort eher privaten Charakter trage: „Es gibt keine den Straßen vergleichbaren Internetseiten, vielmehr befindet sich derjenige, der sich im Internet bewegt, in der Regel auf privat betriebenen Homepages, deren Betreibern ein virtuelles Hausrecht zukommt. Insbesondere im Bereich sozialer Netzwerke … [sollen] die jeweiligen Inhalte … gerade nicht der gesamten Internetöffentlichkeit preisgegeben werden.“ (S. 66 f.)

Dennoch bietet die Studie bietet einen Zugang zu vielen Aspekten des digitalen Grundrechtsschutzes, der an vielen Stellen jedoch – notgedrungen – oberflächlich bleibt. Neue Impulse für politische oder sachliche Lösungen der Probleme in der Digitalwelt oder konkrete Vorschläge zur Weiterentwicklung grundrechtlicher Schutzbereiche finden sich nur vereinzelt: etwa bei der Forderung, die Schutzfunktion der Grundrechte und ihre Drittwirkung (auf das Verhältnis zwischen Privatleuten) im Verfassungstext (stärker) abzubilden (S. 18); beim Vorschlag, die Online-Streife als explizite Ermittlungsmaßnahme im Polizei- und Ordnungsrecht sowie in der StPO zu verankern (S. 44) oder in der Kritik an der historisch bedingten Verengung der Pressefreiheit auf körperliche Druckerzeugnisse (S. 143). Hier hätte eine Beschränkung auf zentrale Problemfelder – etwa der informationellen Selbstbestimmung, des IT-Grundrechts und des Fernmeldegeheimnisses (das auf lediglich vier Seiten abgehandelt wird) – sicher gut getan. In der vorliegenden Fassung erweckt die Studie allein den Eindruck, der Grundrechtsschutz in der digitalen Welt wäre insoweit in Ordnung und bedürfte nur noch marginaler Korrekturen. Brisante staatliche Eingriffe in IT-

Infrastrukturen wie die Vorratsdatenspeicherung, die staatliche Abschaltung von Kommunikationsnetzen, der Einsatz von IMSI-Catchern, stillen SMS oder heimlichen Online-Durchsuchungen sucht man vergebens unter den Anwendungsbeispielen – oder sie werden dort höchst verharmlosend dargestellt. Damit erfüllt die Studie nur bedingt den Anspruch ihres Auftraggebers: das „Vertrauen der Menschen in das Internet zu fördern“(2).

Sven Lüders
ist gelernter Soziologe und Geschäftsführer der Humanistischen Union

Anmerkungen:

(1) DIVSI, Mission Statement, abrufbar unter https://www.divsi.de/ueber-uns/das-institut/mission-statement/ .

(2) DIVSI, ebd.

---

https://www.humanistische-union.de/publikationen/vorgaenge/209/publikation/digitale-grundrechte/
Abgerufen am: 27.04.2024