Rezension: Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework

David Vasella *

Aurelia Tamò-Larrieux hat das vorliegende Werk, ihre Dissertation, zum Thema Privacy by Design 2018 abgeschlossen. Sie untersucht das Problem dabei sowohl von einer rechtlichen als auch einer technischen Seite und leistet damit einen willkommenen Beitrag zur interdisziplinären Betrachtung.

Zitiervorschlag: David Vasella, Rezension: Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework, in: *sui-generis* 2019, S. 235

URL: sui-generis.ch/106

DOI: https://doi.org/10.21257/sg.106

* David Vasella (david.vasella@walderwyss.com), Dr. iur., CIPP/E, Rechtsanwalt, Partner bei Walder Wyss AG, Zürich.

1 Das vorliegende, rund 250-seitige, englischsprachige Werk ist die Dissertation von Aurelia Tamò-Larrieux, die sie bis April 2018 – bis dahin wurde die Literatur berücksichtigt – am Berkman Center der Universität Harvard (bei Prof. Urs Gasser) und an der Universität Zürich (bei Prof. Florent Thouvenin) verfasst hat und die mit summa cum laude ausgezeichnet wurde. Die Autorin widmet sich darin den «Privacy by Design»- und «Privacy by Default»-Grundsätzen, und zwar nicht aus einer nur rechtlichen, sondern auch aus einer technischen Perspektive. In rechtlicher Hinsicht beschäftigt sich Tamò-Larrieux vorwiegend mit dem europäischen Recht – nicht nur, aber besonders der DSGVO – und mit US-amerikanischem Recht, so dass das Werk auch ein Beitrag zur Rechtsvergleichung ist.

2 Die Dissertation von Tamò-Larrieux ist in elf Kapitel eingeteilt, die einer klaren Logik folgen. Sie beginnt mit einer Einleitung («Setting the Stage», S. 1 ff. und «Research Approach», S. 19 ff.) und führt zunächst zu einer knappen Erläuterung des Konzepts von «Privacy» und der unterschiedlichen Regelungsziele des Datenschutzes («Mapping the Privacy Rationales», S. 27 ff.). Das vierte Kapitel («Privacy Protection in an Internet of Things Environment», S. 45 ff.) stellt den Datenschutz in den Kontext des «Internet of Things», mit besonderem Augenmerk auf RFID-Anwendungen, auf «Smart Energy Architectures» («smart grids» und «smart sensors») und auf «smart wearable devices», z.B. Fitness-Tracker. Für jeden dieser Bereiche erläutert Tamò-Larrieux Datenschutzrisiken, vorhandene rechtliche Rahmenbedingungen, anwendbare Industriestandards und technische Datenschutzlösungen («privacy-enhancing tools»).

3 Nach dieser Grundlegung geht Tamò-Larrieux im fünften Kapitel auf die rechtliche Regelung des Datenschutzes in Europa ein (S. 73 ff.), ausgehend von seinen völkerrechtlichen Grundlagen auf Ebene der Vereinten Nationen, des Europarats, der OECD und der EU.

4 Das sechste Kapitel (S. 101 ff.) betrifft technische Mittel des Datenschutzes, von Tamò-Larrieux nach Schutzzielen eingeteilt in die Kategorien Sicherheit (Security), Anonymität, Autonomie und Transparenz. Innerhalb dieser Kategorien werden in knapper Form und mit Hinweisen auf technische Standards entsprechende technische Mittel dargestellt, im Bereich Security u.a. Verschlüsselung, digitale Signaturen, Hash-Funktionen, Message Authentication Codes, biometrische Authentifizierungen, Zertifikate und Public-Key-Infrastrukturen (PKI) und Transportverschlüsselungen; im Bereich der Anonymisierung sodann Anonymisierungs- und Pseudonymisierungsverfahren, die Verwendung mehrfacher Identitäten, die «Obfuscation» von Kommunikationsinhalten und -vorgängen z.B. durch Verwendung von Proxy-Servern; im Bereich der Gewährleistung der Kontrolle («Autonomy Tools») Zugriffs- und Rechtekontrolle, die Sicherstellung der Hoheit über eigene Personendaten durch Tools wie «Personal Data Stores» (einen persönlichen Datenspeicher zur kontrollierten Freigabe von Personendaten), «Personal Information Management Systems» und Privacy Rights Management und sodann Löschtechnologien; im Bereich der Transparenz u.a. die Verwendung von Icons und

Dashboards zur Verdeutlichung von Datenbearbeitungsvorgängen, die Zertifizierung der Datenschutzkonformität, Datenschutz-Folgenabschätzungen und Datenschutzerklärungen. Dieses Kapitel gibt wertvolle Hinweise zur technischen Seite des Datenschutzes, ohne dass die einzelnen Ausführungen, wohl platzbedingt, zu sehr in die Tiefe gehen.

5 Das siebte Kapitel (S. 149 ff.), «Mapping the Privacy Protection Tools Throughout the Life Cycle of Data», greift sodann die Hinweise aus den vorangehenden Kapiteln auf. Tamò-Larrieux geht hier entlang des Lebenszyklus von Daten von der Erhebung über die Auswertung und Nutzung zur Löschung vor und stellt auf insgesamt 15 Seiten jeweils die einschlägigen rechtlichen Anforderungen (z.B. Datenminimierung und Transparenz) den verfügbaren technischen Mitteln gegenüber.

6 Das achte Kapitel heisst «Interplay of Legal and Technical Privacy Protection Tools» (S. 167 ff.). Es untersucht die rechtlichen Vorgaben an die technische Umsetzung, vor dem Hintergrund der Tatsache, dass die DSGVO über Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) zwar die technische Absicherung der Datenschutzgrundsätze verlangt, dazu aber keine konkreten Vorgaben macht. Tamò-Larrieux stellt hier zunächst die (vor allem europa-)rechtlichen Vorgaben dar, nach den im sechsten Kapitel eingeführten Kategorien Sicherheit, Anonymität, Autonomie und Transparenz. Im Anschluss daran geht sie auf die interessante Frage ein, wie sich die Herangehensweisen des Rechts und der Technik an das Problem des Datenschutzes unterscheiden, und leitet Empfehlungen für die Regulierung des Datenschutzes ab.

7 Die Erkenntnisse aus den vorangehenden beiden Kapiteln sieben und acht werden anschliessend im neunten Kapitel am Beispiel des «Internet of Things» einer konkreten Einzelfallbetrachtung zugeführt («Privacy by Design for the Internet of Things: A Startup Scenario», S. 203 ff.). Grundlage ist das Fallbeispiel eines Startups in Europa, das ein Armband zur Schlafmessung (ein «smart wearable») vertreibt. Tamò-Larrieux stellt dar – wieder entlang des Lebenszyklus Erhebung/Auswertung/Nutzung/Löschung –, mit welchen technischen und organisatorischen Massnahmen die Grundsätze von Privacy by Design und Privacy by Default umgesetzt werden können.

8 Kapitel zehn («Strenghtening Privacy by Design», S. 227 ff.) enthält sodann Hinweise an die Adresse des Gesetzgebers bzw. der Politik für die Entwicklung von Leitlinien von «Privacy by Design» über die rein technischen Aspekte hinaus, und Kapitel elf (S. 245 ff.) schliesst mit den Schlussfolgerungen von Tamò-Larrieux.

9 Das Werk von Tamò-Larrieux hat das Verdienst, sich seinem Thema nicht von einer nur rechtlichen oder nur technischen Seite zu nähern, was wohl der falsche Ansatz wäre. Es ist vielmehr ein leicht lesbarer, relativ knapp gehaltener und gut aufgebauter Beitrag zur Verständigung der Bereiche von Recht und Technologie, die gerade bei Themen wie «Privacy by Design», «Privacy by Default» und der Datensicherheit wichtig ist. Für Juristen dürfte der Nutzen des Werks vor allem darin liegen, dass sich Begriffe

technischer Natur wie Pseudonymisierung oder Anonymisierung und stark technologiebezogene Konzepte wie Datensicherheit mit Leben füllen. Wer sich bereits mit Datenschutzrecht beschäftigt hat, wird in rechtlicher Hinsicht dagegen wenig Neues finden. Es geht Tamò-Larrieux aber auch weniger darum, Neuland zu betreten, als vielmehr einen umfassenden Blick auf das Thema zu werfen, und das ist ihr gut gelungen.