Europas neue Datenpolitik Mit der EU-Datenschutzgrundverordnung beginnt der Konflikt um den Datenschutz erst

Benjamin Bergemann und Magnus Römer

Summary: After years of political struggle, the EU has settled on new data protection rules. Since 25 May 2018 the new General Data Protection Regulation (GDPR) has been directly applicable. The aim of the GDPR is to adapt the European data protection rules for the digital age and to harmonize them throughout the EU. Yet, the issue how to use personal data and for what purposes is far from settled. In addition, there are quite different understandings of what are the aims and means of data protection throughout Europe. As a result, the GDPR and its implementation remain contested.

Kurz gefasst: Nach jahrelangem Ringen hat sich die EU auf ein neues Datenschutzgesetz geeinigt. Seit dem 25. Mai 2018 gilt die neue Datenschutzgrundverordnung (DSGVO). Die direkte Geltung der Verordnung, ihr ausgedehnter Anwendungsbereich und neue Instrumente sollen den europäischen Datenschutz an das Datenzeitalter anpassen und weiter vereinheitlichen. Doch gesellschaftliche Konflikte um Datennutzung und unterschiedliche europäische Verständnisse von Datenschutz sorgen dafür, dass die DSGVO auch nach ihrem Inkrafttreten offen und umkämpft bleibt.

Seit dem 25. Mai 2018 gilt die neue EU-Datenschutzgrundverordnung (DSGVO). Juristisch betrachtet ist sie eine Reform des in den 1990er Jahren europäisierten Datenschutzrechts. Aus politischer und gesellschaftlicher Sicht allerdings bildet die DSGVO den Rahmen für zentrale Entwicklungen, die unter dem Schlagwort „Digitalisierung" verhandelt werden. Denn die Digitalisierung ist vor allem auch eine Datafizierung. Daten konstituieren in zunehmendem Maße eine Infrastruktur, auf deren Basis wir unser Zusammenleben organisieren, zum Beispiel beim Filtern relevanter Informationen im Internet, bei der Gestaltung der Energie- und Verkehrswende oder in der medizinischen Versorgung und Forschung. Die DSGVO regelt die Produktion und den Einsatz dieser Daten und kann damit als eine europäische Antwort auf die Frage verstanden werden, wie die Digitalisierung gestaltet werden soll. Besonders die Europäische Kommission und die Datenschutzgemeinde, bestehend aus den behördlichen Datenschutzbeauftragten, NGOs und Verbraucherschutzverbänden, heben diesen Anspruch hervor. In Abgrenzung zu der von ihnen als unterreguliert kritisierten Digitalisierung in den USA erheben sie die DSGVO zu einem alternativen Leitbild des digitalen Wandels, das Innovation und Grundrechte versöhnt. Die DSGVO ist ein zentrales Projekt der EU, mit dem sie als Regulierungsakteur gegenüber globalen Konzernen Machtansprüche reklamiert. Sie gibt jedoch weniger Antworten auf die Herausforderungen des Datenzeitalters, als es die Rhetorik der EU-Institutionen suggeriert. Sie eröffnet eine Arena der Datenpolitik, in der politische Konflikte um Daten und ihre Verwendung nun ausgetragen werden.

Der Weg zur DSGVO war lang: Spätestens als die Europäische Kommission im Jahr 2012 den Entwurf für die Datenschutzverordnung vorstellte, begann ein umkämpfter Gesetzgebungsprozess. Vor allem Unternehmen warnten vor den innovationshemmenden Folgen strenger Datenschutzregeln, während die Datenschutzgemeinde auf den Grundrechtsstatus des Datenschutzes pochte und damit vergleichsweise restriktive Regelungsvorschläge begründete. Nach vier Jahren Verhandlungszeit, in die auch die Enthüllungen über die globale Massenüberwachung der Geheimdienste durch den US-Whistleblower Edward Snowden fielen, konnten sich schließlich die Anhänger eher strenger Datenschutzregeln aus EU-Kommission, EU-Parlament und Datenschutzbehörden gegenüber den Mitgliedsstaaten und der Wirtschaft durchsetzen – wenn auch mit Zugeständnissen. Im Jahr 2016 einigte man sich auf die endgültige Fassung der DSGVO, die nun nach zwei Jahren Übergangszeit ab dem 25. Mai 2018 gilt.

Der Widerstreit zwischen Datenmarkt und Datenschutz als Grundrecht steckt in der DNA des europäischen Datenschutzes. Traditionell hat dieser den Anspruch, Datenverarbeitung sowohl zu ermöglichen als auch – wo nötig – zu begrenzen. So will Datenschutz Datenmärkte schaffen und zugleich Grundrechte schützen. Die DSGVO setzt diese Tradition fort. Überdies schickt sie sich an, Regeln zu setzen, die den aktuellen soziotechnischen Entwicklungen besser als die Datenschutzrichtlinie von 1995 gerecht werden und gegenüber den oft global agierenden Datenverarbeitern wirksamer durchsetzbar sind. Angesichts der seit 1995 stark gestiegenen Bedeutung von Datenverarbeitung liegt es nahe, dass ein Regelwerk dieses Anspruchs nicht unwidersprochen bleibt.

Die DSGVO knüpft nicht nur hinsichtlich dieses dualen Charakters zwischen freiem Datenfluss und Grundrechtsschutz an die Tradition des europäischen Da-

Benjamin Bergemann ist wissenschaftlicher Mitarbeiter in der Projektgruppe Politikfeld Internet. Er forscht zur Genese und zum Wandel der Datenschutzpolitik. *(Foto: David Ausserhofer)*

benjamin.bergemann@wzb.eu

tenschutzes an. Sie schreibt auch seine bestehenden Prinzipien fort. Auch unter der DSGVO bleibt es das primäre Ziel des Datenschutzes, datenverarbeitende Organisationen zu regulieren. Sie dürfen personenbezogene Daten nur verarbeiten, wenn es hierfür eine Rechtsgrundlage gibt (Verbot mit Erlaubnisvorbehalt). Zudem dürfen Daten auch weiterhin nur für festgelegte Zwecke verarbeitet werden (Zweckbindung) und dann nur Daten, die für diese Zwecke auch notwendig sind (Datenminimierung). Gerade diese Prinzipien waren im Gesetzgebungsprozess umstritten, denn sie scheinen der Idee von „Big Data" zu widersprechen. Diese besteht gerade darin, möglichst viele Daten aus unterschiedlichen Quellen für immer neue Zwecke zu nutzen. Dass trotz erheblicher Widerstände an diesen Prinzipien festgehalten wurde, ist daher nicht selbstverständlich.

Ergänzt werden die allgemeinen Datenschutzprinzipien durch Verarbeitungs-, Auskunfts- und Dokumentationsvorschriften. Datenverarbeitende Stellen müssen sich also nicht nur abstrakt an Datenschutzregeln halten, sondern das auch gegenüber Datenschutzbehörden und den Personen, über die sie Daten verarbeiten, nachweisen. Spiegelbildlich zu den Pflichten der Datenverarbeiter haben die betroffenen Personen Rechte gegenüber diesen, darunter das Recht auf Information und Auskunft, Berichtigung und Löschung, ein neues Recht auf Datenübertragbarkeit, das heißt zur Mitnahme der persönlichen Daten zu einem anderen Anbieter, sowie Auskunfts- und Widerspruchsrechte bei automatischen, also „algorithmischen" Entscheidungen.

Gerade Unternehmen sehen sich unter Druck, da die DSGVO mit verschiedenen Maßnahmen darauf hinwirkt, die neuen Datenschutzregeln auch entsprechend durchzusetzen. Dafür sorgen vor allem die deutlich höheren Strafen für Datenschutzvergehen. Strafsätze von bis zu 20 Millionen Euro oder vier Prozent des globalen Umsatzes einer Firma sind möglich. Das alte Bundesdatenschutzgesetz auf Basis der Datenschutzrichtlinie von 1995 sah bisher für einzelne Verstöße Strafzahlungen von maximal 300.000 Euro vor.

Für eine bessere Durchsetzung der Datenschutzregeln, und damit Handlungsdruck, sorgt auch der mit der DSGVO vorgenommene Wechsel des Rechtsinstruments: von der Richtlinie zur Verordnung. Anders als EU-Richtlinien müssen EU-Verordnungen nicht durch die Mitgliedsstaaten in nationales Recht umgesetzt werden. Die Datenschutzgrundverordnung ist direkt in der gesamten EU wirksam und regelt den Datenschutz im Bereich der Wirtschaft und der Verwaltung. Um sich gegenüber global agierenden Konzernen behaupten zu können, führt die DSGVO darüber hinaus das sogenannte Marktortprinzip ein. Dieses besagt, dass nicht nur der Sitz des Datenverarbeiters relevant ist, sondern ebenso der der betroffenen Person. Befindet sich diese innerhalb der EU, findet die DSGVO meist Anwendung, auch wenn der Verarbeiter keine europäische Niederlassung hat. Vor allem für international agierende Unternehmen schwinden damit die Chancen, sich der Regulierung zu entziehen. Die Kombination aus ausgedehntem Geltungsbereich und hohen Strafzahlungen soll Unternehmen von Regelbrüchen abschrecken.

Die EU-weite Geltung und einheitliche Durchsetzung der DSGVO bleibt jedoch umkämpft und muss auch nach dem Inkrafttreten der DSGVO weiter ausgehandelt werden. Denn zum einen trägt die DSGVO deutliche Spuren europäischer Kompromisspolitik. Mitgliedsstaaten verfügen an vielen Stellen weiterhin über nationale gesetzgeberische Spielräume durch sogenannte Öffnungsklauseln. Mit der DSGVO neu eingeführte und mit großen Erwartungen verbundene Instrumente wie Datenschutzfolgeabschätzungen oder Vorschriften zu datenschutzfreundlicher Technikgestaltung müssen von Datenschutzexperten aus Politik, Wirtschaft, Aufsichtsbehörden und Zivilgesellschaft erst gemeinsam konkretisiert werden.

Zum anderen wird die Umsetzung der DSGVO letztlich von nationalen Datenschutzaufsichtsbehörden überwacht. Um trotz dieser Vielfalt an Aufsichtsbehörden Kohärenz zu erreichen, schreibt die DSGVO eine stärkere europaweite Koordination vor. Diese soll Datenverarbeitern und Aufsichtsbehörden gleichermaßen zugutekommen. Bisher waren grenzübergreifend tätige Datenverarbeiter mit einer Vielzahl von Datenschutzbehörden konfrontiert. Unter der DSGVO

soll das sogenannte „One-Stop-Shop-Prinzip“ sicherstellen, dass sich Datenverarbeiter auch im Falle landesübergreifender Datenverarbeitung lediglich einer einzelnen, federführenden Aufsichtsbehörde gegenüber verantworten sollen, nämlich jener ihres Hauptsitzes. Diese federführende Behörde ist unter der DSGVO jedoch zur Kooperation mit allen Behörden verpflichtet, deren Bürgerinnen und Bürger betroffen sind. Im Falle von Uneinigkeiten über Zuständigkeiten oder Entscheidungen einzelner Behörden können jene Behörden – und auch die EU-Kommission – ein sogenanntes Kohärenzverfahren des neuen Europäischen Datenschutzausschusses in die Wege leiten. Im Europäischen Datenschutzausschuss finden sich Vertreter und Vertreterinnen aller nationalen Datenschutzbehörden zusammen und können Beschlüsse der federführenden Behörde mit einer Zweidrittelmehrheit aufheben bzw. eigene Beschlüsse treffen.

Die Möglichkeit, für Behörden und Verarbeiter EU-weit bindende Entscheidungen zu setzen, macht den Europäischen Datenschutzausschuss zu einem mächtigen Gremium. Dessen Kompetenzen sollen zu einer einheitlichen Anwendung der DSGVO führen, eröffnen zugleich aber eine Vielzahl möglicher Konflikte. Die Mitgliedsstaaten haben teils sehr verschiedene Verständnisse von Datenschutz und seiner Durchsetzung, die nun ausgehandelt werden müssen. Dabei werden einzelne Behörden je nach Problem unterschiedliche Allianzen bilden und Kompromisse akzeptieren müssen. Zwar kann dies auf kurze Sicht eine Schwächung einzelner nationaler Datenschutzregelungen bedeuten, langfristig stärkt eine EU-weit vereinheitlichte Anwendung jedoch das allgemeine Niveau der Regeldurchsetzung und trägt dazu bei, die EU als global wirkmächtigen Regulierungsakteur zu etablieren.

Obwohl die jahrelangen Verhandlungen zur Neuordnung des europäischen Datenschutzes also abgeschlossen sind, werden Aushandlungsprozesse den Datenschutz noch stärker prägen als bisher. Somit werden bestehende Konflikte im Datenschutz fortgesetzt, neue Kontroversen entstehen und verdrängte wieder aufbrechen. Die DSGVO wird deshalb oft als unfertig kritisiert, doch gesellschaftliche Konflikte um Datennutzung und die Vielfalt der europäischen Datenschutzverständnisse ließen eine andere Form der Regulierung nicht zu.

Die Politik des Datenschutzes beginnt mit Geltung der DSGVO erst. Für die politikwissenschaftliche Datenschutzforschung heißt das, dass sie nicht bei der Analyse formaler Gesetzgebungsprozesse stehen bleiben darf, sondern die sich formierenden Konstellationen und Konflikte im europäischen Feld des Datenschutzes in den Blick nehmen muss. Eine solche Analyse ist nicht nur aus sozialwissenschaftlicher Sicht relevant. Die Datenschutzgrundverordnung wird große Bereiche der Digitalpolitik der kommenden Jahre prägen, und das über die Grenzen der EU hinaus.

Magnus Römer ist wissenschaftlicher Mitarbeiter in der Projektgruppe Politikfeld Internet. Im Forschungsprojekt „Assessing Big Data“ befasst er sich mit Datenschutzbehörden in Mehrebenensystemen. *(Foto: David Ausserhofer)*

magnus.roemer@wzb.eu

Literatur

Bellanova, Rocco: „Digital, Politics, and Algorithms: Governing Digital Data through the Lens of Data Protection“. In: European Journal of Social Theory, 2017, Jg. 20, H. 3, S. 329–347.

De Hert, Paul/Papakonstantinou, Vagelis: „The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?“ In: Computer Law & Security Review, 2016, Jg. 32, H. 2, S. 179–194.

Newman, Abraham L.: „Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive“. In: International Organization, 2008, Jg. 62, H. 1, S. 103–130.

Wright, David/Hert, Paul de (Hg.) (2016): Enforcing Privacy. Regulatory, Legal and Technological Approaches. Law, Governance and Technology Series 25. Cham: Springer International Publishing.