



Daniel Muster, daniel.muster@it-rm.ch

Identitätsdiebstahl

*„Ich bin nicht ich, sondern ein je-
mand ganz anderer, der mir verblüf-
fend ähnlich ist.“
Der Doppelgänger,
F. M. Dostojewski (1821- 1881)*

Identitätsdiebstahl ist für die Betroffenen ein grosses Übel. Sei, dass ungewollt ihr Mietvertrag gekündigt oder ihr Bankkonto belastet wird. Sei, dass sie unschuldig in ein Strafverfahren involviert oder ungerechtfertigte Ansprüche an sie gestellt werden. Gemäss einer Studie¹ des U.S. Department of Justice sind bis Ende 2013 17 Mio. der in den USA Ansässigen, älter als 16 Jahre, bereits Opfer eines Identitätsdiebstahls geworden. Die Zunahme des Identitätsdiebstahls ist u.a. darauf zurückzuführen:

- Dass die digitalisierte und voll automatische Prüfung der Identität den Sicherheitsanforderungen nicht entspricht und nicht ausreichend zuverlässig ist, siehe ARD-Reportage „Pässe für Kriminelle“² betreffend Durchgangskontrolle bei Flughäfen.
- Dass biometrische Daten zwecks Prüfung der Identität unzureichend geschützt werden, siehe erwähnte ARD-Reportage betreffend Kopie der Attribute von rund 1 Mia. natürlichen Personen in Indien.
- Dass biometrische Daten dort eingesetzt werden, wo sie nichts zur Sicherheit beitragen. So z.B. bei der angedachten technischen Realisierung zur E-ID-Gesetzesvorlage (BGEID), welche im Sommer 2018 vom EJPD ans Bundesparlament überreicht wurde³.
- Dass gewissen Vorkommnissen in der IT zu viel Aussagekraft beigemessen wird. So z.B. im Bundesgesetz über die elektronische Signatur (ZertES). Gemäss Art. 2 Bst. b Ziff. 2 ZertES ermöglicht eine elektronische Signatur die Identifizierung einer Person. Eine elektronische Signatur zusammen mit dem dazugehörigen Zertifikat ver-

¹ Erika Harrell, Victims of Identity Theft, 2014

² <https://www.ardmediathek.de/tv/Reportage-Dokumentation/P%C3%A4ssef%C3%BCr-Kriminelle/Das-Erste/Video?bcastId=799280&documentId=54850588>

³ Botschaft zum BGEID, BBL 2018, 3928



Daniel Muster, daniel.muster@it-rm.ch

mag jedoch nicht, eine Person zu identifizieren; jedenfalls nicht, was sich die Allgemeinheit darunter vorstellt. Denn die Mittel zum Leisten einer elektronischen Signatur sind, im Gegensatz zur eigenen Identität, ohne nennenswerten Aufwand auf weitere Personen übertragbar. Oder aufgrund der Randdaten (Ort, Zeit, Dauer) bei einem Handy wird intuitiv angenommen, dass dessen Eigentümer an diesem Ort zu dieser Zeit damit telefoniert hat.

- Dass Begriffe verwendet werden, welche Assoziationen wecken, welche dem zugrunde liegenden Sachverhalt nicht entsprechen. Dies verleitet dazu, nicht adäquate Sicherheitsmassnahmen zu ergreifen, beispielsweise beim Schutz des Stimm- oder des Bankgeheimnisses, siehe [Muster], Kapitel II.5, „Irrtum - Identifizieren versus Authentisieren“⁴.

Daraus ergeben sich u.a. folgende Fragen:

- Macht es noch Sinn, im Umfeld der elektronischen Signatur eine in der Schadenhöhe unbeschränkte ausservertragliche Haftung aufrechtzuerhalten (Art. 59a OR, Art. 17 ZertES)?
- Wie viel Beweiskraft haben Ereignisse in der IT, wie das Leisten einer elektronischen Signatur, im Rahmen eines Strafverfahrens?
- Im Sachenrecht wird zwischen Eigentum und Besitz, im Strassenverkehrsrecht zwischen Fahrer und Halter eines Fahrzeugs differenziert. Sollte bei Erlassen zwischen Zuordnung der IT-Ereignisse einer Person und deren Identifizierung ebenso unterschieden werden?
- Sollte bei Einwand Identitätsdiebstahl ein beschleunigtes Verfahren im Zivilrecht zwecks Klärung des Sachverhalts eingeführt werden?
- Bedarf es der Bundesbestimmungen betreffend Umgang mit biometrischen Informationen?

Identitätsdiebstahl ab einem gewissen Mass kann unser Wirtschaftsleben, die Sicherheit unseres Landes und unser Verhältnis zu den Behörden beeinträchtigen und dadurch verlangsamen. Zeit, dass diese Problematik auf verschiedenen Ebenen thematisiert wird.

⁴ http://www.it-rm.ch/files/Ident-Auth_daniel_s_Muster_09_09_2018_V_1_1.pdf