EMPIRISCHE FORSCHUNG IM TECHNISCHEN DATENSCHUTZ: EIN JURISTISCHES PROBLEM?

Christoph Sorge

Juniorprofessor, Universität Paderborn, Institut für Informatik
Warburger Straße 100, 33098 Paderborn, DE
christoph.sorge@uni-paderborn.de; http://www.cs.uni-paderborn.de/?netsec

Schlagworte: ***Privacy Enhancing Technologies, technischer Datenschutz, De-Anonymisierung***

Abstract*:* *Die Erforschung technischer Datenschutzmaßnahmen, beispielsweise der Anonymisierung von Daten, kann wesentlich dazu beitragen, das Informationelle Selbstbestimmungsrecht der Nutzer von IT-Systemen zu stärken. Um aber Problemfelder zu identifizieren oder die Effektivität getroffener Maßnahmen zu untersuchen, untersuchen Forscher oft auch das Potential der De-Anonymisierung von anonymen oder für anonym gehaltenen Datensätzen. Der vorliegende Beitrag betrachtet die Rechtmäßigkeit dieser De-Anonymisierung auf Grundlage des deutschen Datenschutzrechts.*

1. Einleitung

In der IT-Sicherheitsforschung wird neben dem Entwurf von Protokollen und Sicherheitsarchitekturen sowie deren analytischer Validierung auch oft empirisch gearbeitet; so wird z.B. untersucht, wie häufig bestimmte Schwachstellen in der Praxis auftreten und welche Verbreitung Sicherheitsverfahren gefunden haben.

Ein spezielles Gebiet in der IT-Sicherheitsforschung ist der Datenschutz durch Technik (Privacy Enhancing Technologies). Technische Maßnahmen sollen Nutzern helfen, ihr Informationelles Selbstbestimmungsrecht auszuüben, indem beispielsweise Transparenz über die Übermittlung personenbezogener Daten hergestellt oder im Idealfall das Entstehen solcher Daten ganz verhindert wird. Im letztgenannten Fall sollten ausschließlich anonyme bzw. anonymisierte Daten vorliegen.

Es reicht aber nicht aus, lediglich technische Maßnahmen zu entwickeln. Wichtig ist auch, ihre Wirksamkeit zu überprüfen sowie im Vorfeld mögliche Problemfelder zu identifizieren. Das bedeutet, dass überprüft werden muss, ob zu bestimmten Daten ein Personenbezug hergestellt werden kann oder nicht. In einigen Fällen kann diese Überprüfung abstrakt vorgenommen werden, doch oft hängt die Möglichkeit zur Herstellung des Personenbezugs von schwer kontrollierbaren Einflussfaktoren ab. Dann ist die Durchführung empirischer Untersuchungen nicht zu umgehen, um das Erkenntnisinteresse zu befriedigen.

Im Folgenden soll zunächst diskutiert werden, wann eine De-Anonymisierung vorliegt; sodann werden Beispiele dargestellt, in denen Forscher eine solche tatsächlich durchgeführt haben. Es folgt ein Überblick über Rechtsfragen, die sich daraus ergeben. Ausgangspunkt der Betrachtung ist das deutsche Bundesdatenschutzgesetz.

2. De-Anonymisierung

§ 3 Abs. 6 BDSG definiert Anonymisieren als „Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." Nach der herrschenden Meinung[1] sind anonymisierte Daten nicht mehr personenbezogen, obwohl der Aufwand der Zuordnung von Daten zu einer natürlichen Person in der eigentlichen Definition des § 3 Abs. 1 BDSG nicht erwähnt wird. Im Zusammenhang mit einem relativen Begriff des Personenbezugs bedeutet dies, dass die Anonymität von Daten davon abhängt, ob der Aufwand zur Herstellung des Personenbezugs *für die jeweilige verantwortliche Stelle* unverhältnismäßig ist. So kann es vorkommen, dass anonymisierte Daten an eine andere Stelle weitergegeben werden, für die sie personenbezogen sind; in diesem Fall liegt eine Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG vor[2]. Die Veröffentlichung von personenbezogenen Daten wird in Literatur[3] und Rechtsprechung[4] ebenfalls als Übermittlung angesehen. In diesem Fall muss darauf abgestellt werden, ob *irgendein* potentieller Empfänger der Daten diese mit einem nicht unverhältnismäßig großen Aufwand einer Person zuordnen kann.

Gelingt Forschern das Herstellen eines Personenbezugs bisher für anonym gehaltener Daten, sind zwei Varianten denkbar: einerseits, dass Daten für eine verantwortliche Stelle anonymisiert sind, die Forscher aber einen Personenbezug herstellen können; andererseits kann der bereits vorliegende Personenbezug auch schlicht verkannt worden sein. In beiden Fällen sind (falls die De-Anonymisierung gelingt) aber bereits die Ausgangsdaten *für die Forscher* nicht anonym – sie sind ja gewillt, den Aufwand einer „De-Anonymisierung" zu betreiben, und schätzen diesen also nicht als unverhältnismäßig ein. Der Begriff der „De-Anonymisierung" führt also eigentlich in die Irre, ist aber andererseits gängig und wird daher im Folgenden beibehalten.

3. Beispiele

Aufsehen erregt hat eine Veröffentlichung von Sweeney[5], der als Beispiel eine Datenbank mit medizinischen Daten betrachtet, die von der Group Insurance Commission in Massachusetts als anonym betrachtet und daher Forschung und Industrie zur Verfügung gestellt wurde. Sie enthielt allerdings Geburtsdatum, Postleitzahl und Geschlecht der Patienten – eine Kombination, die ausreicht, um viele enthaltene Personen mit hoher Wahrscheinlichkeit eindeutig identifizieren zu können. Mit Hilfe eines öffentlich verfügbaren Verzeichnisses registrierter Wähler gelang es Sweeney, den Gouverneur des Staates in der Datenbank zu identifizieren. Da die grundlegende Methodik bereits aus früheren Veröffentlichungen bekannt und auch nicht gerade fernliegend war, ist davon auszugehen, dass bereits bei der Group Insurance Commission keine anonymisierte Datenbank vorlag.

Anders stellt sich die Sachlage im zweiten Beispiel dar: Der DVD-Verleihdienst Netflix schrieb 2006 einen Wettbewerb zur Verbesserung von automatischen Filmempfehlungen aus. Dazu wurden ca. 100 Millionen Filmbewertungen von ca. 480.000 Nutzern, jeweils mit Datum der Bewertungsabgabe, veröffentlicht. Auch diese Datenbank wurde für anonym gehalten, doch zeigten

---

1 *Dammann* in Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage 2011, §3 Rn. 196; *Gola/Schomerus*, Bundesdatenschutzgesetz, 11. Auflage 2012, § 3 Rn. 44

2 *Gola/Schomerus*, §3 Rn. 44a

3 *Gola/Schomerus*, §3 Rn. 33; *Dammann*, BDSG, §3 Rn. 157

4 BVerfG NVwZ 1990, Seite 1162 (Beschluss vom 24.07.1990 - 1 BvR 1244/87).

5 Sweeney, L., k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002, Seiten 557-570

Narayanan und Shmatikov[6], dass bei 40% der Nutzer bereits die Kenntnis von zwei Bewertungen und des ungefähren (auf 14 Tage genau bekannten) Bewertungsdatums zur Identifikation ausreicht. Ob die ursprüngliche Datenbank hier als anonymisiert bezeichnet werden kann, lässt sich nicht eindeutig beantworten. Einerseits entwickelten Narayanan und Shmatikov einen neuen Algorithmus, um Personen in der Datenbank identifizieren zu können. Andererseits hätten auch einfachere, zum Zeitpunkt der Veröffentlichung der Datenbank bereits bekannte Verfahren vermutlich ausgereicht, um wenigstens einen Teil der Personen mit recht geringem Aufwand zu identifizieren.

In zahlreichen weiteren Fällen könnte der Versuch einer De-Anonymisierung von Datensätzen zur Beantwortung offener Fragen beitragen. Beispielhaft sei die Analyse von Webserver-Logfiles genannt; gelänge es, einem nennenswerten Anteil enthaltener IP-Adressen Personen zuzuordnen, könnte dies auch Einfluss auf die juristische Diskussion über den datenschutzrechtlichen Umgang mit IP-Adressen haben.

4. Juristische Problematik

Für den Forscher, der Daten de-anonymisieren möchte, stellt sich zunächst die Frage nach der Einordnung seines Tuns, die hier aus Sicht des BDSG beantwortet wird. In der Regel sind bereits die Ausgangsdaten für den Forscher nicht anonym, da andernfalls der die Herstellung des Personenbezugs auch für ihn nur mit „unverhältnismäßig großem Aufwand“ möglich wäre. Daher ist bereits das Beschaffen dieser Daten als Erheben (§3 Abs. 3 BDSG) einzuordnen. Die tatsächliche Verknüpfung mit Identitäten könnte eine Veränderung darstellen; das Verändern ist in §3 Abs. 4 Satz 2 Nr. 2 als „das inhaltliche Umgestalten gespeicherter personenbezogener Daten“ definiert. Rein technische Vorgänge wie das Umcodieren von Daten sind hierbei ausgenommen. Das Verknüpfen von Daten aus verschiedenen Quellen wird in der Literatur aber bereits als Verändern gesehen[7]. Dies ist auch gerechtfertigt, weil die Daten eine andere Aussagekraft gewinnen – unabhängig davon, ob dies auch anderen Nutzern der Daten möglich gewesen wäre. Mit dem Verändern liegt auch ein Verarbeiten der Daten vor (§3 Abs. 4 Satz 1 BDSG).

Die Zulässigkeit der Erhebung richtet sich für öffentliche Stellen des Bundes nach § 13 Abs. 1 BDSG: „Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.“ Zwar ist der Datenschutz-Forscher nicht an den Sachverhalten interessiert, die in den Daten enthalten sind; dennoch ist die Kenntnis von personenbezogenen Daten unter Umständen erforderlich, gerade um die Sicherheit von Anonymisierungs-Verfahren zu erforschen. Unter der gleichen Voraussetzung ist nach § 14 Abs. 1 BDSG auch eine Verarbeitung der Daten zulässig. Es ist jedoch zu beachten, dass in der Erhebung und Verarbeitung auch ein Grundrechtseingriff liegt; wiegt dieser schwer, so reichen die aufgeführten, sehr allgemeinen Erlaubnisnormen nicht für seine Rechtfertigung aus[8]. Daher ist zunächst eine Abwägung zwischen den Erfordernissen der Forschung und dem Informationellen Selbstbestimmungsrecht des Einzelnen vorzunehmen, auf die später zurückgekommen werden soll.

Für besondere Arten personenbezogener Daten findet sich jedoch eine ausdrückliche Regelung: Nach §13 Abs. 2 Nr. 8 ist das Erheben besonderer Arten personenbezogener Daten durch öffentliche Stellen (nur) zulässig, wenn „dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das

6 *Narayanan, A.; Shmatikov, V.*, Robust De-anonymization of Large Sparse Datasets, IEEE Symposium on Security and Privacy 2008, Seiten 111-125

7 *Gola/Schomerus*, §3 Rn. 30; *Ambs* (in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 191. Ergänzungslieferung 2012, §3 BDSG Rn. 22) erwähnt das „Hinzufügen“ neuer Daten und plädiert für eine weite Auslegung des Begriffs „Verändern“.

8 *Gola/Schomerus*, §13 Rn. 2.

Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann“; fast wortgleich findet sich diese Regelung für die Zweckänderung beim Speichern oder Nutzen personenbezogener Daten in § 14 Abs. 2 Nr. 9 (sowie Abs. 5 Nr. 2 für besondere Arten personenbezogener Daten).

Auch nicht-öffentlichen Stellen ist die Nutzung oder Übermittlung personenbezogener Daten unter dieser Voraussetzung erlaubt (§28 Abs. 2 Nr. 3 BBDSG), wobei hier zusätzlich vorausgesetzt wird, dass die Forschung „im Interesse einer Forschungseinrichtung“ liegen muss. Die Weitergabe unzureichend anonymisierter Daten an Forscher kann daher durchaus auch dann rechtmäßig erfolgen, wenn die unzureichende Anonymisierung erkannt wird. Das „Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten für eigene Geschäftszwecke“ ist nicht-öffentlichen Stellen unter den gleichen Voraussetzungen erlaubt wie öffentlichen Stellen (§ 28 Abs. 6 Nr. 4 BDSG).

In Landesdatenschutzgesetzen finden sich auch weitergehende Regelungen, die nicht nur besondere Arten personenbezogener Daten betreffen. Beispielhaft sei hier §28 DSG-NRW genannt, der die Datenverarbeitung für wissenschaftliche Zwecke regelt. Im Fall der De-Anonymisierung kann die Soll-Bestimmung des Absatzes 1, mit anonymisierten oder pseudonymisierten Daten zu arbeiten, in der Regel nicht eingehalten werden[9]. Für diesen Fall regelt Absatz 2, dass die Verarbeitung zulässig ist, wenn die betroffene Person eingewilligt hat, wenn „schutzwürdige Belange der betroffenen Person […] nicht beeinträchtigt werden“ oder wenn „der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßig großem Aufwand erreicht werden kann und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen Person überwiegt.“ Wiederum ist also eine Abwägung gefordert, auf die wir später zurückkommen werden. § 28 LDSG-NRW enthält außerdem Regelungen über die nachträgliche Anonymisierung bzw. Pseudonymisierung sowie die Veröffentlichung der Daten.

Keine der gesetzlichen Regelungen zur Verarbeitung personenbezogener Daten für Forschungszwecke bezieht sich explizit auf den Fall der De-Anonymisierung oder die Erforschung von technischen Datenschutzmaßnahmen; auch in der Literatur wird bisher, soweit ersichtlich, nur Forschung betrachtet, die an den (z.B. medizinischen) personenbezogenen Daten selbst interessiert ist statt an Methoden der De-Anonymisierung. Weder der Wortlaut noch der Zweck der Normen geben jedoch Anlass, eine Anwendbarkeit auf die Datenschutzforschung abzulehnen.

5. Spezialfall Telekommunikations- und Telemediengesetz?

Weder das Telekommunikationsgesetz noch das Telemediengesetz enthalten Regelungen über die Verwendung von personenbezogenen Daten für Forschungszwecke (mit Ausnahme der Marktforschung). Beide Gesetze enthalten Verpflichtungen für den jeweiligen Diensteanbieter[10], die über die Vorschriften des BDSG hinausgehen. §§14,15 TMG beziehen sich aber lediglich auf personenbezogene Daten; auch für §96 TKG wird die Auffassung vertreten, dass eine Anonymisierung von Verkehrsdaten an Stelle der vorgeschriebenen Löschung treten kann[11]. Somit kann auch hier der Fall auftreten, dass Daten für anonym gehalten und daher an Forscher

9 Pseudonymisierung ist zwar denkbar, doch ist eine Pseudonymisierung durch die Forscher nur unter Aufsicht durch die übermittelnde Stelle zulässig – bei den in der Praxis oftmals auftretenden öffentlichen Daten oder im Ausland befindlichen übermittelnden Stellen ist dies aber kein gangbarer Weg.

10 Statt des Diensteanbieter-Begriffs nennt §91 Abs. 1 Satz 1 TKG als Verpflichtete „Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, […], erbringen oder an deren Erbringung mitwirken“.

11 So *Robert* in: Beck’scher TKG-Kommentar, 3. Auflage 2006, § 96 Rn. 12; trotz zwischenzeitlicher Änderungen des §96 hat sich an der Löschverpflichtung nichts geändert.

weitergegeben werden. In der Praxis sind Telekommunikationsunternehmen hier sehr zurückhaltend, so dass der Fall der unzureichenden Anonymisierung von Nutzungsdaten bei Telemedien praxisrelevanter erscheint. In § 12 Abs. 1 TMG ist bezüglich der Verwendung personenbezogener Daten ein Verbot mit Erlaubnisvorbehalt normiert; mangels einschlägiger Erlaubnisnormen, die sich konkret auf Telemedien beziehen müssten, ist eine Übermittlung solcher Daten an Forschungseinrichtungen zunächst ausgeschlossen. Das TMG erlaubt allerdings ausdrücklich auch elektronische Einwilligungen (§13 Abs. 2), die ggf. einen Ausweg aus der Problematik bieten.

6. Interessenabwägung

Wie sich gezeigt hat, erfordern die in Frage kommenden Erlaubnisnormen eine Abwägung zwischen dem Informationellen Selbstbestimmungsrecht der Betroffenen und dem Forschungsinteresse (das ebenfalls durch ein Grundrecht geschützt ist, konkret durch die Forschungsfreiheit aus Art. 5 Abs. 3 GG). §28 Abs. 2 DSG-NRW kann auch für Fälle, in denen allgemeinere Erlaubnisnormen Anwendung finden, als Blaupause für die Durchführung dieser Abwägung dienen[12].

So könnte es zunächst sein, dass „schutzwürdige Belange der betroffenen Person wegen der Art der Daten oder der Art der Verwendung nicht beeinträchtigt werden“ (so § 28 Abs. 2 Nr. 2 DSG-NRW). Werden, wie in den dargestellten Beispielen, Datenbanken de-anonymisiert, die Daten über eine Vielzahl betroffener Personen enthalten, ist es aber schwierig, dies für alle Personen zu gewährleisten. So ist es zumindest denkbar, dass bewertete Tendenzfilme, Kriegs- oder Horrorfilme dem Bild widersprechen, das eine Person von sich in der Öffentlichkeit zeichnen will. Andererseits ließe sich zumindest bei öffentlich zugänglichen Daten argumentieren, die De-Anonymisierung verletze deshalb keine schutzwürdigen Belange der betroffenen Personen, weil prinzipiell auch beliebige Dritte die De-Anonymisierung durchführen könnten; für die betroffenen Personen könnte eine De-Anonymisierung durch Forscher, die damit auf Missstände aufmerksam machen, insofern sogar vorteilhaft sein. Das Argument verfängt aber nicht, denn das Datenschutzrecht betrachtet die Rechtmäßigkeit einer einzelnen Verarbeitung, ohne auf potentiell rechtswidriges Handeln Dritter Rücksicht zu nehmen.

§ 28 Abs. 2 Nr. 3 DSG-NRW erlaubt die Verarbeitung personenbezogener Daten aber auch dann, wenn „der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßig großem Aufwand erreicht werden kann und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen Person überwiegt“[13].

Dass der *Zweck der Forschung* nicht auf andere Weise erreicht werden kann, erscheint zunächst zweifelhaft – immerhin wäre es möglich, synthetische Testdaten zu erzeugen, anhand derer beispielsweise Verfahren für die De-Anonymisierung überprüft werden können. Dieser Ansatz greift jedoch zu kurz, da die Möglichkeiten zur De-Anonymisierung von Eigenschaften der Daten abhängen. Hätten beispielsweise im Filmbewertungsdatensatz alle Nutzer die gleichen Filme (und dies innerhalb eines kurzen Zeitraums) bewertet, wäre eine De-Anonymisierung nicht möglich gewesen. Ähnliches gilt für die Verfügbarkeit von externen Referenzdaten – so wurden Datensätze

[12] Eine ausführliche Darstellung der Abwägung zwischen Forschungsinteresse und Interessen der Betroffenen findet sich, wenn auch ohne Bezug zur De-Anonymisierung, auch bei *Dammann*, BDSG, §14 Rn.88ff.

[13] Es sei darauf hingewiesen, dass das BDSG in einigen Fällen, beispielsweise bei der Erhebung besonderer Arten personenbezogener Daten durch öffentliche Stellen, ein erhebliches Überwiegen des „wissenschaftlichen Interesses an der Durchführung des Forschungsvorhabens“ fordert. Bei Anwendbarkeit dieser Regelungen ist also das Informationelle Selbstbestimmungsrecht der Betroffenen stärker zu gewichten.

aus der Netflix-Filmbewertungsdatenbank mit solchen der Website IMDB[14] abgeglichen, was gleichfalls mit generierten Testdaten nicht möglich gewesen wäre. Fraglich wäre aus diesem Gesichtspunkt allenfalls die De-Anonymisierung von Datenbanken, die sehr ähnlich zu anderen, bereits untersuchten Datenbanken sind – ein solches Vorgehen wäre aber auch für die Forschung nicht von Interesse.

Das *öffentliche Interesse an der Durchführung der Forschung* ist schwieriger zu bewerten. Da mittlerweile bekannt ist, dass von Laien für anonym gehaltene Daten oft nicht wirklich anonym sind, bedarf der Mehrwert weiterer De-Anonymisierungen stets einer Rechtfertigung. Der Wunsch, möglichst spektakuläre Ergebnisse zu erzielen, mag nachvollziehbar sein, begründet aber noch kein öffentliches Interesse. Doch sind Möglichkeiten und Auswirkungen der De-Anonymisierung anwendungsabhängig; dies zeigt sich auch an dem großen Interesse, das beispielsweise der Veröffentlichung von Narayanan und Shmatikov bezüglich der De-Anonymisierung des Netflix-Datensatzes entgegengebracht wurde, obwohl die Identifikation von Personen in für anonym gehaltenen Datensätzen in anderen Gebieten schon viel früher gelungen war.

Die Erforschung von Verfahren zur De-Anonymisierung kann darüber hinaus auch als notwendiges Komplement zur Erforschung von Anonymisierungsverfahren verstanden werden – ähnlich, wie Kryptographie und Kryptoanalyse einander bedingen. Die De-Anonymisierung greift somit zwar in das Informationelle Selbstbestimmungsrecht Einzelner ein, kann aber zu einem zukünftig besseren Schutz des Informationellen Selbstbestimmungsrechts in der Gesellschaft führen.

Die Veröffentlichung von Arbeiten, die sich mit De-Anonymisierung befassen, kann schließlich auch dazu führen, dass Unternehmen zukünftig mehr Zurückhaltung üben, wenn sie Datensätze mit potentiell personenbeziehbaren Daten veröffentlichen. Ob dieser Effekt dem öffentlichen Interesse an der Durchführung der Forschung zuzurechnen ist, ist diskutabel – er tritt erst nach Veröffentlichung der Ergebnisse ein. Zum Zeitpunkt der eigentlichen De-Anonymisierung steht aber noch nicht fest, ob und in welcher Form eine solche Veröffentlichung überhaupt stattfindet.

Den genannten positiven Effekten der Forschung stehen die schutzwürdigen Belange der betroffenen Personen gegenüber. Welches Interesse überwiegt, lässt sich nicht allgemein bewerten; jedoch dürfte bei einer Abwägung insbesondere die Art der Daten zu berücksichtigen sein, so dass beispielsweise die De-Anonymisierung besonderer Arten personenbezogener Daten (§3 Abs. 9 BDSG bzw. §4 Abs. 3 DSG-NRW) als problematischer anzusehen ist. Gleichwohl ist diese nicht ausgeschlossen, sondern in §13 Abs. 2 Nr. 8 BDSG (für öffentliche Stellen des Bundes) und §4 Abs. 3 DSG-NRW ausdrücklich geregelt.

Als starkes Indiz für das Überwiegen schutzwürdiger Interessen des Betroffenen dürfte schließlich auch eine ursprünglich rechtswidrige Übermittlung an die Forscher zu werten sein; im Fall rechtswidrig *veröffentlichter* Daten ist dabei aber wiederum zu berücksichtigen, dass die De-Anonymisierung oft notwendig sein wird, um die Problematik glaubhaft zu machen und, soweit möglich, eine Rücknahme der Veröffentlichung zu erreichen.

7. Fazit

Im Ergebnis ist festzuhalten, dass die De-Anonymisierung von Daten im Rahmen der Erforschung des technischen Datenschutzes einer Abwägung im Einzelfall bedarf. Die Analyse hat zwar gezeigt, dass die Forschung durchaus gewichtige Argumente auf ihrer Seite hat. Dies befreit Wissenschaftler aber nicht von ihrer Verantwortung, trotz der für den Datenschutz langfristig positiven Effekte ihrer Forschung auch die (kurzfristigen) Interessen der aktuell betroffenen Personen zu berücksichtigen.

[14] www.imdb.com