Jörg Pohle, Benjamin Bergemann & Jan Schallaböck

Für eine Digitalisierung des Datenschutzes[1]

Datenschutz schützt die Grundrechte bei der Digitalisierung. Der Datenschutz selbst ist dagegen kaum digitalisiert. Im Gegensatz zu anderen Bereichen – etwa dem Gesundheitswesen – gibt es keine Debatte über die ausbleibende Digitalisierung des Datenschutzes. Im folgenden Beitrag eröffnen Jörg Pohle, Benjamin Bergemann und Jan Schallaböck diese Debatte. Sie diskutieren, warum die fehlende Digitalisierung des Datenschutzes ein politisches Problem ist. Sie stellen Beispiele vor, wo und wie sich Digitalisierung für die Datenschutzkontrolle nutzen lässt und welche Vorteile das für Bürger*innen, Datenverarbeiter, Aufsichtsbehörden und die gesellschaftliche Wirksamkeit des Datenschutzes hätte.

Einleitung

Die praktische Umsetzung des Datenschutzes stützt sich noch immer weitgehend auf Handarbeit und ist geprägt von einem Wildwuchs an Formaten und inkompatiblen Systemen. Es fehlt an einer vereinheitlichten Praxis und an etablierten Standards für die Datenschutz-Folgenabschätzung (Artikel 35 DSGVO), für Datenschutz by Design und by Default (Artikel 25), für die Information der Betroffenen (Artikel 12–14) und für die Ausübung der Betroffenenrechte (Artikel 15–18, 20–21). Ausgangspunkt für all diese Mechanismen ist regelmäßig eine Bestandsaufnahme, die auch in die Verfahrensdokumentation Eingang findet (Artikel 30).

Der europäische Gesetzgeber hat mit Einführung der Datenschutz-Grundverordnung (DSGVO) sowohl die Pflicht zur Registrierung der Verfahrensdokumentation als auch das ersatzweise bestehende allgemeine Recht auf Einsicht in die Verfahrensdokumentation, welche im alten Bundesdatenschutzgesetz (BDSG) noch enthalten waren, über Bord geworfen. Diese Möglichkeiten – zu Zeiten des BDSG recht unbekannt und wohl nur sehr selten genutzt – galten als reiner Formalismus, weswegen sie wohl als verzichtbar angesehen wurden. Es zeigt sich jedoch gerade in der Umsetzung der DSGVO, dass die Verfahrensdokumentation als Bestandsaufnahme eine unverzichtbare Voraussetzung für den rechtskonformen Umgang mit personenbezogenen Daten darstellt. Öffentliche und elektronisch zugängliche Verfahrensdokumentationen wür-

Zitiervorschlag:
Pohle, Jörg; Bergemann, Benjamin; Schallaböck, Jan (2020): Für eine Digitalisierung des Datenschutzes, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 231/232 [59(3-4)], S. 117-129.

den Austausch, Analyse und Vereinheitlichung erlauben. Sie könnten damit nicht nur die Einhaltung und Kontrolle von Datenschutzvorschriften erheblich erleichtern, sondern auch den Weg für eine weitergehende Automatisierung des Datenschutzes ebnen.

Kurz: Die Chancen der Digitalisierung bei der Umsetzung des Datenschutzes werden nicht genutzt. Und das hat nicht nur Folgen für die Verantwortlichen selbst, sondern auch für die Betroffenen und den Schutz ihrer Grundrechte, sowie für die Aufsichtsbehörden und nicht zuletzt auch für die Gesellschaft insgesamt. Im Folgenden wollen wir den Versuch unternehmen, die Vision und die Wirklichkeit eines automatisierten Datenschutzes aus verschiedenen Perspektiven zu kartieren und schlagen anschließend erste Schritte zu einer Automatisierung des Datenschutzes vor. Wir wollen dazu beitragen, die Automatisierung des Datenschutzes über *Privacy Enhancing Technologies* (PETs) und formale *Compliance* hinaus zu denken und zu einer datenschutz*politischen* Frage zu machen.

Datenschutz und Automatisierung

Datenschutz adressiert die unerwünschten Folgen moderner Informationsverarbeitung und zielt darauf ab, das Eintreten dieser Folgen durch die konkrete organisatorische und technische Gestaltung der Verarbeitung zu verhindern (Steinmüller et al. 1971: 44). Die DSGVO fokussiert dabei, wie Artikel 1 Abs. 2 explizit formuliert, auf Risiken für Grundrechte und Grundfreiheiten als Teilmenge aller gesellschaftlich unerwünschten Folgen.

Als Ausdehnung des Rechtsstaatsprinzips auf alle Informationsverarbeitungen (Steinmüller 1976: 14), also auch auf diejenigen in privater Verantwortlichkeit, legt das Datenschutzrecht einen starken Fokus auf Pflichten für Verarbeiter und die Kontrolle durch Aufsichtsbehörden. Aber auch die Gestaltung von Organisationen, Verarbeitungsprozessen und informationstechnischen Systemen wird adressiert – und das schon seit den Anfängen der Datenschutzdebatte (Pohle 2015). „Soziale Freiheit ist nunmehr nur noch möglich, wenn sie von vornherein in die Konstruktion der Informationssysteme eingeplant, auch mit den Mitteln der modernen Daten- und Kommunikationstechnologien technisch und organisatorisch abgesichert und schließlich in ihrem sozialen Umfeld rechtlich verankert und gewährleistet wird“ (Steinmüller et al. 1978: 2). Jede rechtliche, organisatorische und technische Gestaltung von Informationsverarbeitung setzt jedoch voraus, dass Verarbeitungen beherrschbar gemacht werden, um ihre Folgen erfassen und entsprechende Maßnahmen ergreifen zu können (Steinmüller 1979: 187).

Zu all dem bedarf es nicht nur geeigneter Methoden, sondern auch der Werkzeuge, die bei der Umsetzung helfen – von der individuellen und systemischen Bestandsaufnahme über die Risikoanalyse und die Auswahl der geeigneten Maßnahmen bis hin zur Kontrolle der Datenverarbeitungspraxis. Ebenso braucht es grundlegende Standards, die nicht nur die Vergleichbarkeit von Transparenzinformationen und ergriffe-

nen Maßnahmen erlauben, sondern selbst auch als Treiber des Standes der Technik wirken können.

Für die *Verantwortlichen* geht es primär um die Erfüllung ihrer datenschutzrechtlichen Pflichten. Voraussetzung hierfür ist die Selbstbeobachtung bezüglich ihrer Strukturen und Praktiken, die das Datenschutzrecht – weitgehend implizit – als Vorbedingung für den praktischen Grundrechtsschutz einfordert. Viele, gerade kleinere, Verantwortliche sind damit überfordert – nicht zuletzt, weil sie sich mühsam selbst überlegen müssen, wie und mit welchen Werkzeugen sie Datenschutz praktizieren sollen.

Für die *Betroffenen* geht es nicht allein um die Vergleichbarkeit von Transparenzinformationen, die bei manueller Erstellung ohnehin nicht erreichbar ist, sondern auch um die Wahrnehmung ihrer Rechte gegenüber den Verantwortlichen. Ohne entsprechende Werkzeuge bleiben sie hierbei auf deren Kooperation angewiesen.

Auch die *Aufsichtsbehörden* werden durch die fehlende Automation des Datenschutzes in ihrer Arbeit behindert. Das gilt intern, bei der Bearbeitung von Vorgängen oder bei der Kontrolle von Verantwortlichen, wenn sie sich erst durch Berge von Papier kämpfen müssen, bevor sie überhaupt zur inhaltlichen Prüfung schreiten können. Aber es gilt auch gegenüber der Öffentlichkeit, wenn sie ihrer Aufgabe, „die Anwendung dieser Verordnung [zu] überwachen" (Artikel 57 Abs. 1 Buchstabe a DSGVO), nicht angemessen nachkommen können, weil sie ohne entsprechende automatisierte Verfahren gar nicht die Möglichkeit haben, moderne Informationsverarbeitung jenseits von Einzelfällen zu untersuchen.

Und nicht zuletzt: Wie wir gerade erst wieder in der Corona-Krise lernen, ist es unerlässlich, eine vernünftige Datenbasis zu haben, auf deren Grundlage die *Gesellschaft* über mögliche Maßnahmen diskutieren und entscheiden kann. An einer solchen Datenbasis fehlt es aber für eine der wohl entscheidenden gesellschaftlichen Entwicklungen der vergangenen Jahre und Jahrzehnte: Über den gesellschaftlichen Stand der Datenverarbeitung und deren Implikationen gibt es überraschenderweise keine vernünftige empirische Grundlage, obwohl das tragende Paradigma der Digitalisierung die Vollerhebung zu sein scheint (Klumpp 2014: 277 ff.). Es grenzt an Absurdität, dass Datenverarbeiter nahezu jeden unserer Handlungsschritte protokollieren, aber die Gesellschaft nicht zur Kenntnis nehmen kann, was die Datenverarbeiter tun.

Die Automatisierung des Datenschutzes ist bisher – wenn überhaupt – Gegenstand von Fachdebatten. Dominierend ist hier der Diskurs zu *Privacy Enhancing Technologies* (PETs), in dem die Automatisierung des Datenschutzes allerdings oft auf einen rein individualistisch verstandenen Begriff von „*Privacy*" begrenzt wird (Diaz/Gürses 2012), bei dem ein umfassenderes Verständnis von Datenschutz auf der Strecke bleibt. Versuche, das Thema ganzheitlicher zu diskutieren (vgl. etwa Schartum 2001), sind in der Vergangenheit schnell versandet. Auch anlässlich des zweiten Jahrestages der Anwendbarkeit der DSGVO wurde die Automatisierung des Datenschutzes kaum thematisiert (Ausnahmen: Privacy Company 2019; Digitale Gesellschaft 2020).

Die Diskussion um die Digitalisierung des Datenschutzes wollen wir im Folgenden aus diesen vier Perspektiven – Verantwortliche, Betroffene, Aufsichtsbehörden und Gesellschaft – aufgreifen.

Der gesellschaftliche Wert eines automatisierten Datenschutzes

Die aufgeklärte bürgerlich-liberale Gesellschaft unterstellt, dass ihre politische Deliberation und Entscheidungsfindung auf der Basis umfassender und fundierter Informationen über die Phänomene, über die sie entscheiden soll oder will, stattfindet. Für den gesellschaftlichen Stand der Digitalisierung liegen solche Informationen jedoch bisweilen kaum oder gar nicht vor. Dies beginnt schon bei der Schwierigkeit, den Stand der Technik zu bestimmen, da die Einsatzszenarien kaum systematisiert sind. Noch relevanter ist es für die Frage des konkreten Einsatzes von Verfahren, Systemen und „Code" – vor allem in der Breite und nicht nur an ausgewählten Beispielen. Und es gilt für die Praktiken, die damit verbunden sind. Schließlich geht es vor allem um die Folgen für Individuen, Gruppen und die Gesellschaft, für individuelle Rechte und gesellschaftliche Strukturen.

Als Beispiel könnte man die gegenwärtige „Algorithmen"-Debatte heranziehen, in der über „ethische" Anforderungen an „Algorithmen" diskutiert wird, ohne dass eine Bestandsaufnahme zugrunde gelegt wurde. Wir wissen nicht viel über die *konkreten* Risiken, die in *konkreten* Situationen von *konkreten* Akteuren durch den Einsatz *konkreter* Informatiksysteme für je *konkrete* Betroffene oder gesellschaftliche Werte erzeugt, verstärkt oder verstetigt werden – geschweige denn über deren Relevanz.

Angemessener erscheint es, wenn Verantwortliche ihre Bestandsaufnahme und Risikoanalyse technikgestützt und auf der Basis offener und frei verfügbarer Standards vornähmen und die Ergebnisse maschinenlesbar zugänglich machten, damit diese zusammengetragen und ausgewertet werden können. Auf der gesellschaftlichen Ebene geht es dabei nicht – oder nicht vorrangig – darum, bei einzelnen Verantwortlichen Probleme, Versäumnisse oder gar Gesetzesverstöße aufzudecken, sondern um das Feststellen eines „*State of the digital World*": Wie sieht die Informationsverarbeitung eigentlich in der Praxis aus? Wie ist sie organisiert? Welche Daten werden verarbeitet, für welche Zwecke, in welchem Umfang, mit welchen Betroffenen? Welche Risiken ergeben sich daraus konkret? Welche der Risiken werden im Zuge von Organisations-, Verfahrens- und Technikgestaltung abgemildert oder verhindert – und welche bleiben trotz der erforderlichen organisatorischen und technischen Maßnahmen bestehen? Welche der Maßnahmen stellen dabei den Stand der Technik dar und welche fallen dahinter zurück? An welchen Stellen oder in Bezug auf welche Risiken gibt es deutliche Lücken in der Abdeckung durch technische und organisatorische Maßnahmen, die es zu schließen gilt – und deren Schließung gesellschaftlich organisiert und möglicherweise auch finanziert werden sollte?

Potentiale für Datenverarbeiter

Für Verantwortliche und Auftragsverarbeiter ergibt sich das Interesse an einer Automatisierung des Datenschutzes pragmatisch aus der Bewältigung der Komplexität des Datenschutzrechts und seinen Anforderungen. Insbesondere für größere Organisatio-

nen ist die Umsetzung des Datenschutzrechts oft nur ein weiteres *Compliance*-Projekt, das es zu managen gilt – mit allen Vor- und vor allem Nachteilen, die eine solche Rationalisierung des Grundrechtsschutzes in Organisationen mit sich bringt (Waldman 2019).

Die DSGVO sieht für Verantwortliche und Auftragsverarbeiter eine Vielzahl von Pflichten vor, deren Einhaltung sie auch nachweisen müssen. Vielfach herrscht erhebliche Uneinigkeit darüber, was Datenverarbeiter genau tun müssen, um rechtmäßig zu handeln.[2] Grundvoraussetzung ist jedoch immer die Selbstbeobachtung der eigenen Datenverarbeitung. Erst die Bestandsaufnahme erzeugt Transparenz und damit Prüfbarkeit. Sie ist notwendige Voraussetzung für eine beherrschbare IT. Auch die DSGVO verlangt – teilweise explizit (etwa unter den Voraussetzungen des Artikel 30), teilweise implizit – die Identifikation und Dokumentation der eigenen Verarbeitungstätigkeiten. Je nach Blickwinkel gehören dazu etwa die Daten und Datenflüsse, die Prozesse, die verwendeten IT-Systeme, die beteiligten Akteure, die Rechtsgrundlagen, aber auch bereits ergriffene technische und organisatorische Maßnahmen (TOM) und ein Löschkonzept.

Softwaregestützte Datenschutz-Managementsysteme könnten die Bestandsaufnahme nicht nur erleichtern, sondern auch für mehr Selbstbeobachtung und -reflexion bei den Datenverarbeitern sorgen. Sie könnten durch Schnittstellen zu eingesetzten Anwendungen und deren Protokollierungsfunktionen die Daten und Datenflüsse sowie die verwendeten technischen Komponenten automatisiert erfassen. Die verbreiteten Systeme bieten vor allem Vorlagen und Fragenkataloge zur Dokumentation der eigenen Prozesse und Systeme. Ihr Fokus liegt häufig auf der Erstellung der Verarbeitungsverzeichnisse. Sie verstärken damit die in der Praxis oft anzutreffende Engführung der Bestandsaufnahme auf das Führen eines Verzeichnisses der Verarbeitungstätigkeiten nach Artikel 30.

Datenschutz-Managementsysteme könnten die Selbstreflexion des Verantwortlichen fördern, wenn sie die dokumentierten Informationen aufbereiten und durch Prüfroutinen und -fragen auf begründungsbedürftige Zusammenhänge hinweisen, etwa wenn ein Verein keine Mitgliederverwaltung als Verfahren führt, die Berufung auf die eigenen „berechtigten Interessen“ nicht begründet (Artikel 6 Abs. 1 lit. f) oder alle seine Verfahren auf einem einzigen IT-System betreibt. Einige Softwareprodukte generieren bereits heute Auswertungen auf Basis der eingetragenen Informationen. Was hier erfasst und hervorgehoben wird, hängt ohne Standardisierung jedoch vom Datenschutzverständnis des Herstellers ab.

Die Pflicht zur Bestandsaufnahme geht über in die Pflicht des Verantwortlichen, die durch die eigene Datenverarbeitung erzeugten Risiken für die Betroffenen zu erkennen und durch technische und organisatorische Maßnahmen zu beherrschen (Artikel 24). Bei besonders riskanten Verfahren muss die Risikoanalyse und -behandlung in Form einer Datenschutz-Folgenabschätzung erfolgen (Artikel 35). Das wiederum setzt eine Vorab-Risikobewertung bei *allen* Verfahren voraus, um überhaupt die riskanten unter ihnen identifizieren zu können (Wybitul 2017: 543 f.).

Der Nutzen standardisierter Abfragen und Reportings bei der Risikobewertung, die einige der verfügbaren Systeme heute schon bieten, ist offenkundig: Sie leiten den Verantwortlichen an und erzeugen einheitliche und damit vergleichbare Risikoanaly-

sen. Jedoch ist die Risikoanalyse eine der Anforderungen der DSGVO, über deren rechtmäßige Umsetzung die Meinungen häufig auseinandergehen. Ein Vergleich von drei gängigen Methoden zur Durchführung von Datenschutz-Folgenabschätzungen in Frankreich, Großbritannien und Deutschland hat gezeigt, dass selbst die Aufsichtsbehörden unterschiedliche Auffassungen dazu vertreten, was überhaupt ein Datenschutzrisiko darstellt, von welchen Angreifern sie ausgehen und wie man sie am besten identifiziert (Martin et al. 2020).

Softwaregestützte Datenschutz-Managementsysteme müssten den Verantwortlichen helfen, diese Unsicherheiten zu bewältigen. Das geht nur, wenn sie ihre Methode zur Risikoanalyse ausweisen oder erklären: Welche Angreifer werden betrachtet? Welche Risiken werden betrachtet – die für alle Grundrechte oder nur die Informationssicherheits- oder Privatheitsrisiken? Wie wird die Abschätzung der Schwere und Eintrittswahrscheinlichkeit operationalisiert? Das ist nicht nur eine notwendige Voraussetzung für externe Prüfbarkeit, etwa durch Aufsichtsbehörden, sondern auch um den Verantwortlichen den Gegenstand und die Grenzen der eigenen Risikoanalyse zu verdeutlichen. Derzeit ist uns keine Software bekannt, die diese Anforderungen erfüllt.[3]

Nicht zuletzt müssten zukünftige Systeme sicherstellen, dass sie die Risikoanalyse nicht auf eine Checkliste reduzieren. Zwar rationalisieren sie den Prüfungsprozess, sie verleiten Verantwortliche aber auch dazu, abzuhaken statt abzuwägen und nur das Abhaken zu dokumentieren. Zukünftige Systeme müssten die Verantwortlichen deshalb per Design zu Reflexion, Abwägung und Begründung zwingen. Durch Anleitung, Vereinheitlichung und maschinenlesbare Dokumentation könnten sie trotzdem ihr Rationalisierungsversprechen einlösen.

Werkzeuge für Aufsichtsbehörden

Auch die Aufsichtsbehörden würden von einer stärkeren Automatisierung des Datenschutzes in ihrer Arbeit profitieren – und als Folge die Betroffenen, die Gesellschaft, aber auch die Verantwortlichen. Sie begleiten zwar die Digitalisierung von Verwaltung und Wirtschaft, aber als Avantgarde ihrer eigenen Digitalisierung fallen sie bisher nicht auf. Die Frage, wie die Datenschutzbehörden technisch arbeiten, ist weitgehend unbekannt, denn auch die Verfahrensdokumentationen der Aufsichtsbehörden sind nicht öffentlich. Vielleicht ist die Situation ja besser als gedacht. Für eine umfassende Automatisierung des Datenschutzes müssten die Aufsichtsbehörden in die Fußstapfen der ersten Generation von Datenschützer*innen treten und wie diese zu „*begeisterten Automatisierungsbefürworterinnen*“ werden (Pohle 2018: 238).

Naheliegenderweise kann eine stärkere Digitalisierung des aufsichtsbehördlichen Datenschutzes insbesondere die Vermeidung von Medienbrüchen fördern, die derzeit noch einen nicht unerheblichen Mehraufwand sowohl in der täglichen Arbeit der Behörden, aber auch in der Kommunikation mit ihnen verursachen. Bislang beschränkt sich dies *prima facie* auf die Möglichkeit, die Berufung von betrieblichen Datenschutz-

beauftragten online zu melden – und nicht mehr nur per Brief oder Fax. Aber selbst hierbei handelt es bislang nur um ein Webformular.

Sinnvoll erschiene jedoch ein übergreifendes Gesamtkonzept, in dem es möglich wird, über definierte technische Schnittstellen („*Application Programming Interfaces*“, APIs) softwaregestützte Datenschutz-Managementsysteme an ein aufsichtsbehördliches System anzubinden. Neben Berufungsmeldungen könnte so die gesamte Bandbreite der Kommunikation automatisiert werden.

Ein gutes Beispiel sind Meldepflichten zu Datenschutzverletzungen nach Artikel 33 und 34 DGSVO. Die Meldung von Datenschutzverletzungen stößt behördenintern Verfahrens- und Dokumentationsschritte an. Oft erfordern sie auch die Kommunikationen mit den Verantwortlichen und den Betroffenen. Technische Schnittstellen würden diese Prozesse erleichtern und strukturieren. Zugleich würden die generierten Daten dabei helfen, umfassende Aussagen über Häufigkeit, Schwere und Auswirkungen solcher Datenschutzverletzungen, möglicherweise auch statistische Aussagen über besonders häufig betroffene Branchen, Systeme oder Verarbeitungstätigkeiten zu gewinnen. Wenn die bei den Verantwortlichen eingesetzten Systeme dann auch noch die technischen Protokolldateien mitliefern würden, dann könnten die Aufsichtsbehörden darüber auch mehr, genauere und damit sicher hilfreichere Informationen über die Vorfälle erhalten, als dies derzeit bei manueller Meldung durch Verantwortliche der Fall ist. Für solch ein vertrauenswürdiges *Self-Reporting* bedarf es allerdings technischer Prüfanker in den betreffenden Systemen, die an standardisierten Schnittstellen integre Informationen über Systemzustände liefern können – und diese müssen entwickelt werden (Rost in Pohle/Knaut 2014: 270, Rn. 185).

Eine stärkere Digitalisierung des Datenschutzes würde auch dabei helfen, die beschränkten Ressourcen der Aufsichtsbehörden zielgerichteter einzusetzen, weil die Automatisierung von Teilen der Aufsichtstätigkeit Zeit schafft, sich den wesentlichen Problemen zu widmen und nicht im Klein-Klein der Formalismen zu verharren. Die Aufsichtsbehörden könnten Register für die Verzeichnisse der Verarbeitungstätigkeiten (Artikel 30) und die Datenschutz-Folgenabschätzungen (Artikel 35) einrichten und betreiben, die dort in maschinenlesbarer Form hochgeladen werden müssen, um dann einfache Prüfungen, etwa auf Vollständigkeit, Widerspruchsfreiheit oder auch fehlende Begründungen bei einem Bezug auf das berechtigte Interesse (Artikel 6 Abs. 1 lit. f), automatisiert durchführen zu können. Zugleich ließe sich damit eine Vergleichbarkeitsgrundlage schaffen, etwa über Branchen, eingesetzte Systeme oder Organisationsgrößen, die bei der Identifizierung des Standes der Technik helfen, an dem sich Verarbeiter bei Auswahl und Einsatz von Datenschutz- und Sicherheitsmaßnahmen (Artikel 25 und 32) orientieren müssen, und damit gleichzeitig auch als dessen Treiber wirken kann.

Wenn diese Informationen darüber hinaus in *öffentlichen* Registern bereitgestellt würden, ließen sie sich von den Verantwortlichen auch mit ebenso öffentlichen wie standardisierten Datenschutzerklärungen verknüpfen, aus denen die möglichen Grundrechtsrisiken klar erkennbar sind, die aber zugleich von Aufsichtsbehörden oder Gruppen aus der Zivilgesellschaft mit weiteren Erklärungen oder Informationen versehen sind und somit die Allgemeinverständlichkeit noch einmal erhöhen.

Chancen für Betroffene

Die seit vielen Jahren diskutierten und entwickelten Hilfsmittel für Betroffene basieren auf einer rechtspolitisch fragwürdigen Verschiebung des Datenschutzproblems: sie individualisieren Verantwortung. Statt die Datenverarbeiter zu zwingen, den Schutz der Grundrechte der Betroffenen sicherzustellen, zwingen die Vertreter*innen des sogenannten „Selbstdatenschutzes“ (grundlegend: Roßnagel 1997) die Betroffenen, sich selbst um den Schutz ihrer Grundrechte zu kümmern. Zu den Systemen, die dieser Idee folgen, gehören etwa Anonymisierungs- und Verschlüsselungssysteme, Identitätsmanagementsysteme oder Selbstbeobachtungssysteme. Hierzu gehören etwa Apps auf Smartphones, die Datenflüsse anderer Apps mitprotokollieren, in der Hoffnung, damit den „Datenschatten“ (Anér 1972) der Betroffenen bei Verarbeitern offenzulegen. Solche Systeme können deshalb als gescheitert gelten, da sie sich in der Praxis nicht breit durchgesetzt haben, aber auch praktisch kaum zu einer Verbesserung des Grundrechtsschutzes beitragen können. Sie ignorieren völlig, dass der Datenschutz nicht nur individuelle Beeinträchtigungen, sondern auch gesellschaftliche Folgen im Blick haben muss. Statt die Betroffenen zur digitalen Selbstverteidigung zu nötigen, müsste es um Ansätze gehen, die den Betroffenen helfen, die Datenverarbeiter zu zwingen, ihrer Verantwortung gerecht zu werden.

Eine den Betroffenen dienende Digitalisierung des Datenschutzes müsste zuallererst Werkzeuge zur Verfügung stellen, mit denen Betroffene ihre Rechte gegenüber den Verarbeitern wahrnehmen und durchsetzen können. Um dabei nicht von der „Gnade“ der Verarbeiter abhängig zu sein, bedarf es dazu in den Systemen der Verarbeiter technischer Schnittstellen, mit denen sich Assistenzsysteme der Betroffenen verbinden können, ohne dass diese Verbindung von den Verarbeitern kontrolliert oder gar unterbunden werden könnte. Über diese Schnittstellen würden die Systeme der Verarbeiter nicht nur „Auskunft“ über die beim Verarbeiter über die Betroffenen gespeicherten personenbezogenen Daten erteilen, sondern vor allem auch über die Funktionsweise des Systems selbst, also über die Zwecke, die Verarbeitungsprozesse („Algorithmen“) und über den Stand der Schutzmaßnahmen. Zugleich könnten die Betroffenen darüber auch ihre in der DSGVO statuierten Rechte wahrnehmen, etwa auf Korrektur, Widerspruch oder Löschung. Ein Betroffenen-Assistenzsystem setzt demnach eine entsprechende Technikgestaltung aufseiten des Verarbeiters voraus, der damit Eigenschaften – und dazu gehören auch die damit erzeugten Grundrechtsrisiken – nicht einfach in einer Datenschutzerklärung behaupten, sondern über die gleichen Systeme abrufbar machen muss, die die Daten verarbeiten (für einen frühen Vorschlag für ein solches System, das allerdings nie praktisch zum Einsatz kam, siehe Nguyen/Mynatt 2002). Dabei lässt sich die Integrität der Ausgaben des Systems aufseiten der Verarbeiter gegenüber den Betroffenen dann wieder von den Aufsichtsbehörden überprüfen.

Die Bereitstellung von standardisierten technischen Schnittstellen in den Datenverarbeitungssystemen der Verantwortlichen würde zugleich verhindern, dass es zu einem Wildwuchs an Assistenzsystemen für Betroffene kommt, die dann weniger oder gar nicht eingesetzt werden, oder dass Datenverarbeiter die Gestaltung dieser Syste-

me kontrollieren. Eine solche Situation gibt es heute schon bei Plattformen: Wenn die Betroffenen dort Accounts haben, können sie nach Anmeldung auf einen Teil der über sie gespeicherte Daten zugreifen und diese teilweise korrigieren oder löschen. Jedoch folgen die Plattformen jeweils eigenen Vorstellungen, welche Daten sie wie darstellen und welche Möglichkeiten sie dabei Betroffenen gewähren. Standardisierte technische Schnittstellen würden es erlauben, dass es einzelne Assistenzsysteme bei den Betroffenen gibt, mit denen sich die Datenverarbeitungspraxis einer Vielzahl von Verarbeitern kontrollieren lässt (vgl. das Prinzip der „Unterwachung", Luhmann 1969/2016).

Ungeklärt ist allerdings die Frage, wie mit technischen Werkzeugen auch Kollektivinteressen wie die Vereinigungsfreiheit gestärkt werden könnten.

Der Weg zum Ziel

Automatisierung beeinflusst immer das Informations- und Machtgleichgewicht einer Gesellschaft und ihrer Teilbereiche (Steinmüller 1975: 510). Das gilt auch für die Automatisierung des Datenschutzes selbst. Wie wir versucht haben zu zeigen, kann eine Automatisierung des Datenschutzes dabei helfen, die Machtverhältnisse bei der Umsetzung des Datenschutzes zugunsten der Gesellschaft und der Betroffenen zu verschieben. Diese Potentiale sind jedoch keine lineare, selbsterfüllende Erfolgsgeschichte. Sie müssen errungen werden. Zudem kann – und wird – es auch zu Verselbstständigungen, Anomalien und nicht intendierten Nebenfolgen bei der Automatisierung des Datenschutzes kommen. Neben der bereits angedeuteten Reduktion auf Selbstdatenschutz und formale *Compliance* könnte eine Automatisierung des Datenschutzes etwa auch zu einer nicht akzeptablen Überwachung durch Aufsichtsbehörden führen oder Missbrauchspotentiale im unternehmerischen Bereich durch übergriffige Konkurrenten oder neue Monopolisten schaffen. Aus unserer Sicht sind das jedoch keine Argumente gegen, sondern für eine wachsame Aushandlung und Erprobung eines digitalisierten Datenschutzes. Wir schlagen vor, diesen Prozess durch Typisierung, Standardisierung und die Beteiligung an Softwareentwicklungsprojekten zu beginnen.

Im Datenschutz mangelt es bisher an *Typisierung*, vor allem in der Breite. Als Typisierung im Datenschutz verstehen wir Anforderungs- und Umsetzungsbeschreibungen für wiederkehrende Datenverarbeitungen (z. B. beim Betrieb einer Website) in wiederkehrenden Kontexten (z. B. bei Vereinen und kleinen Unternehmen) und unter Einsatz verbreiteter Mittel (z. B. auf Basis von Wordpress). Typisierung könnte auch in die Bereitstellung von Konfigurationsdateien münden, mit denen sich die Datenschutzkonformität der Systeme auch für ressourcenschwache Verarbeiter wie Vereine herstellen lässt. Die Typisierung deckt konkrete Standardfälle ab, aber auch nur diese. Sie bleibt damit immer unvollständig, was sie von der stärker auf Verallgemeinerung zielenden Standardisierung unterscheidet. Die Typisierung kann der Standardisierung, der Zertifizierung oder *Codes of Conduct* (Artikel 40) als erster Ordnungsversuch vorausgehen oder sie zusätzlich konkretisieren. Die bisherigen vereinzelten Versuche von Typisierungen, etwa Generatoren für Datenschutzerklärungen, vorgefertig-

te Verarbeitungsverzeichnisse oder Handreichungen von Aufsichtsbehörden, sind ein Tropfen auf den heißen Stein.

Die Situation im Bereich der *Standardisierung* ist kaum besser. Es gibt originäre Datenschutzstandards wie das Standard-Datenschutzmodell, die bisher noch wenig verbreitet sind. Daneben existieren datenschutzrelevante ISO-Standards, deren Verhältnis zur DSGVO nicht geklärt ist. Bei den Standardisierungsverfahren stellt sich zudem die Frage nach der *Governance* inklusive der demokratischen Kontrolle, also die Frage, wie die Standardisierungsorganisationen eigentlich ihre Entscheidungen fällen und wer zu beteiligen ist. In dieser Frage überzeugen klassische Standardisierungsprozesse nicht immer. Oft beteiligen sich nur die großen Marktakteure, weil sie über ausreichend Personal, Finanzen und *Know-How* verfügen, was zu einem entsprechenden Ungleichgewicht in den Ergebnissen führen dürfte. Zudem sind viele Standards nicht frei zugänglich, was die gesellschaftliche Auseinandersetzung mit ihnen und nicht zuletzt auch die Integration in freie Software verunmöglicht. Es bedarf öffentlicher Förderung, um auch Akteuren aus der Zivilgesellschaft und der Wissenschaft den Zugang zu Standardisierungsprozessen zu erleichtern. Denn nicht zuletzt sind es am ehesten diese Akteure, die das gesellschaftliche Interesse an auffindbaren, zugänglichen, interoperablen und wiederverwendbaren Standards in diesen Prozessen vertreten können.

Um die Jahrtausendwende war in der Datenschutzdebatte kurzzeitig eine Forderung populär, die es verdient, als dezidiert politische Forderung wieder erhoben zu werden: Datenschutzaufsichtsbehörden sollen sich aktiv in die Softwareentwicklung einbringen (Kessel 1998, Schartum 2001). Eine aktive Beteiligung an Softwareentwicklungsprojekten würde es Aufsichtsbehörden nicht nur erlauben, das Prinzip der „Programmkontrolle“ (Steinmüller et al. 1978: 91 f.) in die Praxis zu tragen, damit sichergestellt wird, dass Anwendungssysteme nur genau das tun *können*, was sie tun *sollen* (Datenschutz by Design, Artikel 25). Wie schon bei der Frage der Typisierung geht es bei einer solchen Beteiligung nicht darum, alles abzudecken, also sich etwa in alle Softwareentwicklungen einzumischen. Ziel sollte eher sein, nach strategischen Kriterien solche Projekte auszuwählen, die als Treiber des Standes der Technik in möglichst großen Bereichen über das einzelne Projekt hinaus wirken können – als „*strategic software development*“ vergleichbar zu „*strategic litigation*“. Sinnvollerweise sollte es sich dabei um Freie-Software-Projekte handeln, um einerseits einen breiten Einsatz in der Praxis und andererseits eine Weiternutzung des in die Software geflossenen Wissens im Rahmen weiterer Projekte zu ermöglichen. Die gleichen Kriterien sollten zivilgesellschaftliche Akteure leiten, wenn sie sich – was sie dringend sollten – in die Softwareentwicklung einbringen.

Ende der informationellen Selbstbeschränkung

Datenschutz ist entstanden, um den gesellschaftlichen Problemen von IT-Systemen gerecht zu werden. Was ist naheliegender, als dafür auch IT-Systeme zu benutzen? Datenschutz dient der Einhegung von Machtungleichgewichten bei der automatisierten Informationsverarbeitung. Ein Datenschutz, der sich selbst der Automation verweigert, droht das Machtungleichgewicht, das er einzuhegen sucht, noch zu vergrößern. Der Aufruf zur Aneignung geeigneter Produktionsmittel gilt, wie wir gezeigt haben, nicht nur für die Aufsichtsbehörden. Auch die Datenschützer*innen bei den Verantwortlichen, in der Zivilgesellschaft und in der Wissenschaft müssen die Digitalisierung des Datenschutzes zu ihrer Aufgabe machen.

JÖRG POHLE Jahrgang 1979, Dr. rer. nat., Forschungsprogrammleiter „Daten, Akteure, Infrastrukturen“ am Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin; jüngste Veröffentlichung: Datenschutz-Folgenabschätzung für die Corona-App (2020) mit K. Bock, C. R. Kühne, R. Mühlhoff, M. R. Ost und R. Rehak.

BENJAMIN BERGEMANN Jahrgang 1990, M. A., ehrenamtlicher Vorstand der Digitalen Gesellschaft e. V., Berlin; engagiert sich für Grundrechte in der digitalen Welt.

JAN SCHALLABÖCK ist Rechtsanwalt mit Tätigkeitsschwerpunkt im Datenschutzrecht.

Quellen

Anér, Kerstin 1972: Attack is the best defence; in: *Management Informatics*, Jg. 1, H. 5, S. 179–180.

Commission Nationale Informatique et Liberté (CNIL) 2019: The open source PIA software helps to carry out data protection impact assessment, abrufbar unter: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

Diaz, Claudia; Gürses, Seda 2012: Understanding the landscape of privacy technologies;in: Proceedings of the Information Security Summit 2012, S. 58–63.

Digitale Gesellschaft 2020: Verbesserung der DSGVO zum Schutz unserer Grundrechte: Empfehlungen der Digitalen Gesellschaft und des Verbraucherzentrale Bundesverbands (vzbv), abrufbar unter: https://digitalegesellschaft.de/2020/05/verbesserung-der-dsgvo-zum-schutz-unserer-grundrechte/.

Kessel, Werner 1998: Kooperation der Datenschutzbeauftragten mit Hard- und Softwareentwicklern; in: Bäumler, Helmut (Hrsg.), „Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen, Neuwied, S. 182–189.

Klumpp, Dieter 2014: Aufhaltsamer Abstieg zur Heteronomie in einer Softwarewelt?; in: Garstka, Hansjürgen; Coy, Wolfgang (Hrsg.), Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis, Berlin, S. 267–284.

Luhmann, Niklas 1969: Unterwachung. Oder die Kunst, Vorgesetzte zu lenken. Vortrag in Berlin 07.11.1969, Manuskript, posthum erschienen in: Der neue Chef. Herausgegeben und mit einem Nachwort von Jürgen Kaube, Berlin 2016.

Martin, Nicholas et al. 2020: Methoden der Datenschutz-Folgenabschätzung: Welche Unterschiede weisen die verschiedenen methodischen Ansätze auf?; in: *Datenschutz und Datensicherheit*, Jg. 44, H. 3, S. 154–160.

Nguyen, David H.; Mynatt, Elizabeth D. 2002: Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems. GVU Technical Report GIT-GVU-02-16, Georgia Institute of Technology, Atlanta.

Pohle, Jörg 2015: Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens; in: *FIfF Kommunikation*, Jg. 32 , H. 2, S. 41–44.

Pohle, Jörg 2018: Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung. Dissertation, HU Berlin, abrufbar unter https://edoc.hu-berlin.de/handle/18452/19886.

Pohle, Jörg; Knaut, Andrea (Hrsg.) 2014: Fundationes I: Geschichte und Theorie des Datenschutzes, Münster.

Privacy Company 2019: Open letter to the European Commission: ten suggestions for improvement of the GDPR, abrufbar unter: https://www.privacycompany.eu/blogpost-en/open-letter-to-the-european-commission-ten-suggestions-for-improvement-of-the-gdpr.

Roßnagel, Alexander 1997: Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger; in: *Zeitschrift für Rechtspolitik*, Jg. 30, Heft 1, S. 26–30.

Roßnagel, Alexander 2018: DSGVO – was bewirkt sie für den Datenschutz?; in: *vorgänge Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, Jg. 57, H. 221/222, S. 17–29.

Rost, Martin 2018: Risiken im Datenschutz; in: *vorgänge Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, Jg. 57, H. 221/222, S. 79–91.

Schartum, Dag Wiese 2001: Privacy Enhancing Employment of ICT: Empowering and Assisting Data Subjects; in: *International Review of Law, Computers & Technology*, Jg. 15, H. 2, S. 157–169.

Steinmüller, Wilhelm 1974: Datenschutzrechtliche Anforderungen an die Organisation von Informationszentren; in: Schmitz, P. (Hrsg.), Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung, Berlin, S. 187–205.

Steinmüller, Wilhelm 1975: Automationsunterstützte Informationssysteme in privaten und öffentlichen Verwaltungen: Bruchstücke einer alternativen Theorie des Datenzeitalters; in: *Leviathan*, Jg. 3, H. 4, S. 508–43.

Steinmüller, Wilhelm 1976: Informationsrecht und Informationspolitik; in: Steinmüller, Wilhelm (Hrsg.), Informationsrecht und Informationspolitik, München, S. 1–20.

Steinmüller, Wilhelm 1979: Legal Problems of Computer Networks: A Methodological Survey; in: *Computer Networks*, Jg. 3, S. 187–198.

Steinmüller, Wilhelm et al. 1971: Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1.

Steinmüller, Wilhelm et al. 1978: Datenschutz bei riskanten Systemen. Eine Konzeption entwickelt am Beispiel eines medizinischen Informationssystems, Berlin.

Waldman, Ari Ezra 2020: Privacy Law's False Promise; in: *Washington University Law Review*, Jg. 97, H. 2, S. 773–834.

Wybitul, Tim (Hrsg.) 2017: EU-Datenschutz-Grundverordnung: Handbuch, Frankfurt am Main.

Anmerkungen

1 Die Autoren danken Mareike Lisker für die Unterstützung bei der Recherche und der Endredaktion des Textes.

2 Zur Rechtsunsicherheit (und dort auch zur Unterkomplexität der DSGVO) statt vieler insbesondere Roßnagel (2018: 23 ff.).

3 Einzig die PIA-Software der französischen Datenschutzaufsichtsbehörde folgt einer offengelegten Methode (CNIL 2019).