Gerichtsentscheidungen de-anonymisiert

Prof. Dr. Dr. Hanjo Hamann 2023-10-02T08:46:45

> Prof. Dr. Olivia Burns, Professorin für Informationssicherheit an der Friedrich-Alexander-Universität Erlangen-Nürnberg, sollte am 8.8.2023 von der Hauptstadt Berlin nach Los Angeles fliegen.

Oder im Anonymisierungssprech der deutschen Justiz: *„Prof. Dr. O. B. Professorin für Informationssicherheit an der …-Universität E.-N. sollte am X.X.2023 von der Hauptstadt A. nach L. A. fliegen.“*

Dieses fiktive Exzerpt eines Tatbestandes und dessen Anonymisierung könnte einer Gerichtsentscheidung entnommen sein. Doch hat diese Anonymisierung tatsächlich Anonymität zur Folge? Während eine Person im technischen Sinn anonym ist, wenn sie nicht innerhalb einer Gruppe von Personen (Anonymitätsmenge) identifiziert werden kann, kann sie im rechtlichen Sinn dennoch als anonym gelten. Das ist der Fall, wenn der zur Identifizierung benötigte Aufwand nicht mehr verhältnismäßig ist.

Im Beispiel ergibt sich bereits aus dem Exzerpt selbst, dass „A.“ für Berlin – die Hauptstadt – stehen muss und „L. A.“ für Los Angeles, da es die gängige Abkürzung ist. Mit einer Google Suche ließe sich wohl die Universität herausfinden und über die spezifische Professur schließlich die Professorin hinter „O. B.“ identifizieren. Folglich kann aus technischer Sicht von Anonymität keine Rede sein. Um festzustellen, ob die Anonymisierung auch aus rechtlicher Sicht unzureichend ist, muss geklärt werden, ob der Identifizierungsaufwand noch verhältnismäßig war. Im Beispiel wird man daran kaum zweifeln können. Doch ist das Beispiel realistisch und sinnbildlich für die Anonymisierungsqualität deutscher Gerichtsentscheidungen? Um dieser Frage nachzugehen, schauen wir uns zunächst an, welche Anonymisierungstechniken die Gerichte einsetzen. Anschließend beschreiben wir ein De-Anonymisierungsexperiment, in dem 54 Jurastudierende nur mithilfe des frei zugänglichen Internets 50 zufällige Entscheidungen der ordentlichen Gerichtsbarkeit de-anonymisieren sollten. Abschließend präsentieren wir die Ergebnisse des Experiments und zeigen auf, wie die Anonymisierungsqualität verbessert werden kann.

1. Wie wird anonymisiert?

Die Anonymisierungstechniken der Gerichte lassen sich grob in Auslassung und Ersetzung unterteilen.[1] Bei der Auslassung wird die zu anonymisierende Information teilweise bis vollständig ausgelassen. Die wohl häufigste Erscheinungsform der teilweisen Auslassung sind Anfangsbuchstaben (in obigem Beispiel: „O. B.“ für Olivia Burns und „L. A.“ für Los Angeles). Bei der Ersetzung wird die zu anonymisierende

Information teilweise oder vollständig durch einen neutralen Bezeichner (in obigem Beispiel: „A.“ für Berlin, „…“ für Friedrich-Alexander oder „X.X.2023“ für 8.8.2023) oder einen generellen Bezeichner (beispielsweise: „Vorname1 Nachname1“ für Olivia Burns oder „Stadt1“ für Berlin) ersetzt.

2. De-Anonymisierungsexperiment

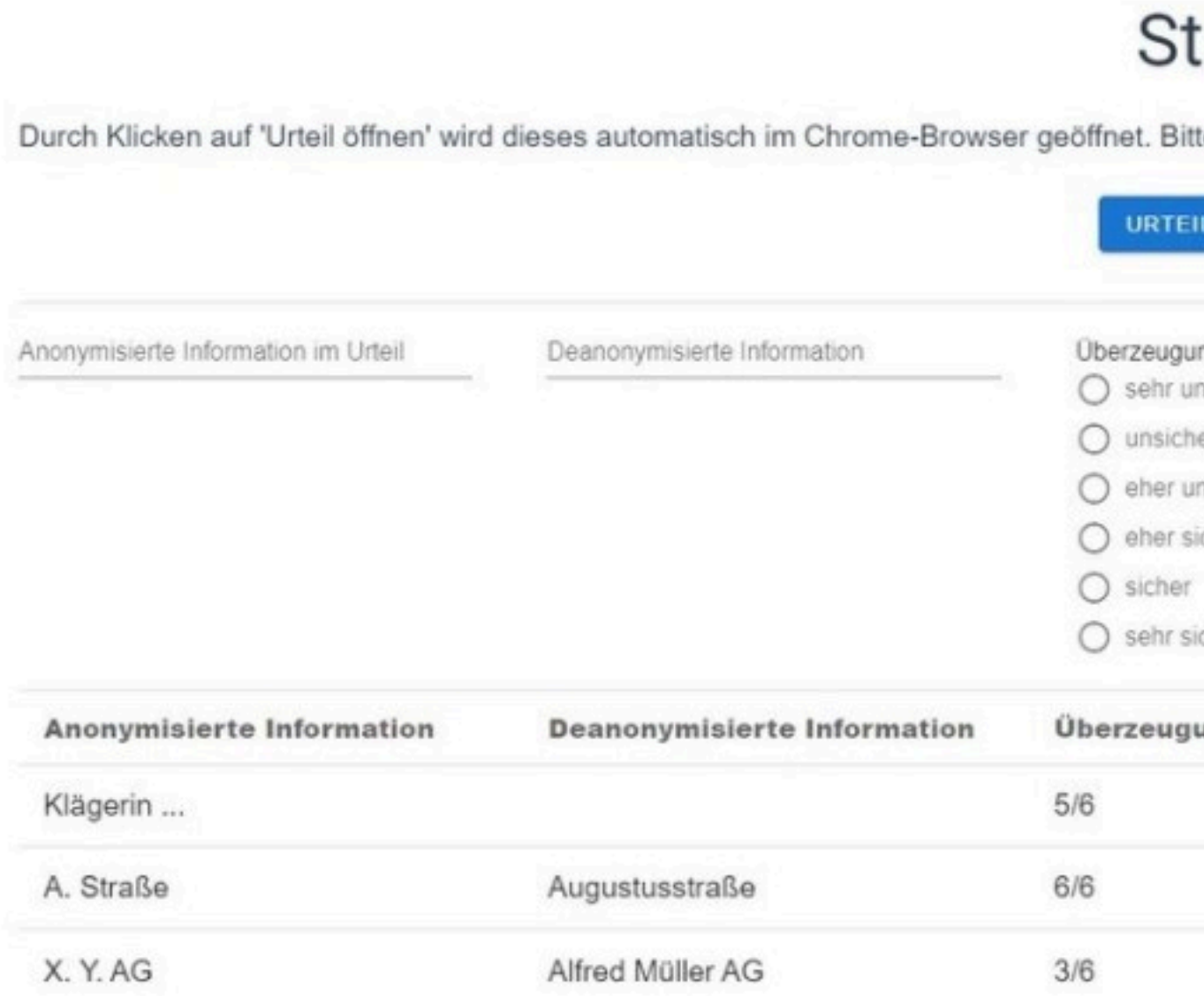
a) Leitgedanke: Minimaler Aufwand

Die Anonymisierungsqualität lässt sich nur empirisch ermitteln, da aus rechtlicher Sicht auf den Aufwand und dessen Verhältnismäßigkeit abgestellt wird. Aus diesem Grund wurde von uns ein De-Anonymisierungsexperiment durchgeführt.[2] Um festzustellen, ob der Aufwand noch verhältnismäßig ist, sind insbesondere Zeit, Kosten und Arbeitskraft zu berücksichtigen.[3] Bei der Konzeption unseres De-Anonymisierungsexperiments wurden diese Faktoren minimal – und damit jedenfalls verhältnismäßig – angesetzt, um aus möglichen De-Anonymisierungen folgern zu können, dass die anonymisierte Textstelle auch aus rechtlicher Sicht nicht als anonym anzusehen war.

b) Experimentaufbau und Teilnehmende

Wir rekrutierten für das Experiment 54 Jurastudierende, die für ihre dreistündige Tätigkeit je einen 30 Euro Amazon-Gutschein erhielten (was dem gesetzlichen Mindestlohn zum Zeitpunkt des Experiments entsprach). Die Studierenden erhielten keine spezifische Anleitung oder Training, wie sie bei der Anonymisierung vorzugehen haben und hatten auch keine Erfahrung mit dem De-Anonymisieren von Daten. Einziges Hilfsmittel war das öffentlich zugängliche Internet, wobei den Studierenden kein Budget zustand, um auf Inhalte hinter einer Bezahlschranke zuzugreifen.

Jede Studentin und jeder Student arbeitete alleine und hatte pro Entscheidung lediglich 35 Minuten Zeit. Diese Zeit umfasste das Lesen der Entscheidung, die Detektion der zu de-anonymisierenden Stellen, die De-Anonymisierung und die Dokumentation der Ergebnisse. Die Studierenden dokumentierten die anonymisierte Information aus dem Urteil und die dazugehörige de-anonymisierte Information in einer Studienansicht. Außerdem hielten sie dort ihren Überzeugungsgrad fest, d.h. wie sicher sie sich waren, dass die de-anonymisierte Information tatsächlich so im Urteil (vor der Anonymisierung) stand. Schließlich gaben die Studierenden die Links zu den Quellen an, aus denen sie ihre De-Anonymisierung ableiteten, sowie eine kurze Begründung. Die Studienansicht[4] sah wie folgt aus:



c) De-Anonymisierungsgegenstand

Für die De-Anonymisierung wurden 50 Gerichtsentscheidungen aus ungefähr 356.000 öffentlich zugänglichen Entscheidungen aller Bundesländer ausgewählt.[5] Dabei wurde sich auf Entscheidungen der ordentlichen Gerichtsbarkeit aus 2016 bis 2020 beschränkt, die zwischen 2000 und 4000 Wörtern lang waren. Die Auswahl der 50 Entscheidungen erfolgte zufällig unter der Maßgabe, dass die verschiedenen Anonymisierungstechniken ausreichend vertreten waren und überhaupt verschiedene anonymisierte Textstellen (wie Namen, Ortsangaben, Webadressen, Nummern) vorlagen. Insgesamt enthielten die 50 Entscheidungen 484 einzigartige anonymisierte Informationen – darunter über 57 % Namen von natürlichen oder juristischen Personen – die gegebenenfalls in mehreren teilweise unterschiedlich anonymisierten Textstellen vorkamen.

3. Auswertung und Ergebnisse

a) Verifizierungsprozess

Bei der Auswertung des Experiments konnte nicht auf die Originalentscheidungen zurückgegriffen werden, um die Richtigkeit der De-Anonymisierungen der Studierenden zu überprüfen. Daher mussten wir die Richtigkeit anders verifizieren, wobei Ausgangspunkt die Quellen, Begründungen und Überzeugungsgrade der Studierenden waren. Zunächst berücksichtigten wir nur solche de-anonymisierenden Informationen, bei denen sich die Studierenden „eher sicher“ bis „sehr sicher“ waren. Wir nennen solche de-anonymisierenden Informationen **potentielle De-Anonymisierungen**. Zum Verifizieren der potentiellen De-Anonymisierungen haben wir in einem nächsten Schritt selbst versucht, Quellen und Argumentationen zu finden. Die Argumentation rechtfertigt, warum die De-Anonymisierung basierend auf den von uns gefundenen Quellen erfolgreich war und definitiv mit der Information aus der Originalentscheidung übereinstimmt. Wir unterscheiden vier Argumentationslinien:

- Rechtliches Argument: Jegliche Information, die direkt aufgrund einer Rechtsnorm folgt (z. B. Zuständigkeiten der Gerichte, Richterinnen und Richter; gesetzliche Vertreter juristischer Personen).
- Geografisches Argument: Jegliche Information, die direkt aufgrund geografischer Eindeutigkeit folgt. Die Eindeutigkeit lässt sich vergleichsweise einfach feststellen, da Ortsangaben leicht zugänglich und abgeschlossen sind, d.h. es gibt nur begrenzt viele Gebietskörperschaften mit dazugehörigen Straßen und Wegen (z. B. Hauptstadt „A.“ muss Berlin sein, da Deutschland nur eine Hauptstadt hat; Städte haben möglicherweise nur eine Straße, deren Name mit einer bestimmten Buchstabenkombination beginnt).
- Aus der Entscheidung heraus: Jegliche Information, die direkt aus der Entscheidung folgt, da sie beispielsweise an späterer Stelle in nicht anonymisierter Form genannt wird.
- Eindeutige Schlussfolgerung: Jegliche Information, die so spezifisch ist, dass sie für sich genommen oder in Kombination mit anderen Informationen eine eindeutige Schlussfolgerung erlaubt (z.B. gibt es an einer bestimmten Universität nur eine Professorin für Informationssicherheit; oder ein Athlet hat bei einem Sportwettkampf einen bestimmten Platz belegt).

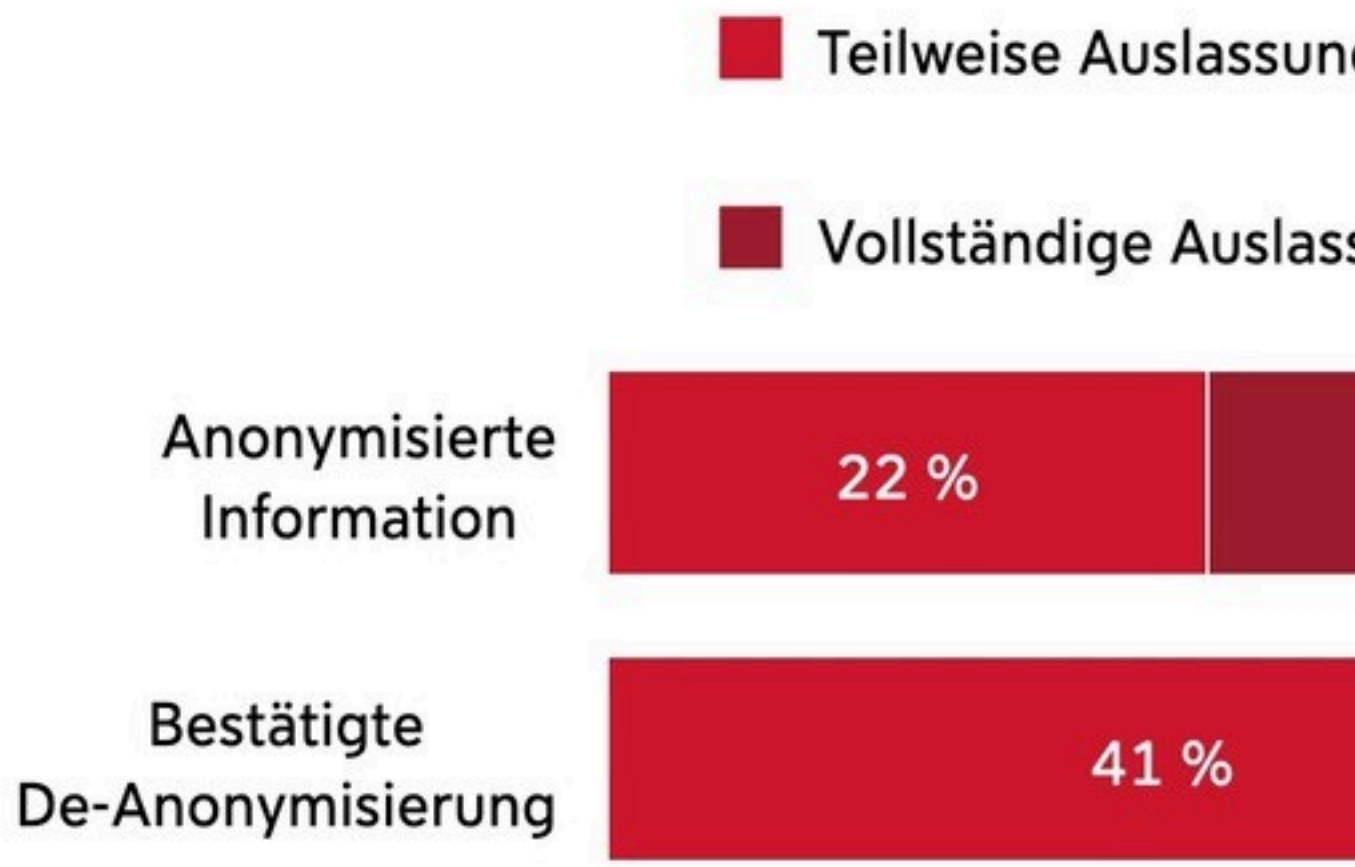
Jede potentielle De-Anonymisierung, die durch diesen Verifikationsprozess bestätigt werden konnte, heißt **bestätigte De-Anonymisierung**.

b) Erfolg der De-Anonymisierung

Die Studierenden konnten 184 (38 %) der 484 anonymisierten Informationen in den Entscheidungen potentiell de-anonymisieren. In 115 Fällen konnten die potentiellen De-Anonymisierungen bestätigt werden. Folglich wurde fast jede vierte anonymisierte Information bestätigt de-anonymisiert. Mehr als jede dritte (37

%) bestätigte De-Anonymisierung war die eines Namens einer natürlichen oder juristischen Person.

Sämtliche Anonymisierungstechniken, d.h. teilweise oder vollständige Auslassung oder Ersetzung, zeigten sich anfällig für De-Anonymisierungen. Dennoch gab es erhebliche Unterschiede zwischen den einzelnen Techniken. Die nachfolgende Darstellung zeigt die Verteilungen der Anonymisierungstechniken an den anonymisierten Informationen und an den bestätigten De-Anonymisierungen:



Am schlechtesten schnitt die *teilweise* Auslassung (Anfangsbuchstaben) ab. Ihr Anteil an den bestätigten De-Anonymisierungen war am größten (40 %). Dagegen wurden nur etwas mehr als ein Fünftel (22 %) der anonymisierten Informationen aus den Entscheidungen mittels teilweiser Auslassung anonymisiert.

Weniger anfällig für De-Anonymisierungen zeigten sich die *vollständigen* Auslassungen und *vollständigen* Ersetzungen. Nur jede zehnte bestätigte De-Anonymisierung war eine De-Anonymisierung mittels vollständiger Auslassung anonymisierter Information, wohingegen mit dieser Anonymisierungstechnik fast jede vierte (23 %) anonymisierte Information anonymisiert war. Ähnlich verhielten sich die Anonymisierungen mittels vollständiger Ersetzung.

c) Aufwand der De-Anonymisierung

Die De-Anonymisierungen erscheinen insbesondere deshalb problematisch, weil der eingesetzte Aufwand minimal war. Ein durchschnittlicher Angriff einer Studentin oder eines Studenten, gerichtet auf eine einzelne Entscheidung, dauerte 33 Minuten[6] und kostete 7 Euro. Die Studierenden berichteten häufig, dass sie nicht ausreichend Zeit für – aus ihrer Sicht – noch mögliche De-Anonymisierungen hatten, weshalb die Zeit nicht noch geringer angesetzt werden kann. Ebenso können die Kosten für die Arbeitskraft nicht niedriger angesetzt werden, ohne den gesetzlichen Mindestlohn zu unterschreiten.

Die Studierenden befanden sich durchschnittlich in ihrem sechsten Semester und machten teilweise Fehler, die auf juristische Unkenntnis oder unsauberes Lesen der Entscheidung zurückzuführen waren. Daher könnte man argumentieren, dass es zur Vermeidung solcher Fehler per se nicht unverhältnismäßig wäre, höher qualifiziertes Personal zur De-Anonymisierung einzusetzen. Vorstellbar wäre auch, alternativ oder zusätzlich, das Personal besser zu instruieren oder weitere Hilfe zur De-Anonymisierung bereitzustellen.

Unser Verifizierungsprozess und die Aussagen der Studierenden lassen vermuten, dass noch mehr De-Anonymisierungen möglich gewesen wären. Da der eingesetzte Aufwand minimal war, ist noch Potential vorhanden, bis der Aufwand die Schwelle zur Unverhältnismäßigkeit überschreitet. Daher sind neben den bereits dargestellten Optionen auch technische Unterstützungen denkbar, wie eine automatische Detektion und Hervorhebung zu de-anonymisierender Informationen. Darüber hinaus ließe sich der De-Anonymisierungsprozess mittels automatischer Schlagwortsuche erleichtern oder gar maschinelle Lernverfahren zur De-Anonymisierung einsetzen. Geht man davon aus, dass noch De-Anonymisierungspotential vorhanden ist, besteht somit die Gefahr einer effizienteren und weitreichenderen De-Anonymisierung.

d) Quellen der De-Anonymisierung

Die Studierenden haben eine Vielzahl unterschiedlicher öffentlich zugänglicher Quellen für ihre potentiellen De-Anonymisierungen angegeben. Diese lassen sich in die Kategorien Nachrichten, Webauftritte natürlicher oder juristischer Personen, andere Entscheidungen, Geschäftsverzeichnisse, Wikis, staatliche Webseiten, Suchmaschinen, die angegriffene Entscheidung, Kartendienste und Sonstiges einteilen. Nachfolgend ist die Häufigkeitsverteilung der angegebenen Quellen nach Kategorien abgebildet:


Nachrichten
Webauftritte nat./jur. Personen
Andere Entscheidungen
Geschäftsverzeichnisse
Wikis
Staatliche Webseiten
Suchmaschinen
Angegriffene Entscheidung
Kartendienste
Sonstige
3 %

Die mit Abstand häufigsten Quellen waren Nachrichten (23 %) und Webauftritte natürlicher oder juristischer Personen (21 %). Bemerkenswert ist, dass die angegriffene Entscheidung und andere Gerichtsentscheidungen zusammen 15 % aller Quellen ausmachten. Dies lag mitunter daran, dass innerhalb einer Entscheidung von den Gerichten als anonymisierungsbedürftig erachtete Informationen an späterer Stelle überhaupt nicht anonymisiert wurden – mutmaßlich, weil sie schlicht übersehen wurden. Außerdem haben andere mit dem Streitgegenstand betraute Gerichte teilweise weniger intensiv (unzureichend) anonymisiert.

4. Fazit

Das De-Anonymisierungsexperiment mit seinen 50 Gerichtsentscheidungen ist nicht repräsentativ für alle deutschen Gerichtsentscheidungen, zeigt jedoch bestehende Schwächen in der Anonymisierungspraxis auf. Allerdings können bereits die folgenden drei Änderungen die Anonymisierungsqualität steigern. Erstens sollten keinesfalls Anfangsbuchstaben zur Anonymisierung verwendet werden, sondern stattdessen immer vollständige Auslassungen oder vollständige Ersetzungen mit neutralen oder generellen Bezeichnern. Als zweite Empfehlung sollte innerhalb einer Entscheidung konsistent jede anonymisierungsbedürftige Textstelle anonymisiert werden. Ebenso sollte diese Konsistenz über Gerichte hinweg erhalten bleiben und idealerweise nicht durch die Medien unterlaufen werden. Drittens sollte die Anonymisierung auf solche nicht anonymisierte Angaben erstreckt werden, die so spezifisch und einzigartig sind, dass sie eindeutige Schlussfolgerungen über anonymisierte Information erlauben. Denn sie sind ein Grund, dass selbst mittels sicherer Techniken anonymisierte Entscheidungen noch anfällig für De-Anonymisierungen waren.

Ein Blick in die Zukunft unterstreicht die Notwendigkeit die Anonymisierungsqualität zu verbessern. Bereits erste Versuche, ChatGPT zur De-Anonymisierung weniger Entscheidungen aus diesem Experiment einzusetzen, waren erschreckenderweise erfolgsversprechend. Eine Automatisierung der De-Anonymisierung scheint somit nicht unrealistisch. Die damit einhergehende Skalierbarkeit würde eine große Gefahr für den Bestand aller öffentlich zugänglichen Gerichtsentscheidungen darstellen. Daher heißt es jetzt: Wenn die Gerichte nicht mit der Zeit anonymisieren, werden die Beteiligten mit der Zeit de-anonymisiert.
