Datenschutz-Erwartungen an die Politik in der 19. Legislaturperiode

Stand: 1. Oktober 2017

Inhalt

Dr. Thilo Weichert
Waisenhofstraße 41, 24103 Kiel
0431/971 97 42
weichert@netzwerk-datenschutzexpertise.de

Ute Bernhardt
Elchdamm 56a, 13503 Berlin
030/280 466 95
bernhardt@netzwerk-datenschutzexpertise.de

Ingo Ruhmann
Elchdamm 56a, 13503 Berlin
030/280 466 95
ruhmann@netzwerk-datenschutzexpertise.de

Karin Schuler
Kronprinzenstr. 76, 53173 Bonn
0228/24 20 733
schuler@netzwerk-datenschutzexpertise.de

www.netzwerk-datenschutzexpertise.de

1 Einleitung

Der Datenschutz ist im Aufbruch und zugleich in der Krise: Einerseits haben wir in Europa vom 25. Mai 2018 an ein weitgehend harmonisiertes Datenschutzrecht insbesondere mit der Datenschutz-Grundverordnung (DSGVO) und schon seit einigen Jahren eine grundrechtsfreundliche Rechtsprechung der Europäischen Gerichtshofs (EuGH). Andererseits zeigt die Politik auf nationaler Ebene nur eine beschränkte Bereitschaft, sich den freiheitlichen und demokratischen Herausforderungen der Digitalisierung anzunehmen und im Interesse des Gemeinwohls den digitalen Grundrechtsschutz weiterzuentwickeln. Deutschland hat schon seit längerem seine ursprünglich fortschrittliche Rolle im Bereich des Datenschutzes aufgegeben.

Dessen ungeachtet besteht eine hohe Sensibilität hinsichtlich des Schutzes der Privatsphäre sowie des Rechts auf informationelle Selbstbestimmung bei einem Großteil der deutschen Bevölkerung und zunehmend auch in Europa und in anderen Teilen der Welt. Die zunehmende Digitalisierung in der Wirtschaft wie auch der privaten Lebensbereiche der Menschen eröffnet große Chancen bei der Verbesserung der Produktivität, durch die Erleichterung des Alltags und für den ökonomischen, technischen und wissenschaftlichen Fortschritt. Zugleich werden die Abhängigkeit von der informationstechnischen Infrastruktur und damit die Verletzlichkeit sowohl individuell wie gesamtgesellschaftlich erhöht. Dies hat direkte Auswirkungen auf unsere freiheitlich-demokratische Grundordnung. Die deutsche Politik hat auf diese Entwicklungen bisher nur reagiert und kaum versucht – evtl. im Gleichklang mit den anderen Staaten und den Organen der Europäischen Union – hierauf gestaltend einzuwirken.

Die zu Ende gegangene 18. Legislaturperiode startete mit einem Koalitionsvertrag, in dem die politische Gestaltung des rechtlichen Rahmens wie auch der informationstechnischen Infrastruktur versprochen wurde. Die Versprechungen, den Beschäftigtendatenschutz zu regulieren, den Hinweisgeberschutz zu verbessern, Selbstbestimmung und Transparenz in der digitalen Welt zu erhöhen und Sicherheitstechnologien, z. B. die Kryptographie, weiterzuentwickeln, wurden teilweise nicht, teilweise unzureichend eingehalten. Auf europäischer Ebene profilierte sich Deutschland, etwa bei der Ausarbeitung der DSGVO, als Bremser bei einem fortschrittlichen digitalen Grundrechtsschutz.

2 Datenschutzrecht: Rechtssicherheit statt Aufweichung!

Bei der Umsetzung der DSGVO in deutsches Recht setzen sich die Bestrebungen fort, das für die EU formulierte Datenschutzrecht aufzuweichen. Die EU-Kommission hat bereits angedroht, gegen das neue Bundesdatenschutzgesetz (BDSG-neu) vorgehen zu wollen. Doch dies ist nur ein Anfang. Auf Bundes- und Länderebene hat die Arbeit erst begonnen, zahlreiche einzelgesetzliche Normen an die DSGVO anzupassen. Wenn auch hier der Weg eingeschlagen wird, den Datenschutz aufzuweichen, droht der Datenschutz für Bürger ebenso wie für Anbieter von IT-Diensten zu einem nicht mehr überschaubaren rechtlichen Minenfeld zu werden, bis die absehbaren Differenzen am Ende durch den EuGH geklärt werden. Die nächste Legislaturperiode wird darüber entscheiden, ob das auch von der Bundesregierung in Brüssel gemeinsam beschlossene Recht angewandt wird oder der IT-Entwicklung der nächsten 10 Jahre der sichere rechtliche Boden entzogen wird.

- Das soeben in Kraft getretene Bundesdatenschutzgesetz (BDSG-neu) muss überarbeitet und insbesondere von europarechts- und verfassungswidrigen Regelungen befreit werden.

Das 2017 verabschiedete neue BDSG verstößt z. B. im Hinblick auf die Datenschutzkontrolle sowie die Sicherung der Betroffenenrechte gegen höherrangiges europäisches und nationales Verfassungsrecht. Diese Mängel sind zu beheben.

- Das bereichsspezifische deutsche Datenschutzrecht wird an die Regelungen der DSGVO angepasst unter Wahrung eines hohen Standards und der Zielsetzung einer möglichst weitgehenden europäischen Harmonisierung.

Bis zum 25. Mai 2018 muss das bereichsspezifische Datenschutzrecht in Deutschland an die Vorgaben der DSGVO angepasst werden, um den Rechtsanwendern und den Betroffenen Rechtssicherheit im Hinblick auf die Gültigkeit der Regelungen zu geben.

- Die auf Bundesebene geltenden Sicherheitsgesetz (Polizei-, Strafprozess- und Geheimdienstrecht) werden im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs evaluiert und überarbeitet.

Das Bundesverfassungsgericht hat insbesondere mit dem Urteil zum Bundeskriminalamtsgesetz (20.04.2016, 1 BvR 966/09, 1 BvR 1140/09) und der Europäische Gerichtshof mit seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten (21.12.2016, C-203/15, C-698/15) sowie seinem Gutachten zum Fluggastdatenaustausch mit Kanada (26.07.2017, 1/15) rechtliche Vorgaben für das Sicherheitsrecht gemacht, die vom bundesdeutschen Recht in vieler Hinsicht unbeachtet geblieben sind. Insofern muss Verfassungskonformität hergestellt werden. Wenn das Bundesverfassungsgericht oder gar der EuGH regelmäßig neue Regelungen für weitere Überwachungsmaßnahmen wegen zumeist offensichtlicher Verstöße gegen Grundrechte kassieren müssen, lässt sich dies zwar für eine symbolische Debatte nutzen, führt aber zu keiner Änderung in der Sicherheitslage.

- Die Bundesrepublik bringt sich auf europäischer Ebene in die Diskussion um die Schaffung einer digitalen Grundrechte-Charta engagiert ein.

Ende 2016 wurde von prominenten Einzelpersonen der Entwurf einer digitalen Grundrechte-Charta für Europa vorgelegt, der das Ziel verfolgt, die demokratischen Freiheiten und Grundrechte in einer modernen europäischen Informationsgesellschaft zu sichern. Dieser Ansatz sollte weiterentwickelt und institutionell umgesetzt werden.

- Die Bundesrepublik setzt sich dafür ein, dass die von der EU-Kommission vorgeschlagene Datenschutz-Verordnung für die elektronische Kommunikation (ePrivacy-Verordnung) mit einem qualifizierten Grundrechtsschutz noch vor dem 25. Mai 2018 verabschiedet und in Kraft gesetzt wird.

Während es für den Datenschutz mit der DSGVO seit 2016 verbindliche europaweit harmonisierte Regeln gibt, die vom 25. Mai 2018 direkt anwendbar sind, gilt für den Schutz der Telekommunikation weiterhin eine Richtlinie aus dem Jahr 2002, die nicht mehr den technischen Gegebenheiten entspricht. Durch die Harmonisierung des Telekommunikationsrechts soll eine rechtssichere

Vereinheitlichung und Vereinfachung für die Bürgerinnen und Bürger wie für die Wirtschaft erreicht werden.

- Die Bundesrepublik setzt sich dafür ein, dass in Europa grundrechtskonforme Grundlagen für die transatlantische digitale Kommunikation geschaffen werden.

Am 12. Juli 2016 beschloss die Europäische Kommission für die Kommunikation mit den USA ein EU-US-Privacy Shield, das den Safe-Harbor-Rechtsrahmen aus dem Jahr 2000 ablöste, der vom EuGH wegen Grundrechtswidrigkeit aufgehoben wurde. Das Privacy Shield wie weitere weiterhin gültige Instrumente, z. B. Standardvertragsklauseln, haben ähnliche verfassungsrechtliche Mängel wie Safe Harbor und müssen durch einen grundrechtskonformen Rechtsrahmen ersetzt werden.

3 Grundrechtskonforme IT-Sicherheit

Die IT-Sicherheit ist eine Aufgabe, die den Vorgaben von drei Grundrechten folgen muss: Dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, dem Datenschutz und dem Fernmeldegeheimnis. Das gegenwärtige Recht reicht nicht aus, auch nur eines dieser Grundrechte zu schützen.

- Das Recht der IT-Sicherheit muss an den Auftrag des Grundgesetzes und die Vorgaben des EU-Rechts angepasst werden.

Der Schutz der IT-Sicherheit hat den Rang eines Grundrechts, das mit anderen in Einklang zu bringen ist. Das deutsche Recht der IT-Sicherheit steht aber in einem fachlich nicht begründbaren Konflikt mit dem Datenschutz. Es ist der Bundesregierung bisher auch misslungen, legitime Eingriffe in das Fernmeldegeheimnis bei der Arbeit der IT-Sicherheitsexperten rechtlich klar und in engen Grenzen zu regeln. Das deutsche Recht in diesem Bereich ist weder verfassungsfest noch konform zu EU-Recht. Der Bundestag hat am Ende der 18. Legislaturperiode einige der offensichtlichsten Verstöße gegen das Grundgesetz abgemildert. Dies reicht aber nicht aus. Der EuGH hat die Bundesregierung unlängst gemahnt, EU-rechtliche Vorgaben umzusetzen. Ein einheitliches, grundrechtskonformes Recht der IT-Sicherheit ist dringend überfällig.

- Es müssen rechtlichen Anforderungen hinsichtlich Datenschutz und Datensicherheit an IT-Produkte generell wie insbesondere im Interesse des Verbraucherschutzes erarbeitet und verabschiedet werden.

Das bisherige Datenschutz- und IT-Sicherheitsrecht formuliert ausschließlich Anforderungen an die verarbeitenden Stellen, nicht aber an die Hersteller und Anbieter von IT-Produkten. Dies führt dazu, dass es bei der Anwendung bzw. Nutzung der Produkte zu Datenschutzverstößen oder zu vermeidbaren Risiken kommt. Durch eine Regulierung der Produktanforderungen soll dies vermieden werden.

- Es bedarf der Entwicklung eines organisatorischen und rechtlichen Rahmens zur qualifizierten Zertifizierung von IT-Produkten in Bezug auf Datenschutz und Datensicherheit.

Die DSGVO sieht ein umfassendes Instrumentarium der Datenschutz-Zertifizierung vor. Um dieses mit Leben zu füllen, sind die hierfür nötigen Rahmenbedingungen zu schaffen.

4 Beschäftigtendatenschutz

- Ein modernes, grundrechtsfreundliches und technikadäquates Beschäftigtendatenschutzgesetz muss erarbeitet und verabschiedet werden.

Seit über 30 Jahren wird über die Notwendigkeit eines grundrechtswahrenden Datenschutzgesetzes für Arbeitnehmer bzw. Beschäftigte diskutiert. Dessen Notwendigkeit ist angesichts des Technikeinsatzes im betrieblichen Bereich und der Vorgaben der DSGVO nicht mehr zu bestreiten. Arbeitgeber wie Beschäftigte haben einen Anspruch auf Rechtssicherheit beim Umgang mit Beschäftigtendaten.

5 Datenverarbeitung generell

- Das Kartell-, das Wettbewerbs- und das Steuerrecht müssen an den Umstand angepasst werden, dass digitale Leistungen oft nicht mehr mit Geld, sondern mit Daten bezahlt werden.

Bisher war das Datenschutzrecht weitgehend Ordnungsrecht. Die Durchdringung personenbezogener Datenverarbeitung bei Konsum und Wirtschaft macht es nötig, die rechtlichen Rahmenbedingungen an die neuen Gegebenheiten anzupassen.

- In der öffentlichen Verwaltung ist eine eGovernment-Infrastruktur aufzubauen mit sicheren Identifizierungs-, Authentisierungs- und Verschlüsselungsverfahren bei der elektronischen Kommunikation.

Die Akzeptanz und der gesellschaftliche Nutzen von eGovernment können nur erreicht werden, wenn für Datenschutz, Datensicherheit und Rechtssicherheit die rechtlichen und technischen Rahmenbedingungen geschaffen werden.

- Das Informationsfreiheitsrecht ist im Sinne eines Transparenzrechts und von Open Government weiterzuentwickeln.

Die Digitalisierung ermöglicht es, über das Internet die Transparenz der Verwaltung und damit sowohl die Akzeptanz wie auch die Partizipation der Bevölkerung zu erhöhen. Diese Möglichkeiten sind zu nutzen.

- Die gesellschaftlichen Konsequenzen der Digitalisierung auf das Bewusstsein der Menschen, ihr Konsum- und Kommunikationsverhalten und ihre Wahrnehmung der demokratischen Rechte sind durch staatliche geförderte Forschung zu erkunden.

Die Digitalisierung führte zu völlig neuem Konsum- und Kommunikationsverhalten mit völlig neuen Möglichkeiten für die Menschen. Dabei erfolgt zugleich eine ökonomische und informationelle Machtkonzentration, die für die demokratische Gesellschaft neue Risiken schafft, und es entstehen

informationelle Ungleichgewichte zwischen Anbietern und Nutzern, die informationelle Fremdbestimmung begünstigen. Diese Mechanismen sind zu erforschen und die Ergebnisse in der Politik zu berücksichtigen.

Der beste Schutz der Grundrechte bei der Digitalisierung ist das Prinzip der „Privacy by Design“. Auch die DGSVO fordert eine Stärkung dieser Entwicklungsansätze. Auch wenn darüber debattiert wird, Datensparsamkeit zu „erneuern“ durch Datenautonomie und eine Datenökonomie, so bleibt die entscheidende Voraussetzung für jede Art der Steuerung, der Selbstbestimmung und des autonomen Umgangs mit Daten der Einbau von technischen Vorkehrungen zur Umsetzung der Schutzprinzipien des Grundgesetzes. Für jede Art von zukunftsfähiger IT muss „Privacy by Design“ daher leitendes Gestaltungsprinzip sein.

- Die Vermittlung von Medienkompetenz ist durch gemeinsame Anstrengungen mit den Bundesländern verbindlich in Lehrplänen im Bereich der schulischen und außerschulischen Aus- und Fortbildung vorzusehen und auszubauen.

Die Digitalisierung stellt für die Einzelnen eine Herausforderung dar, die nur durch bessere Kenntnis der technischen, rechtlichen, organisatorischen und sozial-ökonomischen Bedingungen bewältigt werden kann.

- Ähnlich dem Normenkontrollrat ist ein Expertengremium einzurichten, das Gesetzgebungsverfahren und Initiativen der Bundesregierung zur Digitalisierung einer Folgenabschätzung unterwirft – gewissermaßen als übergreifende Form der in der DSGVO vorgesehenen Folgenabschätzung.

Die Digitalisierung wird von den Bundesministerien kaum mit einer kohärenten Perspektive verfolgt, Gesetzgebungsverfahren sind vielfach eine Reaktion auf aktuelle Anlässe und lassen einen an Datenschutz und Grundrechten orientierten Gestaltungswillen vermissen. Ein Expertengremium ist geeignet, den politischen Alltag um die Betrachtung langfristiger Wirkungen zu ergänzen und zusätzliche Anstöße für eine an Bürgerrechten ausgerichtete Digitalpolitik zu geben.