Buchbesprechung: Bull, Hans Peter, Netzpolitik: Freiheit und Rechtsschutz im Internet (Baden-Baden 2013)

Glaser, Andreas

BUCHBESPRECHUNGEN

Ambrock, Jens, Die Übermittlung von S.W.I.F.T.-Daten an die Terrorismusaufklärung der USA. Schriften zum Öffentlichen Recht, Band 1255. Berlin 2013, Duncker und Humblot. 241 S.

Die Informationserhebung der Sicherheitsbehörden und die europäisch-amerikanische Kooperation in diesem Bereich sind durch den NSA-Skandal in eine fundamentale Akzeptanzkrise geraten. Das gilt nicht nur für die Praxis, sondern auch für die Rechtsgrundlagen (dazu *Wolf*, JZ 2013, 1039; *Mayer*, Verfassungsblog vom 18. 11. 2013). Wer tut was im Netz? Wer darf was im Netz? Und wer darf was auf deutschem Boden? Das tradierte Konzept einer rechtlichen Begrenzung von Polizei und Nachrichtendiensten bei gleichzeitiger limitierter Ermächtigung dieser Behörden zu begrenzten Zwecken scheint an der Praxis zu zerschellen, und das über ein Jahrzehnt nach den Attentaten vom 11. September 2001. Die Globalisierung der Informationsnetze macht diese anfällig für den Nachrichtenhunger der Dienste aller Länder. Schon vor einem Jahrzehnt ist dem Telekommunikationsgeheimnis eine „offene Flanke" hinsichtlich seiner internationalen Dimension attestiert worden. Und was damals am Beispiel des Funkverkehrs exemplifiziert werden konnten, potenziert sich nun im Netz. Insider der Nachrichtendienstwelt sind zwar nicht überrascht über die technischen Möglichkeiten und das faktische Stattfinden der neuen Formen von Rasterfahndung im Netz, wohl aber über deren Ausmaß. Und gegenwärtig sind zentrale Fragen noch nicht einmal geklärt, geschweige denn beantwortet: In welchem Maße haben sich deutsche Stellen an der massenhaften Ausspähung des Netzes beteiligt? Und was geschah von deutschem Boden aus? Auch wenn wir durch die Enthüllungen von *E. Snowden* nun über Aktivitäten der USA und einiger ihrer Kooperationspartner besser informiert sind, so bedeutet dies nicht, dass Vergleichbares nur durch sie stattfindet oder zumindest projektiert ist. Umso wichtiger ist es, die rechtlichen und technischen Möglichkeiten sowie Grenzen möglicher Schutzmaßnahmen auszuloten.

Ambrock hat sich einer vermeintlich äußerst speziellen Materie angenommen: des SWIFT-Abkommens, welches in der Öffentlichkeit eher zufällig und außerhalb seines eigentlichen Anwendungsbereichs Aufmerksamkeit erlangte, nämlich im Kontext der Übermittlung von Fluggastdaten an amerikanische Sicherheitsbehörden. Hier entstand ein Vorläufer der Vorratsdatenspeicherung. Dabei regelt das Abkommen eigentlich Folgefragen der Abwicklung des internationalen Zahlungsverkehrs. Anwendungsbereich und Zustandekommen des Abkommens bilden den 1. Abschnitt des Buches (S. 19–62). Am Anfang stand die Trennung zweier Datennetze der privaten Society For Worldwide Interbank Financial Telecommunication (SWIFT) zur Abwicklung namentlich des transatlantischen Zahlungsverkehrs. Da nun ein amerikanisches und ein europäisches Netz mit nur ganz limitierten Verbindungen untereinander entstanden, stand letzteres der US-amerikanischen Fahndung nach den Finanzquellen des internationalen Terrorismus nur noch sehr eingeschränkt offen. Um dennoch beides – Zahlungsverkehr und Fahndung – zu ermöglichen, wurde das Abkommen zur Informationsübermittlung geschlossen. Die Darstellung ist detailliert und sehr kenntnisreich; man merkt der Untersuchung an, dass der Autor an einem auf internationales Wirt-

schaftsrecht fokussierten Lehrstuhl gearbeitet hat. Aber damit nicht genug. Zugleich wird deutlich, dass das Verfahren zur Ratifikation des Abkommens in Europa zu einem Testfall der neuen EU-„Verfassungsarchitektur" nach dem Vertrag von Lissabon wurde. Das EU-Parlament, das dem Vertrag am Ende zustimmte, wollte sich seine Mitwirkungsrechte nicht nehmen lassen. Die drohende Kollision zwischen Völkerrecht einerseits und Europarecht andererseits konnte erst im letzten Moment abgewendet werden. Der nachfolgende, sehr gründliche Abschnitt befasst sich mit dem Inhalt des Abkommens und seiner Vereinbarkeit mit dem EU-Datenverarbeitungsstandard – dem Art. 8 GRC sowie Art. 8 EMRK –, wobei zwischen Informationserhebung, -speicherung und -auswertung unterschieden wird. Diese Untersuchung ist gleichfalls sehr gründlich, steht allerdings wegen der Neuheit bzw. des aktuellen Wandels mancher Rechtsfragen, des partiellen Fehlens von Gerichtsentscheidungen und einer bisweilen etwas sparsamen Literaturverarbeitung auf etwas weniger gesicherten Grundlagen. Hier bleibt das Buch erfreulich nüchtern: Es verliert sich nicht in Spekulationen, sondern arbeitet die schon jetzt erkennbaren Erkenntnisstände auf. Dabei gelangt es zur Feststellung einer erheblichen Anzahl von Mängeln des Abkommens, deren Beseitigung am Ende (S. 209 f.) empfohlen wird. Andernfalls bleibe zur Vermeidung von Europa- und Menschenrechtsverstößen eigentlich nur die Alternative der Kündigung.

Die auf dem Weg zu diesem Ergebnis erzielten Erkenntnis- und Orientierungsgewinne sind hoch und reichen weit über die hier untersuchte Spezialmaterie hinaus. Sie liegen zunächst in der Erschließung verzweigter Einzelfragen und Regelungszusammenhänge im Datenverarbeitungsrecht. Sie gehen darüber aber hinaus, indem allgemeine Grundsätze und Maßstäbe herauspräpariert werden, die im Kontext von Grundrechten, Datenverarbeitungsrecht und internationaler Zusammenarbeit relevant werden können. Das gilt namentlich für das an dieser Stelle noch wenig erschlossene Europarecht, kann aber auch im Hinblick auf das deutsche Recht mit Gewinn gelesen werden. Informationsregulierungsrecht ist grenzüberschreitendes und internationales Recht – oder es ist nicht! Wichtig ist hier der nach wie vor hervorgehobene Territorialbezug der Datenerhebung, die im Ausland eben nicht oder jedenfalls nicht so effektiv möglich ist, die fundierte Feststellung der Unvergleichbarkeit des (schwachen) amerikanischen Datenschutzes mit dem (höheren) europäischen Niveau sowie die eingeschränkte Geltung und Durchsetzung der Safe-Harbor-Prinzipien. Sehr aufschlussreich sind aber auch en passant Erkenntnisse darüber, wie in den Ratifikationsprozessen auch in Europa bei den Abgeordneten Fehlvorstellungen erzeugt oder aufrechterhalten werden, so dass kritische Punkte in den Parlamenten gar nicht diskutiert werden (können) (S. 74 f.). Und in der Vertragsdurchführung können rechtliche Ausnahmefälle nachher zu faktischen Regelfällen werden, welche eine erhebliche Verschlechterung des Grundrechtsschutzes zur Folge haben können (S. 126 ff.). Die neue Symmetrie der EU-Gewalten nach Lissabon ist also ähnlichen Gefährdungen ausgesetzt wie die alte Gewaltenteilung in den Mitgliedstaaten.

Was lehrt uns das? Ist dies alles Schall und Rauch, der stilvolle Sunset über der Datenschutzinsel der Seligen, die längst von ihrem letzten Bewohner verlassen worden ist? Was helfen bereichsspezifische Regelungen, wenn im Hintergrund der große Informationsstaubsauger der Nachrichtendienste arbeitet? Es gibt wohl nur drei Alternativen: (1) Die Rückkehr zum konsentierten und nachprüfbar eingehaltenen Recht. Immerhin: Nach Auskunft von EU-Kommissarin *Reding* „halten sich die Amerikaner laut einer Prüfung der Kommissionsbehörde in Bereichen, wo es bereits Abkommen gibt, an die bisherigen Vereinbarungen" (DIE WELT KOMPAKT vom 26. 11. 2013, S. 26). (2) Die Schaffung neuer Rechtsgrundlagen ohne Illusionen, aber mit nachprüfbaren Vollzugsstandards: Dazu zählt ein flächendeckendes No-Spy-Abkommen gewiss nicht,

wenn sich alle Beteiligten einig sind, dass Spionagetätigkeit zur Normalität gehört und auch in Zukunft gehören wird. Spezielle und operationalisierbare rechtliche Grenzen und Schranken sind aber möglich und sinnvoll. (3) Oder aber eine Trennung von Netzen. Dann gäbe es in den neuen nationalen oder europäischen Netzen ein anderes Datenschutzniveau als im weltweit offenen Internet. Die möglicherweise kostenträchtige Auswahl läge dann wohl beim Nutzer. Vom SWIFT-Abkommen lässt sich viel lernen. Ein wichtiges Buch zur richtigen Zeit.

Christoph Gusy, Bielefeld

Roßnagel, Alexander/*Moser-Knierim*, Antonie/*Schweda*, Sebastian, Interessenausgleich im Rahmen der Vorratsdatenspeicherung. Der Elektronische Rechtsverkehr, Band 28. Baden-Baden 2013, Nomos. 273 S.

Der Datenschutz und die Wahrung des Telekommunikationsgeheimnisses werden von den Bundesbürgern hoch geschätzt. Es kann daher nicht verwundern, dass über die Einführung der Vorratsdatenspeicherung intensiv gestritten wird. Unter Vorratsdatenspeicherung versteht man die Speicherung von Verbindungsdaten, wie z. B. die Zeit einer Telekommunikationsverbindung und der an ihr beteiligten IP-Adressen oder Telefonnummern. Nicht erfasst werden die Inhaltsdaten, wie z. B. der Inhalt eines Telefongesprächs oder einer E-Mail. Mit der Europäischen Richtlinie 2006/24/EG wurden die Mitgliedstaaten verpflichtet, Anbietern von öffentlich zugänglichen Kommunikationsdiensten aufzuerlegen, die von ihnen erzeugten oder verarbeiteten Daten für mindestens sechs Monate und höchstens zwei Jahre zu speichern. Für die Maßnahme hatte sich zum Zweck der Verfolgung schwerer Straftaten insbesondere Großbritannien stark gemacht, da London zu dieser Zeit eine Reihe von Terroranschlägen hatte hinnehmen müssen. Das deutsche Umsetzungsgesetz vom 20. Dezember 2007 scheiterte vor dem Bundesverfassungsgericht. Die neu geschaffenen §§ 113a, 113b TKG sowie § 100g Abs. 1 S. 1 StPO wurden am 21. Dezember 2007 für verfassungswidrig erklärt. Die Entscheidung erging mit 4:4 Stimmen denkbar knapp. Eine Vorratsdatenspeicherung sei zwar mit „Art. 10 nicht schlechthin unvereinbar". Das Umsetzungsgesetz trage jedoch „dem besonderen Gewicht des hierin liegenden Eingriffs" nicht hinreichend Rechnung. Der Verwendungszweck der Daten sei nicht hinreichend begrenzt, die Datensicherheit nicht hinreichend berücksichtigt. Zudem genügten die Vorschriften nicht den verfassungsrechtlichen Anforderungen an Transparenz und Rechtsstaatlichkeit. Bis heute ist es nicht gelungen, ein neues Umsetzungsgesetz durchzusetzen. Zwischenzeitlich hat die Europäische Kommission gar wegen Nichtumsetzung ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet. Zusammen mit Belgien ist Deutschland der einzige Mitgliedstaat, der seiner Umsetzungspflicht noch nicht nachgekommen ist.

Inzwischen sind die Befürworter der Vorratsdatenspeicherung auch auf europäischer Ebene unter Druck geraten. Ein Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, der von der Europäischen Kommission in Auftrag gegeben war, hat gewichtige Defizite bei der Zielerreichung festgestellt. Der EuGH überprüft zwischenzeitlich die Vereinbarkeit der Vorratsdatenspeicherung mit der europäischen Grundrechtecharta. Der Generalanwalt *Pedro Cruz Villalón* geht in seinen Schlussanträgen vom 13. Dezember 2013 davon aus, dass die Richtlinie in ihrer jetzigen Ausgestaltung nicht mit Artt. 7, 8 der GRCh zu vereinbaren ist. Zwar sei es ein „vollkommen legitimes Ziel (…) die Verfügbarkeit der erhobenen und auf Vorrat gespeicherten Daten zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten sicherzustellen", jedoch sei die Speicherungsdauer von bis zu zwei Jahren unverhältnismäßig.

Mit der Entscheidung des EuGH ist in der ersten Hälfte 2014 zu rechnen. Damit steht für Europa die Frage auf der Tagesordnung, wie die Richtlinie zu überarbeiten ist.

Die Große Koalition in Deutschland hat auf diese jüngsten Entwicklungen bereits reagiert. Im Koalitionsvertrag wird einerseits erklärt, die Richtlinie werde zügig umgesetzt. Die Verhängung von Zwangsgeldern soll vermieden werden. Der Zugriff auf die Daten soll aber nur bei schweren Straftaten, zur Abwehr akuter Gefahren für Leib und Leben und nach Genehmigung durch den Richter erfolgen. Die Datenspeicherung sollen die Telekommunikationsunternehmen übernehmen. Zudem will sich Deutschland darum bemühen, auf europäischer Ebene auf eine Verkürzung der Speicherungsfrist auf drei Monate hinzuwirken.

Vor diesem Hintergrund ist das anzuzeigende Werk von hoher Aktualität. Es präsentiert die Ergebnisse eines Forschungsprojektes „Interessenausgleich im Rahmen der Vorratsdatenspeicherung (INDOVAS)" und stellt die Frage, wie eine Vorratsdatenspeicherung ausgestaltet werden kann, die die Ziele der Sicherheit und Freiheit bestmöglich zum Ausgleich bringt. Das vom Bundesministerium für Forschung und Bildung finanzierte Projekt ist in enger Zusammenarbeit der Projektgruppe verfassungsverträgliche Technikgestaltung (Kassel) mit dem Institut für Europäisches Medienrecht (Saarbrücken) durchgeführt worden. Beide Institute sind in den letzten Jahren durch kenntnisreiche Publikationen in den Bereichen Datenschutz und Netzpolitik hervorgetreten.

Der Gang der Darstellung ist zügig resümiert. Zu Beginn der Untersuchung wird die politische Bedeutung der Suche nach einem Interessenausgleich herausgearbeitet (S. 13 – 24). Die Argumente für und gegen eine Vorratsdatenspeicherung werden zusammengefasst und die unterschiedlichen Positionen identifiziert, die in Ausgleich gebracht werden müssen. Hierbei geht es nicht nur um das Verhältnis Staat-Bürger, sondern auch um die Belastung der Unternehmen durch die Kosten der Vorratsdatenspeicherung sowie die Zuordnung von Zuständigkeiten und Befugnissen der involvierten Behörden. Im zweiten Kapitel wird die bisherige Ausgestaltung der Vorratsdatenspeicherung in den Mitgliedstaaten skizziert. Hier wird mit der Methode der funktionalen Rechtsvergleichung nach Best-Practices gesucht. Das Forschungsteam konnte hierfür auf das umfangreiche Korrespondentennetzwerk des Instituts für Europäisches Medienrecht zurückgreifen. Im Anhang finden sich 26 instruktive Steckbriefe, in denen die Umsetzungsregelungen in den untersuchten Mitgliedstaaten aufgeschlüsselt werden. Hilfreiche Ansätze für die Regelung der Datensicherheit lassen sich z. B. in Italien finden. Dort werden einzelne Parameter der Verarbeitung von Verkehrsdaten durch eine Allgemeinverfügung der italienischen Datenschutzbehörde definiert und überwacht. Als Negativbeispiel fallen die britischen und französischen Regelungen auf, da sie den Rechtsschutz vernachlässigen (S. 87 f.).

Die wesentlichen Leitlinien für den angestrebten Interessenausgleich ergeben sich naturgemäß aus dem Verfassungsrecht. Im dritten Kapitel (S. 89 – 122) werden deshalb die Eckpunkte für eine Ausgestaltung der Vorratsdatenspeicherung herausgearbeitet, die sich aus der Rechtsprechung des BVerfG ergeben. Gestaltungsvorschläge für einen optimalen Interessenausgleich werden im vierten Kapitel (S. 123 – 182) entwickelt. Insgesamt werden 17 Ausgestaltungselemente untersucht, die sich auf die Datenerhebung, die Sicherungsverpflichtung und die Datenverwendung beziehen. Übersichtlich wird hier zwischen Empfehlungen differenziert, die sich an den europäischen oder den deutschen Gesetzgeber richten. Sie werden noch einmal im fünften Kapital (S. 183 – 190) in Thesenform zusammengefasst. Darüber hinaus entwickeln die Autoren das Konzept einer Überwachungsgesamtrechnung.

Dem Autorenteam ist eine bemerkenswerte Ausarbeitung gelungen. Ihre Lektüre kann schon deshalb dringend empfohlen werden, weil sie Einseitigkeiten vermeidet und die Probleme in ihrer ganzen Vielfalt und Komplexität auffächert. Auch alternative Ermittlungsmaßnahmen wie z. B. das Quick Freeze-Verfahren werden zur Diskussion gestellt. Quick Freeze vermeidet zwar anlasslose längere Bevorratung von Daten. Der Nachteil liegt aber naturgemäß darin, dass die Verbindungsdaten zum Zeitpunkt der Anforderung schon gelöscht sein können, wenn nicht die Ermittlungsbehörden praktisch zeitgleich mit der Begehung der Straftat von dieser erfahren und aktiv werden („Kriminalität in Aktion"). Jedoch bleiben die Autoren nicht bei einer Beschreibung der gegenwärtigen Vorschläge und ihrer Risiken stehen. Vielmehr legen sie ein Gefahrenszenario zugrunde, welches vom ubiquitous computing als dem Trend der Zukunft ausgeht. Der allgegenwärtige Computereinsatz – vom Lifestyle-Accessoire wie dem Fitness-Armband über die Autobahnmaut bis hin zum total vernetzten Haus – eröffnet Möglichkeiten der „Totalüberwachung", die wir uns derzeit noch nicht einmal vorstellen können. Da das Autorenteam aus der Sicht des Verfassungsrechts argumentiert, hat es den Belang der Freiheitssicherung bei der Interessenoptimierung fest im Blick und bemüht sich um eine ausgewogene Gesamtkonzeption wie sie – so die Bewertung des Autorenteams – auch in Österreich angestrebt worden ist.

Kritisch ist anzumerken, dass sich die Autoren eine Rückkopplung ihrer Vorschläge auf das System der Strafprozessordnung im Detail nicht mehr vorgenommen haben. Auffällig sind insbesondere Friktionen im Verhältnis zur TKÜ-Anordnung nach § 100a StPO, die neben der Erfassung der Inhaltsdaten regelmäßig auch die Übermittlung der laufend anfallenden Verbindungsdaten mit umfasst. Sollte der Gesetzgeber tatsächlich den Zugriff auf Vorratsdaten an strengere Voraussetzungen binden, als sie in § 100a f. StPO für die TKÜ-Anordnung vorgesehen sind, so lässt sich eine „Flucht in die TKÜ" unschwer prognostizieren. Es ist gerade aus Sicht einer Überwachungs-Gesamtbilanz wenig gewonnen, wenn vermehrt Überwachungen nach § 100a StPO geschaltet werden, nur weil der Zugriff auf Vorratsdaten zu defensiv ausgestaltet wurde. So dürfte z. B. eine zwingende Pflicht zur Benachrichtigung des Betroffenen spätestens sechs Monate nach Abruf der Daten in vielen verdeckt geführten Verfahren dazu führen, dass der retrograde Abruf unterbleibt und statt dessen lieber länger abgehört wird, um nicht die Offenlegung des Verfahrens zur Unzeit zu riskieren. Generelle Ausnahmen für Gewerbetreibende und Geheimnisträger – insoweit nicht abgestimmt mit den Verwertungsregeln für Berufsgeheimnisträger nach § 160a Absatz 4 StPO – laden zur Umgehung geradezu ein. Auch der gut gemeinte Vorschlag, staatsanwaltschaftliche Eilanordnungen binnen 24 Stunden richterlich bestätigen zu lassen, dürfte dem Grundrechtsschutz eher abträglich sein, führt er doch in der Praxis dazu, dass ein mit der Sache nicht vertrauter Richter im Eildienst entscheiden muss und nicht der reguläre Ermittlungsrichter, der die Akten kennt und kritisch nachfragt.

Die Vorschläge des Autorenteams werden sich im Detail dem Praxistest noch stellen müssen. Am Verdienst der Autoren ändert das nichts. Die rechtspolitische Diskussion der letzten Monate hat gezeigt, dass die Praxis mit einer Begrenzung einer Höchstspeicherfrist auf sechs Monate (S. 137) offenbar sehr gut leben kann. Wahrscheinlich wird sogar eine kürzere Frist genügen. Dass die Vorratsdatenspeicherung – soll sie nicht der Türöffner für den umfassenden Überwachungsstaat werden – durch ein komplexes Netz von Grundrechtsgarantien eingehegt werden muss, ist unstreitig. Dem Autorenteam gelingt es, hier die möglichen Handlungsfelder abzugrenzen und in ihr Konzept der Überwachungsgesamtrechnung einzubinden. Es dürfte sich lohnen, mit diesem Konzept Erfahrungen zu sammeln. Um sicherzustellen, dass nicht durch alle Überwachungsmaßnahmen zusammen alle Aktivitäten der Bürger rekonstruiert werden kön-

nen, soll es eine doppelte Verhältnismäßigkeitsprüfung geben. Es solle nicht nur bei einer neuen Maßnahme ihr verhältnismäßiger Einsatz ermitteln werden. Vielmehr sei „zusätzlich auf der Basis einer Gesamtbetrachtung (Überwachungs-Gesamtrechnung) aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastung bürgerlicher Freiheiten zu prüfen" (S. 177). Die Folge einer solchen Prüfung wäre, dass der Gesetzgeber gegebenenfalls nur eine Maßnahme austauschen und nicht hinzufügen dürfe. Eine regelmäßige Kontrolle des gesamtgesellschaftlichen Überwachungsgrades soll durch Berichtspflichten der Datenschutzbeauftragten gewährleistet werden. Die Durchführung der Prüfung vor Einführung eines neuen Überwachungsinstruments ist durch Verfahrensregeln zu sichern (S. 180). Dem Werk ist zu wünschen, dass es mit diesem Ansatz den aktuellen Diskurs in Deutschland und Europa zum umfassenden Grundrechtsschutz hin beeinflusst und insgesamt versachlicht.

Bernd Holznagel, Münster

Bull, Hans Peter, Netzpolitik: Freiheit und Rechtsschutz im Internet. Baden-Baden 2013, Nomos. 154 S.

Hans Peter Bull ist ein für die Auseinandersetzung mit rechtlichen Fragen betreffend das Internet prädestinierter Autor. Mit der Perspektive der durch potenziellen Missbrauch vertraulicher Informationen im Internet eingeschüchterten Menschen ist er als erster Bundesbeauftragter für den Datenschutz überhaupt (1978 – 1983) ebenso vertraut wie mit den Bedürfnissen der Polizei bei der Verhütung und Verfolgung von Straftaten aufgrund seiner Tätigkeit als Innenminister des Landes Schleswig-Holstein (1988 – 1995). Das profunde faktische Hintergrundwissen fließt in die wissenschaftlich und rechtspolitisch ausgerichtete Schrift auf ganzer Strecke ein.

Inhalt und Ausrichtung des Buches spiegeln sich im Titel treffend wieder. Es geht dem Autor um eine Gesamtsicht der Rechtsprobleme im Zusammenhang mit dem Internet. Er sucht die Balance zwischen dem Ideal möglichst weitreichender Freiheit einerseits und der Notwendigkeit effektiven Rechtsschutzes zugunsten der in ihren Rechten beeinträchtigten Menschen andererseits. Dabei unterbreitet er zahlreiche Vorschläge, wie eine umfassende, alle Gesichtspunkte einbeziehende, einseitige Lösungen vermeidende „Netzpolitik" aussehen könnte.

Das große Verdienst *Bulls* liegt zunächst darin, dass er ungeachtet der nicht mehr überschaubaren Literatur aus allen Bereichen (Zivilrecht, Öffentliches Recht, Strafrecht) und zu allen denkbaren Detailproblemen die beiden rechtlichen Brennpunkte in Bezug auf das Internet nie aus den Augen verliert: den Schutz der – oft untereinander im Gegensatz stehenden – Individualrechte und die Wahrung der Allgemeininteressen (S. 18 f.). Illustrativ sind die von ihm aufgezeigten Widersprüchlichkeiten, die bei einseitiger Optik zur Verabsolutierung bestimmter Rechtspositionen verleiten können (S. 21 f.). Treffend weist er beispielsweise darauf hin, dass das Persönlichkeitsrecht sozialer Einbindung unterliegt. Zielführend ist auch *Bulls* Ansatz, zur Lösung von Rechtsproblemen betreffend das Internet im Regelfall auf die auch außerhalb des Internets geltenden Rechtsgrundsätze zurückzugreifen (vgl. S. 25). Diese Grundannahmen wendet *Bull* auf zahlreiche Problemfelder an.

Im Ersten Teil (S. 32 – 79) wendet sich der Autor den Rechten des Individuums zu. Dabei folgt er seiner Strategie, neuartige Erscheinungen und Probleme im Internet mithilfe vertrauter Rechtsfiguren zu lösen. So erblickt er beispielsweise in der Verbandsklage ein effektives Instrument zur Ergänzung des mitunter zu wenig praktikablen Individu-

alrechtsschutzes (S. 28 f.). Folgerichtig lehnt er die Entwicklung eines gesonderten „Grundrechts auf Internet“ ab (S. 39 ff.). Die Rechtsprechung des Bundesverfassungsgerichts ausgehend vom „Volkszählungs-Urteil“ über die Kennzeichenüberwachung (S. 60 ff.) bis zur Vorratsdatenspeicherung (S. 73 ff.) hält er für zu weitgehend, zu einseitig den Datenschutz betonend, strukturelles Misstrauen gegenüber sämtlichen Behörden säend. Er geißelt die angebliche „Beschwörung des Unrechtsstaates“ (S. 63 f.) und versucht das in der Gesellschaft weit verbreitete Unbehagen mithilfe harmloser Beispiele wie der Erstellung von Kundenprofilen und der Belästigung durch E-Mail-Werbung zu entkräften (S. 65 ff.). Unweigerlich fragt man sich als unter dem Eindruck der Enthüllung der weltweiten Überwachungen durch den US-amerikanischen Geheimdienst NSA stehender Leser, ob der Autor – noch in Unkenntnis dieser Ereignisse – nicht bisweilen eine zu ausgeprägte Gelassenheit an den Tag legt. *Bull* gelingt es aber schon bald wieder, den zweifelnden Leser auf seine Seite zu ziehen, wenn er – allerdings im Dritten Teil des Buches – zu Recht auf die völlige Verpuffung der auf den ersten Blick scheinbar spektakulären Enthüllungen auf Plattformen wie WikiLeaks verweist (S. 101 f.).

In einem kürzeren Zweiten Teil (S. 80 – 96) relativiert *Bull* unter dem Titel „Die ökonomische und technische Perspektive“ einige Forderungen wie die Unentgeltlichkeit aller Inhalte des Internets und die Netzneutralität mit überzeugenden Argumenten. Dabei weist er mit Recht darauf hin, dass auch und vielleicht gerade im Internet erhebliche wirtschaftliche Interessen im Spiel sind, die bei idealistischer Verklärung bestimmter Postulate leicht verschleiert werden können.

So zuträglich *Bulls* praktische und politische Informiertheit an vielen Stellen des Buches für das Verständnis des Lesers ist, so befremdlich wirken einige Passagen im Dritten Teil (S. 97 – 118). Deplatziert ist meines Erachtens die auf die Person, nicht auf das sachliche Argument zielende Kritik an einem vom Volk gewählten Berliner Abgeordneten, dessen Auffassungen zum Verhältnis von Bürger/Innen und Staat *Bull* nicht teilt (exemplarisch S. 103: „[…] in der simplen Weltanschauung dieses Abgeordneten, der als Softwareentwickler erfolgreich sein mag, aber offensichtlich von sozialen und politischen Zusammenhängen nichts weiß“).

Teilweise nur wenig nachvollziehbar sind die durch den Autor konstruierten Bezüge des Internets zur direkten Demokratie in Deutschland. *Bull* bedient sich dabei, um direktdemokratische Entscheidungsprozesse zu kritisieren, allgemeiner und keineswegs das Internet spezifisch betreffender, sondern vielmehr seit langem bekannter und in vielem widerlegter Einwände wie etwa „dass eine gut organisierte und finanzstarke Minderheit ihre Interessen gegen die weniger artikulationsfähige Mehrheit durchsetzt“ (S. 104). Er hadert mit dem Hamburger Volksentscheid gegen die Einführung einer Gesamtschule, wobei er selbst einräumen muss, dass in diesem Fall „übrigens das vorgeschriebene Quorum deutlich überschritten“ wurde. Was dies im Besonderen mit dem Internet zu tun haben soll, erschließt sich nicht ohne Weiteres.

Hat sich der Leser von den teilweise polemisch vorgetragenen Argumenten nicht zu sehr verschrecken lassen, erwarten ihn im Vierten Teil (S. 119 – 148) wiederum sachlich formulierte und in vielem bedenkenswerte rechtspolitische Vorschläge. Ziel ist eine Entschlackung des Datenschutzrechts, das zum reinen Selbstzweck zu werden droht (S. 131 f.). Kernpunkt der Forderungen ist der Grundsatz: „Was nicht verboten ist, ist erlaubt“ (S. 136). In Fortführung seines Ansatzes lehnt *Bull* ein Spezialrecht für das Internet ab und plädiert für eine Anpassung des jeweiligen Fachrechts (S. 138 ff.). Angesichts der überaus interpretationsoffenen Bestimmungen der von der Europäischen Kommission vorgeschlagenen Datenschutz-Grundverordnung

(dazu S. 141 ff.) dürfte sich *Bulls* Prognose, dass die Datenschutzdebatte auf nationaler Ebene fortgeführt werden wird (S. 144 ff.), wohl als richtig erweisen. Abschließend betont der Autor, dass der Erfolg seiner Vorschläge maßgeblich auf einem Grundvertrauen der Menschen in die staatlichen Behörden basiert (S. 148). Gerade dieses Vertrauen wird – allen Abstumpfungseffekten der öffentlichen Meinung zum Trotz – durch wiederholte Fälle staatlichen Datenmissbrauchs allerdings untergraben. Hier wird der Verlauf der rechtspolitischen Diskussion stark von den künftigen Ereignissen bei Polizei und Geheimdiensten geprägt werden.

Hans Peter Bull hat mit seiner engagiert und klar formulierten sowie gut lesbaren Schrift einen grundsätzlichen Beitrag zur Diskussion über die rechtliche Regulierung des Internets verfasst. Es gelingt ihm vorzüglich, dem am Recht des Internets interessierten Leser Orientierung zu bieten und an wichtige Grundlinien zu erinnern. Zu wünschen wäre, dass einige Gedanken darüber hinaus Eingang in den politischen Entscheidungsprozess finden. Die teilweise in der Form überzogene Kritik an den politischen Gegenpositionen – und vor allem auch an den sie vertretenden Menschen – schmälert die Überzeugungskraft der Argumente indessen bis zu einem gewissen Grad.

Andreas Glaser, Zürich