Trifft die DS-GVO die Falschen?

Jörn Erbguth

Seit fast acht Monaten gilt die Datenschutzgrundverordnung. Zeit für eine Bestandsaufnahme: Wo wirkt sie und wo steht sie besseren Lösungen im Weg?

Datenschutz weckt gemischte Gefühle. Europa hat die schärfste Datenschutzgesetzgebung der Welt. Doch scheint dies der Datensammelwut von Facebook und Google bislang kaum Einhalt zu gebieten. Auch die staatliche Überwachung nimmt zu. Während die einen deshalb an der Effektivität der DS-GVO zweifeln, machen sie die anderen zum Sündenbock. So wurde das Fiasko um die Gesundheitskarte mit dem Datenschutz in Verbindung gebracht. Hier müsse „abgerüstet" werden, hieß es über Weihnachten quer durch die Presselandschaft. Dass die meisten europäischen Länder trotz DS-GVO bei der Digitalisierung im Gesundheitswesen weiter sind, schien dabei nicht zu interessieren. Möglicherweise haben diese Äußerungen auch mehr die ins Stocken geratenen Verhandlungen zur ePrivacy-Verordnung im Visier.

Sind Webseiten jetzt datenschutzfreundlicher?

Wie hat sich die DS-GVO auf die Online-Aktivitäten ausgewirkt? Anwälte haben viel Geld mit der Anpassung von Datenschutzerklärungen verdient, doch wurden Webseiten auch datenschutzfreundlicher? Ist es ein Fortschritt im Datenschutz, wenn wir immer mehr Cookie-Banner wegklicken müssen, aber die Komplettüberwachung unserer Internetaktivitäten etwa durch Google Analytics sogar noch zugenommen hat? Der Fokus scheint nach wie vor auf den eher unschuldigen Cookies zu liegen und nicht darauf, welche Informationen damit gesammelt werden – geschweige denn, was mit diesen Informationen danach gemacht wird. Für einfache Nutzungsstatistiken müssten die Daten nicht zu Webseiten-übergreifenden Profilen zusammengeführt werden. Webseitenbetreiber „bezahlen" vielmehr „kostenlose" Statistiken mit den Daten der eigenen Besucher.

Doch hier scheint Änderung in Sicht: In Frankreich schritt die Aufsichtsbehörde CNIL wegen unzureichender Einwilligungen in umfangreiches Geo-Tracking von Smartphone-Apps ein. Es müsse besser über die beabsichtigte Datennutzung aufgeklärt werden. Die übergreifende Profilerstellung von Google Analytics nur mit „Optimierung des Nutzungserlebnisses" zu begründen, dürfte damit schwieriger werden. Die CNIL ist jedoch nicht nur hier Vorreiterin. Sie ist auch die erste Aufsichtsbehörde, die konkret zum Datenschutz bei Blockchains Stellung genommen hat. Öffentliche Blockchains bieten im Prinzip die Möglichkeit, ohne datensammelnde Intermediäre wie Google, Amazon oder Facebook auszukommen. Der Zugriff auf Daten kann durch kryptographische Technologie „by design" geregelt werden.

Doch öffentliche Blockchains haben ihren Ursprung bei den Kryptoanarchisten und spielen nach ihren eigenen Regeln. Wie steht die DS-GVO zu Unveränderlichkeit, zu unklaren und verteilten Verantwortungsstrukturen und zur teilweisen Anonymität der Teilnehmenden? Die Unveränderlichkeit der Daten auf einer Blockchain kann dadurch entschärft werden, dass die eigentlichen Daten extern gespeichert werden und die Daten auf der Blockchain nur zur Verifikation dienen. Wie ein digitaler Fingerabdruck beweisen „Hashwerte" dann lediglich die Authentizität der externen Daten, geben aber keine weiteren Informationen preis. Die Artikel-29-Gruppe hatte 2014 Hashing im Kontext der Anonymisierung kritisch erörtert. Der Personenbezug sei nicht „zuverlässig" zu beseitigen. Oft übersehen wird jedoch der darauf folgende Hinweis, dass bei entsprechender Gestaltung der Verfahren ein Entfallen des Personenbezugs durchaus möglich ist.

Kritischer sind die organisatorischen Vorgaben der DS-GVO. Bei einem Peer-to-Peer-System, wie es etwa eine öffentliche Blockchain ist, sind die Teilnehmenden ggf. gleichzeitig Betroffene, Auftragsverarbeiter und Verantwortliche. Während die DS-GVO die Betroffenen schützt, belegt sie Verantwortliche und Auftragsverarbeiter mit umfangreichen Pflichten wie z.B. der Identifizierung, Vertragsgestaltung sowie Kontroll- und Auskunftspflichten. Teilnehmer einer öffentlichen Blockchain können diese nicht nur schwer erfüllen. Diese Pflichten könnten zudem ihre Datenschutzinteressen als Betroffene beeinträchtigen. Von der Bundesregierung bis zur EU-Kommission besteht daher eine große Unsicherheit. Steht die DS-GVO dezentralen Strukturen im Weg? Als Antwort sollten die Aufsichtsbehörden die Verordnung flexibel auslegen und mit klaren Best Practices einen Weg zur Realisierung eines besseren Datenschutzes mit Hilfe dezentraler Systeme vorgeben. •

Dipl.-Inf. und Dipl.-Jur. Jörn Erbguth berät zu Blockchain und Datenschutz. Er ist Vorstandsmitglied des EDV-Gerichtstags e.V.