Forschungsprojekt zum digitalen Identitätsdiebstahl – Research in Progress –

Susan Gonscherowski[1], Fabian Rack[2], Oliver Vettermann[2]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstraße 98, 24103 Kiel
[2] FIZ Karlsruhe, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen

Abstract. Der Beitrag befasst sich mit den rechtlichen Rahmenbedingungen der Benachrichtigung von Opfern eines Identitätsdiebstahls. Für die Entwicklung eines Frameworks auf dessen Grundlage die Betroffenen proaktiv informiert werden können, sind zunächst die Anforderungen des Datenschutzrechts, Urheberrechts und sich daraus ergebende mögliche Kollisionen verschiedener verfassungsrechtlich geschützter Güter zu klären. Basis des Frameworks ist die Auswertung öffentlich zugänglicher Ansammlungen von Daten - den Datensenken. Diese enthalten personenbezogene Daten, welche für einen Identitätsdiebstahl missbraucht werden können. Denkbar ist jedoch auch, dass dem dadurch einschlägigen Datenschutzrecht das Grundrecht auf Informationsfreiheit gegenüberzustellen und entsprechend abzuwägen ist. Dient der Betrieb einer Datensenke der Sicherung des Lebensunterhalts und wurde die Senke als Bestandteil eines Geschäftsmodells erschaffen, spielen auch die zivilrechtlichen Erwägungen eine Rolle bei der Gestaltung des Frameworks.

Keywords: Digitale Identität, Identitätsdiebstahl, Datenschutz, Datensenken, Haftung

1 Einleitung

Das vorzustellende Projekt beschäftigt sich dem Titel gemäß mit dem Umgang von Opfern des digitalen Identitätsdiebstahls und einer Information ebendieser über den Verlust der Vertraulichkeit ihrer personenbezogenen Daten. Internetnutzer verfügen über diverse Teilidentitäten [1], die für die Nutzung verschiedener Dienste angelegt werden. Die Anmeldung bei diesen Diensten erfolgt häufig mittels E-Mail-Adresse/Benutzername und Passwort. Je nach Dienst sind weitere personenbezogene Daten im Benutzerkonto hinterlegt, z.B. Konto- oder Kreditkartennummer, Adresse, Telefonnummer, Name etc. Da Nutzer häufig dieselbe Authentifikation für mehrere Dienste (Online-Shopping, E-Mail-Postfach, Soziales Netzwerk) verwenden [2], stellt die Veröffentlichung nur weniger Informationen für den Betroffenen bereits ein hohes Risiko dar.

Aber nicht nur die Nutzer selbst, auch Unternehmen legen Teilidentitäten über Nutzer an. Auskunfteien erstellen umfangreiche Profile, die der Berechnung der

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Kreditwürdigkeit eines Kunden dienen. Die hier hinterlegten Informationen, wie Sozialversicherungsnummern, werden z.T. lebenslang vergeben und können nicht geändert werden. Für Angreifer bietet sich hier ein sehr lohnendes Ziel, denn die Daten veralten nicht und können auch als Identitätsnachweis dienen. Jüngstes Beispiel für die Brisanz dieser Problematik ist der Fall Equifax.[3] 44% der US-Amerikaner sind von diesem Datenraub bei der Wirtschaftsauskunftei betroffen und müssen nun damit rechnen, dass ihre Daten in betrügerischer Absicht missbraucht werden. Das Ziel des Projektes ist, eine effektive Nachbetreuung der Opfer zu ermöglichen und zukünftige IT-Sicherheitsvorfälle besser verhindern zu können. Zu diesem Zweck soll im Rahmen rechtlicher Gegebenheiten ein Software-Framework entwickelt werden, welches die Opfer unter Beachtung psychologischer Kenntnisse bzw. Standards in angemessener Weise informiert und Mittel und Wege des Umgangs mit dem digitalen Identitätsdiebstahl aufzeigt oder gar auf letzte Sicherungsmaßnahmen hinweist.
Bei der Untersuchung und Erarbeitung dieser Ziele betreuen die Projektpartner die rechtlichen Aspekte des vorzustellenden Projektes. Insbesondere stellen sich hier schon zu Beginn rechtliche Fragen, die bislang wenig geklärt sind – so zum Beispiel, inwieweit Datensenken und digitale Identitäten nach geltendem Recht geschützt sind und ob wissenschaftliche Untersuchungen diesbezüglich rechtmäßig sind oder sich in einer rechtlichen Grauzone bewegen.

Da das Projekt sich aktuell noch in Arbeit befindet, werden im Sinne eines Research in Progress nur erste Ergebnisse in rechtlicher Hinsicht dargestellt und mögliche, daraus resultierende, Fragen dargelegt. Der Fokus des Beitrags beschränkt sich daher auf die Datensenken und deren Betreiber im rechtlichen Kontext sowie auf rechtliche Beschränkungen bei der Verwertung von Datensenken zu unterschiedlichen Zwecken.

2 Der Begriff der Datensenke

Grundlegend ist zunächst der Begriff der Datensenke. Angelehnt an die Terminologie aus der Geologie, wo eine Senke jeden Ansammlungsort von geologischen Materialien meint, ist sodann auch hier der Ansammlungsort von Daten zu verstehen, wie sie beispielsweise bei Datenendeinrichtungen (kurz DEE) auftreten. [4] Eine derartige Datensammlung ist insbesondere ein Phänomen von Big Data, zeichnet sich also gerade durch willkürliche, ungeordnete „Datenhaufen“ aus. [5] Konkret entspricht eine Datensenke daher jedem Aufzeichnungsmedium, welches die Daten bis zum tatsächlichen Verarbeitungs- oder Verwendungszeitpunkt bereithält. [6] Datensenken sind daher nicht eindimensional, sondern können selbst zu einem späteren Zeitpunkt als Datenquelle verwendet werden. Ob es sich dabei um die Ursprungsquelle handelt, ist dagegen für den Begriff irrelevant.

Kern des geplanten Frameworks sind öffentlich zugängliche Datensenken, die personenbezogene bzw. personenbeziehbare Daten, wie E-Mail-Adressen (mit zugehörigen Passwörtern oder Hashes), Kreditkartennummern, Namen usw. enthalten. Diese Senken sind beispielsweise über Paste Pages, Foren, File Hosting-

Plattformen oder Leak Announcement Pages zu erreichen. Über diese Seiten werden regelmäßig entsprechende Daten veröffentlicht oder getauscht. Theoretisch können die Daten auch käuflich erworben werden. Auf diese Möglichkeit wird jedoch aus ethischen Gründen verzichtet, da fragwürdige Geschäftsmodelle nicht bestätigt werden sollen. Datensenken, die zur Veröffentlichung bestimmte Daten enthalten, wie beispielsweise Online-Telefonbücher, werden ebenfalls nicht berücksichtigt.

3 Verfassungsrechtliche Grundlagen

Dem Verfassungsrecht kommt diesbezüglich eine gewichtige Rolle zu, bildet es doch in der Normenhierarchie die Grundlage für die grundrechtskonforme Auslegung Anwendung von einfachgesetzlichen Vorschriften wie denen des Datenschutzrechts. Zunächst ist daher zu betrachten, inwieweit den Datensenken ein originärer grundrechtlicher Schutz zukommt. Die Frage stellt sich zwar nicht auf der Grundlage, dass Datensenken verfassungsrechtliche Rechtssubjekte sein könnten, da letztere nur natürliche Personen und juristische Personen des Privatrechts im Sinne des Art. 19 III GG sind. Ist die Datensenke allerdings einem oder mehreren Grundrechten zuzuordnen, so könnte derartigen Infrastrukturen im Rahmen von Schutzpflichten ein besonderer Schutz zukommen, welcher vom Gesetzgeber einzurichten ist. Kommt der Gesetzgeber diesem nicht nach, kann sich in Ausnahmefällen auch unmittelbar auf das Verfassungsrecht gestützt werden. [7] Im Rahmen der bisherigen Untersuchung ergab sich eine Zuordnung der Datensenke zur Rundfunk- und Pressefreiheit des Art. 5 I 2 GG, zur aus Art. 13 I GG folgenden Unverletzlichkeit der Geschäftsräume sowie dem IT-Grundrecht als Teilaspekt des allgemeinen Persönlichkeitsrechts gem. Art. 2 I i.V.m. 1 I GG.

Dem Schutz der Rundfunk- und Pressefreiheit aus Art. 5 I 2 GG ist die Datensenke insoweit zuzuordnen, als sie die Aussendung von Informationen an die Allgemeinheit enthält. [8] Die Schutzdimension der Datensenke erschöpft sich also in dem Informationsweg, also seiner Gewährleistung von der erstmaligen Entstehung bis zur Veröffentlichung, und weiteren Verwendung, einschließlich der Betriebs- und Geschäftsräume hinsichtlich des Redaktionsgeheimnisses. [9] Weiterhin erfasst Art. 5 I 2 GG auch den Informantenschutz [10], auf Ebene des Datenschutzes folglich den Status des Whistleblowers. Die Datensenke als Informationsmedium ist daher als (vorübergehender) Träger von Informationen, welche der Allgemeinheit zugänglich gemacht werden sollen, geschützt. Kaum anwendbar erscheinen hingegen die jeweiligen objektiv-rechtlichen Gewährleistungen, wie z.B. das Institut der freien Presse [11] oder die Programmfreiheit des Rundfunkanbieters [12].

Hinsichtlich der Privatheit der Kommunikation innerhalb der Geschäftsräume einschließlich der darin enthaltenen Speichermedien, welche letztlich die Datensenke in physischer Form darstellen, kann auch auf Art. 13 I GG zurückgegriffen werden. Schließlich ist der Schutz derartiger Räumlichkeiten, welche der Allgemeinheit nicht zugänglich sind, durch das Bundesverfassungsgericht anerkannt. [13] Sofern Eingriffe

im Sinne des Art. 13 II-V, VII GG drohen, ist Art. 13 I GG das gegenüber Art. 5 I 2 GG speziellere Grundrecht. [14]

Die Privatheit der Daten selbst und dahingehenden Restriktionen kraft verfassungsrechtlichem Datenschutz entspringen dagegen dem allgemeinen Persönlichkeitsrecht des Art. 2 I i.V.m. 1 I GG, insbes. dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Verwendet der Betreiber zur Absicherung seiner Daten bzw. Systeme entsprechende technische Mittel, z.B. eine Firewall oder andere Cybersecurity-Mittel, entspringt dem eine Indizwirkung: Hinter dem digitalen Schutzwall befinden sich Daten und Systeme, die es zu schützen gilt und dass in den Schutz und die Sicherheit vertraut wird. Gerade dieses Vertrauen in die Informationstechnik schützt die genannte Ausprägung des allgemeinen Persönlichkeitsrechts. [15] Der Gesetzgeber hat diesbezüglich einen weiten Gestaltungsspielraum, begrenzt durch Persönlichkeitsrechte Dritter bzw. den bestehenden Datenschutz. Werden Sicherheitslücken durch staatliche Maßnahmen aufrechterhalten, bestünde darin eine Grundrechtsverletzung.

Der Betreiber kann sich demgemäß auf das IT-Grundrecht aus Art. 2 I i.V.m. 1 I GG und andere dargestellte Grundrechte stützen. Nicht zu vergessen ist weiter, dass in Sonderkonstellationen auch den Betreiber verfassungsrechtliche Schutzpflichten treffen können. Grundsätzlich sind Grundrechte ausschließlich als Abwehrrechte gegen den Staat, die konkrete Ausgestaltung in Privatrechtsverhältnissen als Sache des Gesetzgebers zu verstehen. [16] „Je nach Gewährleistungsinhalt und Fallgestaltung kann die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates vielmehr nahe oder auch gleich kommen.“ [17] Im vorliegenden Falle bedeutet dies, dass – sollte sich die Gewährleistung eines Schutzes digitaler Identitäten und diesbezüglicher Datensenken aus einer verfassungsrechtlichen Schutzpflicht ableiten – auch private Unternehmen, welche den Schutz und damit staatliche Aufgaben übernehmen, unmittelbar grundrechtsgebunden sind. Dies kommt allerdings auf den Einzelfall der Ausgestaltung an.

Die erläuterten Aspekte führen allerdings zu neuen Teilfragen. So könnte zwar aus dem IT-Grundrecht für Datensenken-Betreiber folgen, dass sie zum Eigenschutz die Information ihrer Nutzer übernehmen – sofern es sich nicht um eine staatliche Aufgabe handelt. Letzteren Aspekt, also die mögliche Verpflichtung des Staates kraft Schutzpflicht, gilt es vertieft zu untersuchen. Des Weiteren ist das Verhältnis zwischen möglichen Hinweisgebern und der warnenden/informierenden Institution zu klären.

4 Datenschutzrechtliche Schutzaspekte

Auch wenn der Betrieb einer Datensenke durch das Grundgesetz geschützt ist, so ergeben sich aus den enthaltenen Daten möglicherweise Kollisionen mit anderen Schutzgütern des Grundgesetzes, bspw. mit dem Recht auf informationelle Selbstbestimmung, sofern personenbezogene Daten enthalten sind. In diesen Fällen wird eine Abwägung zwischen den Rechten des Datensenkenbetreibers und den Rechten der Betroffenen erfolgen müssen. Die Risiken für die Rechte und Freiheiten der Betroffenen sind den Interessen des Datensenkenbetreibers gegenüberzustellen. [18] In erster Linie ist der Zweck der Datensenke und damit der Datenverarbeitung zu betrachten. [19] In diesem Zusammenhang ist auch die Rechtmäßigkeit der Datenverarbeitung zu prüfen. Der Betrieb einer öffentlich zugänglichen Datensenke, die personenbezogene Daten enthält, ist nur unter bestimmten Bedingungen möglich. Entweder haben die Betroffenen in die Veröffentlichung eingewilligt (Art. 6 I a DSGVO) oder es gibt eine Rechtsvorschrift, die den Betreiber dazu berechtigt, z.B. eine Verpflichtung zur Veröffentlichung (Art. 6 I c DSGVO) oder ein berechtigtes Interesse des Verantwortlichen oder eines Dritten, gemäß Art. 6 I f DSGVO. [20]

Im Internet finden sich jedoch häufig Datensenken, die diese Anforderungen nicht erfüllen. [21] Derartige Datensenken stellen aufgrund ihrer öffentlich gemachten Inhalte stets eine Verletzung des Datenschutzrechts dar. Art, Umfang, Umstände und Zwecke der Verarbeitung führen zu einem hohen Risiko eines möglichen Missbrauchs, z.B. eines Identitätsdiebstahls. Da die Betroffenen in der Regel nicht über die Veröffentlichung ihrer personenbezogenen Daten informiert sind, werden sie sich des Missbrauchs erst bewusst, wenn sich dieser in Form von beispielsweise Mahnungen oder negativen Kredit-Scorings bemerkbar macht. Bis zu diesem Zeitpunkt können jedoch Jahre vergehen. [22] Die strafrechtliche Verfolgung wird durch diese z.T. sehr langen Zeiträume zwischen Datendiebstahl bzw. Missbrauch und Kenntnis des Betroffenen erschwert oder gar verhindert. Bisher gibt es nur wenige Angebote, die eine Möglichkeit bieten, entsprechende Senken zu durchsuchen und präventiv gegen einen Datenmissbrauch vorzugehen. Zudem verlangt dieses Vorgehen von den Betroffenen ein hohes Maß an Eigeninitiative. [23]

Im Rahmen des Projektes soll ein System entwickelt werden, das öffentliche Datensenken analysiert und die Ergebnisse so auswertet, dass bei einem hohen Risiko die Betroffenen proaktiv benachrichtigt werden. Ein entsprechendes Framework muss jedoch konzeptionell den Ansprüchen des Datenschutzrechts genügen. Für die Operationalisierung der gesetzlichen Vorgaben in konkrete Maßnahmen wird auf das Standard-Datenschutzmodell zurückgegriffen. [24] Dessen Schutzziel-Systematik erlaubt eine umfassende Analyse der durch die Datenverarbeitung bestehenden Risiken. Darüber hinaus sind für jedes Schutzziel bereits generische Maßnahmen formuliert, die weitere Eingriffe durch das Framework in die informationelle Selbstbestimmung der Betroffenen eliminieren oder wenigstens abmildern sollen. Da sich beispielsweise das hohe Risiko für die Rechte und Freiheiten natürlicher

Personen auf die Datenverarbeitung durch das Framework vererbt, ist wahrscheinlich eine Datenschutz-Folgenabschätzung gemäß Art. 35 I DSGVO vorzunehmen. Ziel ist es, den Betroffenen frühzeitig Interventionsmöglichkeiten zu geben Handlungsoptionen aufzuzeigen. Auf diese Weise können sie frühzeitig Gegenmaßnahmen einleiten und auch die straf- und zivilrechtliche Verfolgung würde erheblich vereinfacht.

5 Zivilrechtliche Anforderungen, Haftung der Akteure

Auch das Zivilrecht adressiert einige Fragestellungen an den Umgang mit Datensenken. Flankierend zum datenschutzrechtlichen Umgang mit Identitätsdaten stellt sich die Frage, inwieweit Identitätsdatensammlungen auch immaterialgüterrechtlich geschützt sind. Insbesondere ist hier an das komplexe und kleinteilige Datenbankschutzrecht sui generis zu denken, welches Datenbanken unter Investitionsschutz stellt und Entnahmehandlungen weitgehend verbietet. Die Frage ist deshalb wichtig, weil der Umgang mit Identitätsdatensammlungen in den meisten Fällen Kopien derselben erfordert und diese Kopien unter einem Lizenzvorbehalt stehen könnten. Gerade Akteuren, die Identitätsdatensammlungen untersuchen, ist hier an Rechtssicherheit gelegen. Dasselbe kann angenommen werden für Anbieter von Leak-Checkern, bei denen sich Betroffene aktiv informieren können, ob sie Opfer von Breaches geworden sind. Insgesamt sei als Tendenz vorgegriffen, dass der Datenbankschutz bei Identitätsdatensammlungen nur im Ausnahmefall greift. Sollten Sammlungen dennoch geschützt sein, wird untersucht, ob die genannten Akteure Schranken zu Gunsten der Wissenschaft oder der öffentlichen Sicherheit für sich in Anspruch nehmen können.

Ein weiterer Punkt ist die zivilrechtliche Haftung von Betreibern von Datensenken für das Vorhalten von Datensammlungen: Haften sie selbst auf Unterlassung und auf Auskunft; müssen sie Schadensersatz leisten? Hier sind medienrechtliche Haftungsmaßstäbe einzubeziehen.

6 Fazit

Die Information von Betroffenen eines Identitätsdiebstahls ist nicht nur unter datenschutzrechtlichen Gesichtspunkten zu betrachten. Andere grundrechtlich geschützte Schutzgüter sind in die Entwicklung eines entsprechenden Benachrichtigungssystems ebenso einzubeziehen, wie mögliche zivilrechtliche Haftungsrisiken, die sich aus der Auswertung von Datensenken ergeben können.

Verweise

1. Pfitzmann, Andreas/ Hansen, Marit: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity,

and Identity Management. Über: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (Aufgerufen am 27.11.2017).

2. Siehe Hasso-Plattner-Institut zur Mehrfachnutzung von Passwörtern, über: https://hpi.de/news/jahrgaenge/2016/sicherheitsrisiko-passwort-hpi-studie-zur-mehrfachnutzung-von-passwoertern.html (Aufgerufen am 27.11.2017).
3. Sokolov, Daniel: Hacker-Jackpot – Credit Bureau Equifax gehackt. Über: https://www.heise.de/newsticker/meldung/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt-3824607.html (Zuletzt besucht am 14.11.2017).
4. Zum Begriff der Datenendeinrichtung siehe auch https://web.archive.org/web/20070928000507/http://www.tfh-berlin.de/~siegel/hypermed/netzd/netzd.htm (Aufgerufen am 28.09.2017).
5. So zumindest Hoeren, Thomas: Thesen zum Verhältnis von Big Data und Datenqualität. In: MMR 2016, 8 (8).
6. Microsoft Press - Computer Lexikon, 7. Auflage 2003, Begriff: Datensenke.
7. Klein, Eckart: Grundrechtliche Schutzpflicht des Staates. In: NJW 1989, 1633 (1636).
8. Zum Merkmal Schemmer in: Epping/Hillgruber (Hrsg.), BeckOK GG (Stand: 01.06.2017), Art. 5, Rn. 66 sowie 43; Kühling in: Gersdorf/Paal (Hrsg.) BeckOK InfoMedienR, Art. 5, Rn. 74.
9. Schemmer in: BeckOK GG, Art. 5, Rn. 44.
10. BVerfGE 107, 292 (329 f); 117, 244 (258 f).
11. Hierzu BVerfGE 20, 162 (175); 66, 116 (133).
12. Hierzu Schemmer in: BeckOK GG, Art. 5, Rn. 70 f.
13. Vgl. nur BVerfGE 120 274 (309).
14. Kloepfer, Michael: Verfassungsrecht, Band II, München 2010, § 66, Rn. 11.
15. Vgl. Gersdorf in: BeckOK InfoMedienR, Art. 2, Rn. 28, 29.
16. Zum Charakter der Grundrechte siehe BVerfGE 7, 198 (205).
17. BVerfGE 128, 226 (249).
18. Frenzel in: Paal/Pauly Datenschutz-Grundverordnung, Art. 6 Rn. 30 (BeckOK).
19. Frenzel in: Paal/Pauly Datenschutz-Grundverordnung, Art. 6, Rn. 27 (BeckOK).
20. Albrecht/ Jotzo: Das neue Datenschutzrecht der EU, Baden-Baden 2017, S. 52.
21. Vgl. hierzu exemplarisch für wiederkehrende Datenpannen Eikenberg, Ronald: Hetzner gehackt, Kundendaten kopiert. Über: https://www.heise.de/security/meldung/Hetzner-gehackt-Kundendaten-kopiert-1884180.html (Abgerufen am 28.09.2017)
22. Vgl. Schulzki-Haddouti, Christiane: Bayern: Gemeldete Datenpannen nehmen massiv zu über: https://www.heise.de/newsticker/meldung/Bayern-Gemeldete-Datenpannen-nehmen-massiv-zu-3643086.html (Abgerufen am 06.09.17).
23. Vgl. hierzu den Sicherheitstest des Bundesamtes für Sicherheit in der Informationstechnologie (https://www.sicherheitstest.bsi.de/) oder das Online-Angebot des Hasso-Plattner-Instituts (https://sec.hpi.de/leak-checker/search).
24. Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele V.1.0 – Erprobungsfassung von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern), Über: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V_1_1.pdf (Abgerufen am 14.11.2017).