Multi-Party Computation als Instrument zur Umsetzung datenschutzkonformer behördlicher Datenabgleiche

Eine interdisziplinäre Analyse am Beispiel der Diskussionen um das Gesetz zur Selbstbestimmung über den Geschlechtseintrag

Linda Seyda[1], Andreas Brüggemann[2], Gerrit Hornung[1] und Thomas Schneider[2]

Abstract: Am 12. April 2024 wurde das Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG) im Bundestag beschlossen. Trans*, intergeschlechtliche und nicht-binäre Personen können ab dem 1. November 2024 ohne entwürdigende Verfahren ihren Vornamen und Geschlechtseintrag beim Standesamt durch Eigenerklärung ändern. Zur Weiterverfolgbarkeit des Individuums nach Namensänderung war zwischenzeitlich eine automatisierte Datenweitergabe an Sicherheitsbehörden vorgesehen. Die entsprechende Vorschrift wurde in den Ausschussberatungen ersatzlos gestrichen. Zur Begründung dafür wurde die Vereinheitlichung mit dem sonstigen Namensrecht angeführt, nicht aber Datenschutzbedenken. Die ursprünglich in § 13 Abs. 5 SBGG-Regierungsentwurf (RegE) geplante Regelung könnte jedoch in einer geplanten Reform des Namensänderungsgesetzes erneut aufgegriffen werden, woraus sich berechtigte Sorgen bzgl. Überwachung, Datenschutz und Diskriminierung ergeben. Diesen kann mit einer auf Multi-Party Computation basierenden Lösung begegnet werden, welche eine datensparsame Handhabung ermöglicht. Dieser Beitrag betrachtet datensparsame behördliche Datenabgleiche zu Nachverfolgbarkeitszwecken am Beispiel des nunmehr verworfenen § 13 Abs. 5 SBGG-RegE aus interdisziplinär rechtlich-kryptographischer Sicht.

Keywords: Multi-Party Computation, Selbstbestimmungsgesetz, Datenschutz, Private Set Intersection

1 Einleitung

§ 2 SBGG ermöglicht es trans*, intergeschlechtlichen und nichtbinären Menschen, durch Erklärung gegenüber dem Standesamt ihren Vornamen und ihren Geschlechtseintrag ändern zu lassen. Dazu sind ab dem vollendeten 14. Lebensjahr keinerlei weitere Nachweise erforderlich. Die Erklärung ist drei Monate vor ihrer Abgabe anzumelden; die Anmeldungen zur Erklärung sind seit August 2024 möglich. Zum Schutz der Betroffenen sieht das Gesetz in § 13 SBGG ein Offenbarungsverbot vor. Dadurch ist verboten, Informationen zum früheren Geschlechtseintrag ohne Zustimmung der betreffenden Person auszuforschen und weiterzugeben.

In § 13 Abs. 5 SBGG-RegE [BT23] waren Ausnahmen von diesem Offenbarungsverbot dergestalt vorgesehen, dass Änderungen des Vornamens und des Geschlechtseintrags an Sicherheitsbehörden übermittelt werden sollten. Damit sollten die enumerativ aufgelisteten Behörden, darunter u.a. das Bundeskriminalamt und das Bundesamt für den militärischen

[1] Universität Kassel, linda.seyda@uni-kassel.de; gerrit.hornung@uni-kassel.de
[2] TU Darmstadt, brueggemann@encrypto.cs.tu-darmstadt.de, https://orcid.org/0000-0002-8102-9328; schneider@encrypto.cs.tu-darmstadt.de, https://orcid.org/0000-0001-8090-1316

doi:10.18420/inf2024_11

Abschirmdienst, ihre Einträge überprüfen und aktualisieren können. Hätte keine Eintragung über die betroffene Person vorgelegen, hätten die empfangenden Behörden die übermittelten Daten unverzüglich eigenverantwortlich löschen müssen.

An diesem Regelungsvorschlag wurde kritisiert, dass die vom SBGG begünstigten Personen, nach langem Leidensweg [Sl24] durch das vormals einschlägige Transsexuellengesetz (TSG)[3], nun durch diese Regelungen „unter Generalverdacht" [Kö23] gestellt würden. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) kritisierte die geplante Vorschrift und äußerte u.a. erhebliche rechtliche Bedenken bzgl. der Verhältnismäßigkeit von § 13 Abs. 3 und Abs. 5 SBGG-RegE [BfDI23, S. 3].

Durch die Streichung von § 13 Abs. 5 SBGG-RegE sind die mit den Datenübermittlungen verbundenen Probleme abgemildert, aber nicht vollständig beseitigt worden. Denn die früheren Personenangaben bleiben in amtlichen Registern und Informationssystemen enthalten (§ 13 Abs. 3 SBGG), und Mitteilungen und Informationen zwischen amtlichen Registern und Informationssystemen sowie Abrufe aus diesen sind aufgrund anderer Rechtsvorschriften weiterhin zulässig (§ 13 Abs. 4 SBGG).

Ein Beispiel hierfür ist § 20a BZRG, wonach schon bisher die Meldebehörden bei Namensänderungen eine Meldung an die Registerbehörden vornehmen müssen. Ähnlich wie im geplanten § 13 Abs. 5 SBGG-RegE sind letztere verpflichtet, die Daten zu löschen, wenn bei Ihnen keine entsprechenden Einträge vorhanden sind. Die Diskussionen um § 13 Abs. 5 SBGG-RegE sind deshalb paradigmatisch für das größere Problem behördlicher Datenabgleiche in Fällen, in denen die übermittelnde Behörde die Erforderlichkeit der Übermittlung auf Empfängerseite nicht beurteilen kann.

Im Folgenden werden nach einem Überblick über die ursprünglich geplante Datenübermittlungspraxis (Abschnitt 2) die (datenschutzrechtlichen) Bedenken diesbezüglich beleuchtet (Abschnitt 3) und anzustrebende Anforderungen an einen datenschutzfreundlicheren Prozess spezifiziert (Abschnitt 4). Anschließend wird in Abschnitt 5 gezeigt, dass kryptographische Techniken eine *selektive* Übermittlung ermöglichen, bei der auf der Empfängerseite nicht relevante Daten erst gar nicht anfallen und somit nicht gelöscht werden müssen.

2 § 13 Abs. 5 SBGG-RegE: Einstieg und Überblick

Der Verlauf der Gesetzgebung in Bezug auf das SBGG und die Debatte über eine mögliche automatisierte Datenweitergabe an Behörden zeigt, dass der Gesetzgeber an dieser Übermittlungspraxis festhält und jedenfalls im Fall des § 13 Abs. 5 SBGG-RegE den Datenschutz nicht hinreichend berücksichtigt hat. Zudem zeigen sich auch geltende Vorschriften wie § 20a BZRG als verbesserungsfähig. Daher wird am Beispiel des § 13 Abs. 5 SBGG-RegE im Folgenden gezeigt, dass diese Praxis insb. nach datenschutzrechtlichen Gesichtspunkten kritisch zu sehen ist. Darüber hinaus werden technische Bedenken präsentiert und schließlich reale Risiken für die namensändernden Personen aufgezeigt.

[3] Vom BVerfG in sechs Entscheidungen in Teilen für verfassungswidrig erklärt [BT23, S. 19 m.w.N.]

Zu den insgesamt zehn zu informierenden Behörden nach erfolgter Änderung des Vornamens und des Geschlechtseintrags gehörten u.a. das Bundeskriminalamt, die Bundespolizei, das Bundesverwaltungsamt für das Nationale Waffenregister, das Bundesamt für Verfassungsschutz, das Bundesamt für den militärischen Abschirmdienst sowie die Landeskriminalämter; für die gesamte Aufzählung siehe [BT23, S. 11].

Automatisiert an diese zu übermitteln gewesen wären der Familienname, die bisherigen und geänderten Vornamen, Geburtsdatum und -ort, Staatsangehörigkeiten, bisheriger und geänderter Geschlechtseintrag, Anschrift sowie das Änderungsdatum. Begründet wurde diese Übermittlung damit, dass die Nachverfolgbarkeit einer Person nach einer Änderung des Geschlechtseintrags und der Vornamen gewährleistet werden sollte [BT23, S. 57].

In den Ausschussberatungen wurde die Vorschrift ersatzlos gestrichen. Als Grund dafür ist die Vermeidung „unterschiedlicher Regelungen zur (automatisierten) Datenweitergabe bei Änderungen des Geschlechtseintrages und der Vornamen [...] insb. im Vergleich zu sonstigen Namensänderungen“ angeführt [BT24, S. 39]. In einem in der Beschlussempfehlung enthaltenen Entschließungsantrag [BT24, S. 31] der Koalitionsfraktionen fordern diese die Bundesregierung auf, das öffentlich-rechtliche Namensrecht zu reformieren und hierzu bis Ende 2024 einen Vorschlag vorzulegen. Dieser solle für verschiedene Formen der Namensänderung (d.h. diskriminierungsfrei auch, aber nicht nur im Zuge der Änderung des Geschlechtseintrags) einheitliche Übermittlungsvorschriften zur Sicherung berechtigter staatlicher Ordnungsinteressen vorsehen. Die Entschließung betont ausdrücklich, dass dies datenschutzkonform und effektiv erfolgen muss, erläutert diese Anforderung aber nicht weiter.

3 Vertiefung zu § 13 Abs. 5 SBGG-RegE: Kritik

Die in Art. 13 Abs. 5 SBGG-RegE geplante Vorschrift wurde aus datenschutzrechtlichen, technischen und tatsächlichen Gründen kritisiert. Hinsichtlich Parallelregelungen wie § 20a BZRG und insb. mit Blick auf die durch den Bundestag geforderte Reform des Namensrechts ist diese von fortdauernder Relevanz. Dies auch deshalb, weil jede Offenbarung der Eigenschaft als trans*, intergeschlechtliche oder nicht-binäre Person Risiken bis hin zur Gewalt gegen die Person mit sich bringt.

3.1 Konfligierende Grundsätze der Datenverarbeitung und bisherige Übermittlungspraxis

Bei Übermittlungen wie denen nach § 20a BZRG oder § 13 Abs. 5 SBGG-RegE handelt es sich um eine Verarbeitung personenbezogener Daten (Art. 4 Nr. 1 DS-GVO). Damit ist der Anwendungsbereich des grundrechtlichen (Art. 7, 8 GRCh, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und des einfachgesetzlichen Datenschutzrechts eröffnet. Zur Abgrenzung vom Anwendungsbereich der JI- Richtlinie muss nach Verarbeitungsvorgängen differenziert werden. Dabei ist jedenfalls für die Übermittlung der Daten seitens der Standesämter als meldende Behörde von einer Einschlägigkeit der DS-GVO auszugehen, da diese nicht für die Ermittlung,

Aufklärung und Verhütung von Straftaten zuständig sind (vgl. Art. 2 Abs. 2 lit. d DS-GVO). Lediglich für die empfangenden Behörden könnte die JI-Richtlinie maßgeblich sein.[4]

Besondere Herausforderungen ergeben sich zudem schon hinsichtlich der Grundsätze der Datenrichtigkeit und der Datenminimierung, die im Folgenden untersucht werden.[5]

Der Grundsatz der Datenrichtigkeit findet sich in Art. 5 Abs. 1 lit. d DS-GVO. Danach müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. EG 39 zur DS-GVO fordert, dass alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Durch eine Änderung des Vornamens und des Geschlechtseintrags werden die bisher bei den Behörden verarbeiteten Daten unrichtig. Insofern streitet der Grundsatz der Datenrichtigkeit für eine automatisierte Übermittlung der aktualisierten Daten – aber nur für diejenigen betroffenen Personen, über die bereits Eintragungen in den Datenbeständen der Sicherheitsbehörden existieren. Die Richtigkeit von Datenbeständen nach Namensänderungen dürfte auch im mutmaßlichen Interesse der betroffenen Person liegen, so auch der BfDI [BfDI23, S. 2]. Insb. im Falle von Namensänderungen nach dem SBGG steht es für Betroffene im Vordergrund, ihre Geschlechtsidentität diskriminierungsfrei zu verwirklichen und dementsprechend mit dem von ihnen gewählten Vornamen angesprochen zu werden [HT23].

Nach dem Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DS-GVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Auf diese Weise werden der Datenverarbeitung Grenzen gesetzt und die Tiefe des Eingriffs in das Grundrecht auf Datenschutz beschränkt [Ro19, Rn. 116]. „Auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind die personenbezogenen Daten, wenn der Zweck ohne ihre Verarbeitung nicht erreicht werden kann“ [Ro19, Rn. 121]. Dementsprechend müsste der Zweck der Verarbeitung zunächst benannt werden. Als solcher kommen „berechtigte Sicherheitsinteressen“ in Betracht, die die empfangenden Behörden verfolgen. Diese bestehen jedoch nur im Hinblick auf die Daten der Personen, die bereits in den Datenbeständen der empfangenden Behörde verarbeitet werden. Für alle anderen personenbezogenen Daten besteht kein Sicherheitsinteresse und es entfällt (objektiv) schon der Zweck der Verarbeitung. Hierbei besteht das faktische Problem, dass die Meldebehörde, die über den korrigierten Datenbestand verfügt, weder wissen kann, noch wissen darf, über welche Personen bereits Einträge im Datenbestand der Sicherheitsbehörde vorhanden sind. Im Falle einer Übermittlung i.S.d. § 13 Abs. 5 SBGG-RegE resultiert dies darin, dass objektiv nicht

[4] Die folgenden Überlegungen sind im Grundsatz auf solche Übermittlungen übertragbar, die unter die JI-Richtlinie fallen oder außerhalb des Unionsrechts liegen.

[5] Die Zulässigkeit nach der DS-GVO wirft weitere Fragen auf, die hier nicht im Detail behandelt werden können. So ist z.B. unklar, ob die zu übermittelnden Daten unter Art. 9 DS-GVO fallen, obwohl die Eigenschaft als trans*, intergeschlechtlicher und nichtbinärer Menschen als solche keine Rückschlüsse auf Sexualleben oder sexuelle Orientierung ermöglicht. Die im Folgenden diskutierten Grundsatzfragen stellen sich aber unabhängig von der Anwendbarkeit von Art. 9 DS-GVO und den aus ihr ggf. folgenden gesteigerten Verhältnismäßigkeitsvorgaben.

erforderliche Daten übermittelt werden. Damit streitet der Grundsatz der Datenminimierung gegen die durch § 13 Abs. 5 SBGG-RegE repräsentierte Datenübermittlung.

Datenrichtigkeit und Datenminimierung stehen daher in der vorliegenden Situation im Widerspruch zueinander. Dazu kommt, dass unrichtige oder veraltete Daten in der Regel „weder erheblich noch auf das notwendige Maß beschränkt“ sind, was dazu führt, dass die Verarbeitung falscher Daten nicht nur gegen den Grundsatz der Datenrichtigkeit verstößt, sondern auch dem der Datenminimierung widerspricht und folglich unzulässig ist [Ro19, Rn. 138; Eu14, Rn. 93; Fr21, Rn. 39]. Demnach ist es geboten, veränderte Vornamen und Geschlechtseinträge in Datenbeständen zu korrigieren, da andernfalls die Beschränkung auf das notwendige Maß entfiele. Das notwendige Maß übersteigen würde eine Weitergabe der Daten einer betroffenen Person etwa an den militärischen Abschirmdienst, obwohl die konkrete Person niemals für diesen relevante Aktivitäten ausgeführt hat.

Der BfDI wägt die Grundsätze der Datenminimierung und der Datenrichtigkeit in einer Gesamtbetrachtung mit dem Recht auf informationelle Selbstbestimmung sowie dem Interesse aller Personen an der Vermeidung von Verwechslungen ab [BfDI23, S. 5]. Er resümiert, dass es sich bei Änderungen von Vornamen und Geschlechtseintrag um durch das allgemeine Persönlichkeitsrecht geschützte Bereiche handele, weswegen der Grundsatz der Datenminimierung überwiege [BfDI23, S. 5].

Es verbleibt ein datenschutzrechtliches Dilemma, insb. dadurch, dass die derzeitige und auch in § 13 Abs. 5 SBGG-RegE angedachte Form der Übermittlung theoretisch eine Entscheidung zwischen Datenrichtigkeit und Datenminimierung fordert. Diese Problematik war dem Gesetzgeber zumindest bei Schaffung des § 20a BZRG (an welchen § 13 Abs. 5 SBGG-RegE angelehnt war [BT23, S. 57]) bekannt. In der Gesetzesbegründung heißt es: „Die Mitteilungen über Namensänderungen können nicht auf die Personen beschränkt werden, über die das Register eine Eintragung enthält, da dies den [...] Behörden, [...], regelmäßig nicht bekannt ist.“ [BT96, S. 30] Aus technischer Sicht ist diese Ansicht jedoch nicht mehr zutreffend, da durchaus Techniken existieren, die diese Beschränkung ermöglichen (vgl. Abschnitt 5).

Der BfDI wirft in seiner Stellungnahme [BfDI23, S. 4] die Frage auf, ob anstelle von § 13 Abs. 5 SBGG-RegE die bisherigen Regelungen ausreichend seien, wonach Änderungen des Geschlechts und des Vornamens exklusiv den Registerbehörden mitgeteilt werden müssen. Dies würde es anderen Behörden sodann ermöglichen, durch Abfragen selbst für eine Aktualität und Richtigkeit ihrer eigenen Register zu sorgen. Auf diesem Wege würden nur die Daten von Personen zwischen den Behörden ausgetauscht, die ohnehin bereits dort verzeichnet sind [BfDI23, S. 4]. Dies lässt den Schluss zu, dass die bisherige Aktualisierungspraxis auf Einzelabfragen fußt. Eine genaue Beschreibung der Vorgänge findet sich nicht. Dabei bleibt außer Acht, dass auch diese Anfragen von Sicherheitsbehörden an die Registerbehörden sensible Informationen offenlegen können. Bspw. dann, wenn der Verfassungsschutz bei einer Registerbehörde Änderungen einer Person abfragt und davon abzuleiten ist, dass gegen diese Person Ermittlungen geführt werden. Denkbar wäre auch, dass jede Sicherheitsbehörde

ihren gesamten Datenbestand an die Registerbehörden zum Abgleich schickt – was aber wiederum die umfassende Übermittlung sensibler Daten an diese zur Folge hätte.

3.2 Technische Bedenken

Durch die Weitergabe sämtlicher Eintragsänderungen an Behörden gemäß § 13 Abs. 5 SBGG-RegE erhielten die jeweiligen Behörden nicht nur die für sie relevanten Änderungen, für welche Registereinträge angeglichen werden müssen, sondern auch für sie irrelevante Eintragsänderungen zu ihnen unbekannten Personen. Die Weitergabe dieser irrelevanten Änderungen ist somit für die Behörde zur Erfüllung ihrer Aufgaben nicht direkt notwendig, stellt jedoch durch das grundlose Anfallen sensibler Informationen ein Risiko dar. Die durch § 13 Abs. 5 SBGG-RegE geforderte unverzügliche Löschung dieser Daten ist technisch schwierig umzusetzen, u.a. wegen des Erfordernisses mehrfacher Überschreibungen, und zudem nicht verifizierbar. Zudem wäre ein vorsätzliches oder auch versehentliches Abgreifen bereits vorliegender Daten (z.B. durch automatisierte Logs oder Backups) unverhältnismäßig einfach.

3.3 Tatsächliche Bedenken: Queerfeindlichkeit und queerfeindliche Straftaten

Jede Offenbarung und die inhärente Information darüber, dass die betroffene Person trans*-, intergeschlechtlich oder nicht-binär ist, birgt Risiken für sie. Dies zeigt sich an fortwährender Diskriminierung und Gewalt gegen diese Personen. Informationen über eine Änderung des Geschlechtseintrags und damit einhergehende Änderungen geschlechtstypischer Vornamen sind deshalb sensibler als Änderungen des Nachnamens. Die damit verbundenen Diskriminierungsrisiken sind struktureller Art; ein Hinweis auf sie geht deshalb nicht mit einem Generalverdacht gegenüber den Sicherheitsbehörden oder deren Mitarbeiter*innen einher.

Zu nennen sind in diesem Zusammenhang sogenannte „Rosa Listen“. Diese wurden insb. zu Zeiten des Nationalsozialismus geführt, um in Strafverfolgungsbehörden vermeintliche oder tatsächliche Homosexuelle zu registrieren [Ve]. Auch in der Geschichte der BRD wurden solche Listen weiterverwendet. Zuletzt kam es 2005 zum sog. IGVP-Skandal, als in der Polizeisoftware einiger Länder der Begriff der Homosexualität Personen zugeordnet wurde und Täter*innen danach gefiltert werden konnten [Ve]. Ähnliches könnte auch trans* Personen drohen: Dokumentiert sind diesbezüglich Fälle aus den USA, in denen versucht wurde, an Listen von Personen mit geänderten Geschlechtseinträgen zu gelangen [Kl22]. In Deutschland (Bayern) stieg die Zahl queerfeindlicher Straftaten in 2023 um über 100 Prozent im Vergleich zum Vorjahr [SZ24].

Durch die im Entschließungsantrag [BT24, S. 31] genannte Möglichkeit der Änderung „fremdländisch“ klingender Namen könnten sich diese Risiken durch anlasslose automatisierte Datenweitergabe ausweiten. Insb. angesichts jüngst abgehaltener rechtsextremer „Geheimtreffen“ [Be24] ist es wichtig, Betroffene vor dem Risiko rechtswidriger und menschenverachtender Verfolgung zu schützen. Derart sensible Informationen sollten daher nur so sparsam wie möglich verarbeitet werden. Für das Datenschutzrecht bedeutet

dies, dass durch seine Anwendung zum einen die Risiken zu mindern sind, die durch die Verarbeitung personenbezogener Daten selbst entstehen. Jedoch hat die DS-GVO gem. Art. 1 Abs. 2 auch den generellen Schutz von Grundrechten und -freiheiten zum Ziel, insb. die Vermeidung von Diskriminierungen. Sofern also vor den beschriebenen Gefahren durch datenschutzfreundliche Prozesse und Technologien geschützt werden kann, entspricht dies der Zielsetzung des europäischen Gesetzgebers, s. auch Erwgr. 2 zur DS-GVO.

3.4 Zwischenfazit

Eine Praxis der automatisierten Datenübermittlung aller Geschlechts- und Namensänderungen an sämtliche Sicherheitsbehörden, wie sie in § 13 Abs. 5 SBGG-RegE vorgesehen war, ist aus datenschutzrechtlicher Sicht problematisch. Demgegenüber besteht ein berechtigtes Interesse des Staates daran, Bürger*innen durch seine Sicherheitsbehörden identifizieren zu können. Korrekte Datenbestände liegen auch im mutmaßlichen Interesse betroffener Personen, in Zukunft mit dem korrekten Namen angesprochen zu werden. Eine falsche Ansprache aufgrund fehlerhafter Daten würde zudem dem Grundgedanken von § 13 Abs. 1 SBGG, dem Verbot der Ausforschung des vorher getragenen Namens, widersprechen.

Es verbliebe die Möglichkeit der Aktualisierung der Datenbestände durch Einzelabfragen. Diese sind jedoch zeitaufwändig und ineffektiv. Außerdem wird durch Einzelabfragen der Melde- oder Registerbehörde bekannt, dass über die betroffene Person ein Eintrag in der Datenbank der Sicherheitsbehörde existiert, sodass ein weiteres Datenschutzproblem entsteht.

Ideal wäre ein Ausgleich zwischen den Interessen der namensändernden Bürger*innen nach Privatheit und den Ordnungsinteressen des Staates. Ein solcher scheitert aber bisher daran, dass dem Gesetzgeber scheinbar keine datensparsame Alternative zur Übermittlung sämtlicher Geschlechts- und Namensänderungen mit den in § 13 Abs. 5 SBGG-RegE genannten (Klartext-)Daten bekannt ist. Im Folgenden soll demgegenüber gezeigt werden, dass durchaus technische Alternativen bestehen, die grundrechtsschonende Gestaltungen ermöglichen und somit auch dem Entschließungsantrag [BT24, S. 31] entsprechen. Notwendige Anforderungen und technische Möglichkeiten für eine solche datensparsame Übermittlung werden im Folgenden vorgestellt.

4 Datenschutzbezogene und funktionale Anforderungen

§ 13 Abs. 5 SBGG-RegE enthielt eine exakte Vorgabe zu Anlass und Umfang der Datenübermittlung. Die beabsichtigte Funktionalität lässt sich davon abstrahieren; sie liegt in der Benachrichtigung von Sicherheitsbehörden zu Eintragsänderungen bzgl. der von ihnen im Datenbestand geführten Personen. Mittels solcher Benachrichtigungen wären die Sicherheitsbehörden dann in der Lage, veraltete Einträge anzugleichen. Die Funktionalität kann, wie auch in Abb. 1 dargestellt, wie folgt abstrahiert werden:

- Die Behörde, die Eintragsänderungen erfasst (i.S.d. SBGG-RegE das Standesamt), verfügt über eine Liste neu erfasster Eintragsänderungen.

- Eine Sicherheitsbehörde verarbeitet Daten von Personen, bei denen die Aktualität der Daten gewährleistet werden muss.
- Die Sicherheitsbehörde wird über Änderungen von Einträgen zu in ihrem Datenbestand geführten Personen informiert, also über Änderungen bzgl. der Schnittmenge zwischen Personen mit geänderten Einträgen und ihrem Datenbestand.

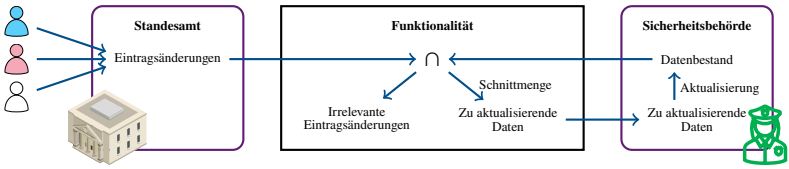

Abb. 1: Beabsichtigte Funktionalität zur Datenweitergabe an Sicherheitsbehörde

Die Interaktion mit mehreren Sicherheitsbehörden lässt sich aus mehreren solcher elementarer Funktionalitäten zwischen zwei Behörden zerlegen. Zu betonen ist nun, dass sich unter den vom Standesamt erfassten Eintragsänderungen nicht nur solche zu Personen im Datenbestand der Sicherheitsbehörde befinden (vgl. Abschnitte 1 und 3.2). Viel mehr existieren auch weitere irrelevante Eintragsänderungen zu Personen, welche der Sicherheitsbehörde unbekannt sind. Die Funktionalität erfordert damit keine Preisgabe dieser Daten, welche somit zugunsten der Datenminimierung bestenfalls auch nicht übermittelt werden sollten.

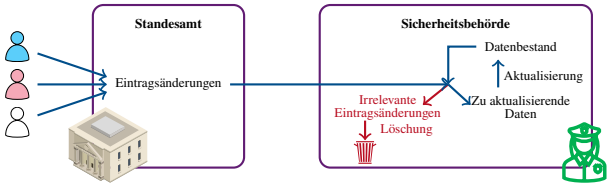

Abb. 2: Umsetzung der Funktionalität laut SBGG RegE

§ 13 Abs. 5 SBGG-RegE setzt diese Funktionalität jedoch durch die Übermittlung aller Eintragsänderungen an die Sicherheitsbehörde um (siehe Abb. 2). Die Differenzierung zwischen zu aktualisierenden Daten und irrelevanten, unverzüglich zu löschenden Änderungen wird somit der Sicherheitsbehörde überlassen. Die Offenlegung aller Eintragsänderungen geht durch die irrelevanten Änderungen über die beabsichtigte Funktionalität hinaus und ist, wie in Abschnitt 3 erläutert, mit signifikanten Risiken verbunden. Stattdessen ist das Verbergen irrelevanter Änderungen zugunsten der Datenminimierung erstrebenswert:

Anforderung 1: Eintragsänderungen zu der Sicherheitsbehörde unbekannten Personen dürfen der Sicherheitsbehörde nicht offenbart werden

Als Alternative ist theoretisch eine Umkehrung der Datenweitergabe nach § 13 Abs. 5 SBGG-RegE dergestalt denkbar, dass die Sicherheitsbehörde ihren Datenbestand an das Standesamt übermittelt, welches sodann zwischen relevanten und irrelevanten Daten differenziert, sodass nur die Schnittmenge mit relevantem Datenbestand der Sicherheitsbehörde mitgeteilt würde. Wenngleich dieser Ansatz Anforderung 1 erfüllen würde, erhielte das Standesamt nun ausführliches Wissen über den Datenbestand der Sicherheitsbehörden, was dem

Grundsatz der Datenminimierung widerspräche und behördliche Geheimhaltungsinteressen verletzte. Zudem ist fraglich, ob z.B. Standesämter über in solchen Fällen erforderliche technische Sicherheitsmaßnahmen zum Schutz der Behördendaten verfügen.

Anforderung 2: Der Datenbestand (oder Teile davon) der Sicherheitsbehörde darf anderen Behörden nicht offenbart werden

Unzureichend für die Erfüllung beider Anforderungen wäre es, die erforderlichen (Klar-)Daten an eine unabhängige dritte Partei zu übermitteln, welche die erforderliche Differenzierung vornimmt. Diese zusätzliche Partei wäre ein *Single Point of Failure*, durch den ein unbeabsichtigtes Datenleck oder z.B. interne oder externe Angriffe zur Offenlegung der Daten beider Parteien führen könnte.

5 Umsetzung mittels Multi-Party Computation

Eine datenschutzfreundliche Umsetzung der beabsichtigten Funktionalität sollte außer der geforderten Ausgabe an die Sicherheitsbehörde in Form der Liste von Eintragsänderungen zu in ihrem Datenbestand geführten Personen, keine weiteren Informationen offenbaren, also insb. Anforderungen 1 und 2 erfüllen. Während für den Kern der Funktionalität – die Bestimmung der Schnittmenge aller Eintragsänderungen und der Datenbestände – die Eingaben beider Parteien notwendig sind, müssen diese nicht notwendigerweise einer Partei im Klartext vorliegen. Stattdessen bietet sich Multi-Party Computation, kurz MPC, an, welche mittels kryptographischer Techniken beiden Parteien ohne direkten Austausch ihrer Eingabedaten die sichere Berechnung der Funktionalität erlaubt [vgl. z.B. Li20]. Präziser handelt es sich hier um eine Variante von Private Set Intersection (PSI) zur Berechnung von Schnittmengen [vgl. z.B. MAL23]. MPC und PSI erfüllen nicht nur die vorherigen Anforderungen, sondern garantieren allgemeiner, dass neben den durch die Funktionalität selbst definierten Ausgaben (vgl. Abb. 1), also der für die Sicherheitsbehörde bestimmten Schnittmenge aus Eintragsänderungen und Registereinträgen, keiner Partei die Ermittlung jedweder zusätzlicher Informationen ermöglicht wird.

Im Folgenden wird zunächst das Anwendungsspektrum von PSI und MPC im Allgemeinen erläutert. Weiterhin werden sowohl die Sicherheitsgarantien als auch die Limitierungen von MPC elaboriert und schlussendlich die Nutzung von PSI spezifisch für den behördlichen Datenabgleich in Bezug auf das SBGG diskutiert.

5.1 Anwendungsbeispiele von Private Set Intersection

PSI ist seit über 20 Jahren Thema akademischer Arbeiten und kommt in der Praxis mittlerweile auch auf Endgeräten zum Einsatz. Ein prominentes Beispiel dafür sind Komponenten in den Browsern Safari und Chrome, welche Nutzer*innen warnen, wenn ihre genutzten Passwörter von Datenlecks betroffen sind [Ap21; Ne19]. Auch im Behördenumfeld wurde bereits in Kollaboration mit der Polizei Hamburg an der Nutzung von PSI geforscht [Tr22]. Hierdurch können zwei Sicherheitsbehörden mittels PSI bestimmen, welche Personen sich in den Datenbeständen beider Behörden befinden, um anschließend im Falle ausreichender rechtlicher Grundlage weitere Daten zu diesen Personen auszutauschen.

5.2 Multi-Party Computation im Allgemeinen

PSI und deren Praxisanwendungen sind Beispiele für MPC, jedoch ist MPC selbst ein deutlich allgemeinerer Ansatz, welcher auch zur datenschutzfreundlichen Verarbeitung von verteilten Daten in zahlreichen anderen Anwendungsszenarien genutzt werden kann. MPC kann wie folgt beschriebene Probleme zwischen n miteinander kommunizierenden Parteien lösen:

- Partei 1 hat private Daten x_1, Partei 2 hat private Daten x_2, usw.
- Alle Parteien kennen eine gemeinsame zu berechnende Funktionalität F, formalisiert als $(y_1, \ldots, y_n) = F(x_1, \ldots, x_n)$
- Partei 1 soll die Ausgabe y_1 erhalten, Partei 2 Ausgabe y_2, usw.

MPC erlaubt, dass die Parteien die Funktionalität F gemeinsam so berechnen, dass Partei i neben ihrer eigenen Eingabe x_i und ihrer Ausgabe y_i keine weiteren Informationen erhält, insb. also außer indirekt durch y_i kein Wissen über die Eingaben anderer Parteien. Jede im Klartext effizient berechenbare Funktionalität F kann auch in MPC sicher berechnet werden [BGW88; GMW87; Ya86]. Klassisches PSI beschreibt den Fall, in welchem zwei Parteien Mengen X und Y vorliegen und i.d.R. die zweite Partei die Schnittmenge erfahren soll. Die berechnete Funktionalität ist also $F(X, Y) = (\varepsilon, X \cap Y)$, wobei $\cap$ der Schnittmengenoperator und ε die leere Ausgabe ist. Diese Basisfunktionalität kann jedoch beliebig erweitert werden.

5.3 Sicherheit von Multi-Party Computation

Ein naheliegender erster Ansatz für PSI ist, dass beide Parteien zunächst Hashwerte ihrer Datensätze bestimmen und dann diese statt den Datensätzen selbst austauschen. Hierbei ist eine sogenannte kryptographische Hashfunktion notwendig, die als Einwegfunktion genutzt werden kann, d.h., dass das Berechnen des ursprünglichen Werts aus einem gegebenen Hashwert nicht effektiv möglich ist. Eine solche Lösung ist jedoch keinesfalls eine sichere Lösung für MPC/PSI. Sicherheitsbehörden würden immer noch Informationen über die Hashwerte zu ihnen unbekannten Personen erhalten. Diese erlauben, im Nachhinein für andere Personen Hashwerte zu berechnen und diese mit den empfangenen Hashwerten zu vergleichen, um einige oder alle ursprünglichen Eingaben des Standesamtes zu rekonstruieren. Ein Testen für alle möglichen Namen ist bspw. zwar mit einem gewissen Aufwand verbunden, jedoch ist dieser durch die begrenzte Menge möglicher Namen deutlich zu gering, um die Sicherheit des Systems zu gewährleisten. Derartige Handlungen könnten zwar ein verbotenes und bußgeldbewehrtes Ausforschen i.S.d. § 13 Abs. 1, 14 SBGG darstellen, dies schließt entsprechende Risiken aber nicht aus.

Die Sicherheit von MPC ist stattdessen als *ideale* Umsetzung der angestrebten Funktionalität definiert, bei welcher die Parteien außer ihren eigenen Ein- und Ausgaben keine weiteren Informationen wie z.B. Eingaben anderer Parteien und Zwischenergebnisse erfahren können. MPC kann also als eine Black-Box beschrieben werden, in der die gesamte Berechnung stattfindet und die sämtliche intern verwendeten Daten verbirgt. Die Sicherheit wird formal

auf Grundlage von in der Kryptographie etablierter und langjährig bewährter Grundannahmen bewiesen. Zwar erfordert MPC Kommunikation zwischen den verschiedenen Parteien, jedoch sind die von einer Partei empfangenen Daten praktisch zufällig oder verschlüsselt (ohne dass die Partei einen entsprechenden Schlüssel zur Entschlüsselung erhält). Damit sind die Daten für diese Partei wertlos mit Ausnahme der zu bestimmenden Ausgabe, die der Partei zur Verfügung stehen soll. Eine solche Interaktion in Bezug auf den hier behandelten behördlichen Datenaustausch durch PSI ist in Abb. 3 illustriert. Durch die Sicherheit von MPC ist insb. die Sicherheitsbehörde nicht in der Lage, aus ihrem eigenen Datenbestand temporärer Artefakte der Berechnung, empfangener Nachrichten usw. jedwedes neues Wissen außer den für sie relevanten Eintragsänderungen zu erfahren. Insb. verhindert MPC, dass wie durch § 13 Abs. 5 SBGG-RegE geplant (siehe auch Abb. 2) zusätzliche Daten zwischenzeitig anfallen und dann ordnungsgemäß gelöscht werden müssen.

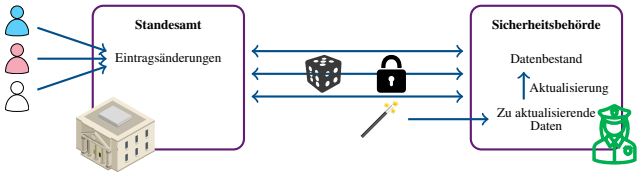

Abb. 3: Sichere, datenschutzfreundliche Umsetzung der Funktionalität durch MPC

5.4 Limitierungen von Multi-Party Computation

Eine zentrale Limitierung von MPC ist deren potenziell höhere Komplexität als die einer Datenverarbeitung wie in § 13 Abs. 5 SBGG-RegE. Dies führt zu höherem Rechen- und Kommunikationsaufwand und dadurch langsamere Berechnung und höherem Aufwand zur Implementierung eines solchen Systems. Jedoch existieren bereits akuelle Lösungen für PSI, die selbst für Millionen von Einträgen innerhalb weniger Minuten die private Schnittmenge bestimmen können [MAL23].

Eine weitere Limitierung betrifft die Sicherheitsdefinition selbst. MPC berechnet sicher die gewählte Funktionalität, offenbart also nicht mehr, als durch die Funktionalität explizit definiert. Damit kann die Funktionalität selbst zum Risiko werden, wenn sie nicht sorgsam gewählt ist. MPC schützt den Prozess der Berechnung. Unabhängig davon muss aber betrachtet werden, welche Risiken durch die gewünschte Ausgabe der Funktionalität selbst bestehen, da diese durch ihre Abhängigkeit von den Eingaben auch gewisse Rückschlüsse auf diese erlaubt. Zusätzlich erlaubt MPC den Parteien, beliebige private Eingaben zu liefern. Die Nutzung von PSI für den behördlichen Datenaustausch nimmt etwa an, dass die Sicherheitsbehörde ihren Datenbestand als Eingabe liefert, aber hindert diese nicht daran, stattdessen z.B. zusätzliche Personen ihrer Eingabe hinzuzufügen. Dies kann nicht durch kryptographische Mittel allein verhindert werden.

Auch kann die Datenminimierung durch MPC zu einer schlechteren Nachvollziehbarkeit und Prüfbarkeit des Systems führen, da bspw. Zwischenergebnisse zu keinem Zeitpunkt preisgegeben werden. Zuletzt sind Fehler in den formalen Sicherheitsbeweisen, aber vor allem in der

Implementierung der formalen MPC-Lösung möglich. Speziell die Implementierung und der spätere Betrieb eines entsprechenden Systems können wie in allen digitalen Systemen durch menschliche und technische Fehler zusätzliche Sicherheitsprobleme hervorrufen.

5.5 Überlegungen zur Anwendung für behördlichen Datenabgleich

PSI bestimmt zunächst lediglich die Schnittmenge, also die Menge genau übereinstimmender Einträge. Für eine Nutzung zum behördlichen Datenabgleich reicht dies jedoch nicht aus. Es ist anzunehmen, dass sich Datensätze in einen zur Identifikation der Person relevanten Teil und weitere zusätzlichen Daten aufteilen lassen. Bei Namensänderungen nach dem SBGG wäre als identifizierender Teil u.a. der vorherige Name ausschlaggebend, um mit alten Einträgen in den Registern der Sicherheitsbehörden verglichen zu werden, während den Sicherheitsbehörden im Falle einer Übereinstimmung zusätzlich der korrespondierende neue Name mitgeteilt werden sollte. Dies ist entsprechend bei der Formulierung der exakten Funktionalität zu berücksichtigen wie z.B. bereits in ähnlichen Arbeiten [Tr22]. Weiterhin sollte *Fuzzy PSI* [Uz21] genutzt werden, um Fehler, Unvollständigkeit oder Ungenauigkeiten in den vorhandenen Daten, insb. der Datenbestände der Sicherheitsbehörden, zu kompensieren, indem neben exakten Übereinstimmungen auch ähnliche Einträge erkannt werden.

Die beabsichtigte Funktionalität bietet jedoch auch ein nicht unerhebliches Missbrauchspotential: Die Sicherheitsbehörden werden über Eintragsänderungen zu allen Personen informiert, zu denen sie selbst Daten als Eingabe liefern, welche grundsätzlich aus ihrem Datenbestand stammen sollten. Jedoch hindert MPC Sicherheitsbehörden nicht daran, Daten zu weiteren Personen als Teil ihres Datenbestandes zu deklarieren, um somit etwaige Eintragsänderungen zu erfahren. Derartige Risiken sind nicht neu, bspw. sind innerbehördliche Datenabfragen zu Einzelpersonen abseits der behördlichen Aufgaben dokumentiert [Be19]. Ein automatisierter Prozess mittels MPC verstärkt das Risiko jedoch durch seine höhere Skalierbarkeit. Weiterhin legen Sicherheitsbehörden nicht mehr gegenüber einer anderen Behörde ihre Anfrage im Klartext vor, womit eben genau die zuvor formulierte datenschutzbezogene Anforderung 2 das Entdecken oder Prüfen auf solch unrechtmäßige Nutzung erschwert.

Hier bieten sich einige Sicherheitsvorkehrungen an, welche das Missbrauchspotential lindern, aber nicht vollständig beseitigen können. Kontrollierbar ist dies nur auf Seite der Sicherheitsbehörde, womit dort adäquate weitere Maßnahmen getroffen werden sollten. Zuletzt ist zugunsten der Prüfbarkeit von Seiten der meldenden Behörde, jedoch zulasten von Anforderung 2 auch möglich, dass lediglich die Schnittmenge bestimmt wird, aber die Sicherheitsbehörde keine assoziierten neuen Einträge erhält, sondern mittels der reinen Schnittmenge nur erfährt, welche Daten sich geändert haben. Diese könnte die Behörde dann in einem zweiten Schritt manuell anfragen, womit der Prozess besser überprüfbar wäre, zeitgleich aber die Schnittmenge durch die Anfragen auch der anderen Seite offenbaren würde. Somit würde Anforderung 2 zugunsten der Überprüfbarkeit teilweise verletzt, was umgekehrt ein signifikantes Missbrauchsrisiko auf Seiten der Standesämter bedeutet. Insb. in ländlichen Gebieten gehören

Behörden wie etwa Standesämter zum sozialen Nahbereich der Bevölkerung, in welchem eine Verbreitung von ursprünglich dienstlich erlangten Informationen ungeachtet gesetzlicher oder vertraglicher Verschwiegenheitspflichten ein immenses Risiko darstellen kann.

6 Fazit

Die vorliegende Untersuchung zeigt, dass eine Übermittlung von Änderungen behördlicher Datenbestände im Lichte berechtigter staatlicher Ordnungsinteressen dann geboten sein kann, wenn bereits bestehende Einträge in Datenbeständen korrigiert werden müssen. Eine pauschale und anlasslose Übermittlung steht jedoch nicht im Einklang insb. mit gesetzlich vorgeschriebenen Grundsätzen der Datenverarbeitung, weil die Mitteilungen über Namensänderungen nicht immer auf die Personen beschränkt werden können, die für die jeweilige Zielbehörde relevant sind. Einzelabfragen der Behörden mit unrichtig gewordenem Datenbestand bei den Meldebehörden stellen ebenfalls ein datenschutzrechtliches Problem dar und sind somit keine Alternative zur pauschalen Übermittlung.

Ein Ausweg aus diesem Dilemma kann jedoch durch technische Lösungen erreicht werden. MPC kann dabei für den behördlichen Abgleich sensibler Daten genutzt werden, um mittels moderner Kryptographie die einander offengelegten Daten auf solche zu reduzieren, die für die Aufgabenerfüllung der Behörden erforderlich sind. Die Identität von der Zielbehörde unbekannten Personen wird zu keinem Zeitpunkt offenbart. Ein Kompromiss, bzw. ein Interessenausgleich, zwischen den Ordnungsinteressen des Staates und Datenrichtigkeit gegenüber dem Interesse der Bevölkerung an Privatsphäre und Datenminimierung ist somit möglich.

Ob ein Datenaustausch überhaupt stattfindet, ist zuvorderst eine Entscheidung des Gesetzgebers, der die legitimen Interessen des Staates schützen darf. Dabei hat er verfassungsrechtliche Grenzen zu wahren, insb. den Grundsatz der Verhältnismäßigkeit. In diesem Rahmen sind mildere Mittel, etwa technische Alternativen, wie das in diesem Beitrag vorgeschlagene MPC, zumindest zu erproben.

Es verbliebe - trotz des Einsatzes von Maßnahmen wie MPC - ein Restrisiko: Unterstellt, Datenabgleiche würden auf diese Weise durchgeführt, kann dennoch nicht vollständig verhindert werden, dass Behördenpersonal nachvollziehbare Änderungen im Datenbestand unrechtmäßig nutzt. Es sind langfristig auch gesamtgesellschaftliche Maßnahmen wie Aufklärung und Diskurs auszuschöpfen, um Diskriminierung jeglicher Art entgegenzuwirken.

Danksagung

Diese Arbeit wurde durch die Deutsche Forschungsgemeinschaft (DFG) im Rahmen des GRK 2050 Privacy & Trust/251805230 gefördert. Sie wurde mitgefördert durch die DFG über den SFB 1119 CROSSING/236615297 und den Europäischen Forschungsrat über das Horizon 2020 EU-Förderprogramm (Fördervereinbarung Nr. 850990 PSOTI).

Literaturverzeichnis

[Ap21] Apple Support: Passwortüberwachung, 2021, URL: https://support.apple.com/de-de/guide/security/sec78e79fc3b/web, Stand: 24. 04. 2024.

[Be19] v. Bebenburg, P.: Polizisten missbrauchen Personenabfrage, um an Infos über Helene Fischer zu kommen. Frankfurter Rundschau 03.08.2019, 2019, URL: https://www.fr.de/hessen/hessen-beamte-missbrauchen-polizeisystem-infos-ueber-helene-fischer-kommen-zr-12875917.html, Stand: 25. 04. 2024.

[Be24] Bensmann, M.; von Daniels, J.; Dowideit, A.; Peters, J.; Keller, G.: Geheimplan gegen Deutschland. Correctiv 10.01.2024, 2024, URL: https://correctiv.org/aktuelles/neue-rechte/2024/01/10/geheimplan-remigration-vertreibung-afd-rechtsextreme-novembertreffen/, Stand: 03. 03. 2024.

[BfDI23] Stellungnahme des BfDI zum SBGG-E, 2023, URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Selbstbestimmung-Geschlechtseintrag.pdf?__blob=publicationFile&v=2, Stand: 17. 04. 2024.

[BGW88] Ben-Or, M.; Goldwasser, S.; Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. Association for Computing Machinery, S. 1–10, 1988.

[BT23] BT-Drs. 20/9049, 2023, URL: https://dserver.bundestag.de/btd/20/090/2009049.pdf, Stand: 29. 04. 2024.

[BT24] BT-Drs. 20/11004 (el. Vorabfassung), 2024, URL: https://dserver.bundestag.de/btd/20/110/2011004.pdf, Stand: 29. 04. 2024.

[BT96] BT-Drs. 13/4709, 1996, URL: https://dserver.bundestag.de/btd/13/047/1304709.pdf, Stand: 03. 05. 2024.

[Eu14] EuGH: C-131/12 – Google Spain. In: NJW. 2257, C. H. Beck, 2014.

[Fr21] Frenzel, E. M.: DS-GVO Art. 5. In: Paal, B. P.; Pauly, D. A. (Hrsg.): Datenschutz-Grundverordnung. 3. Aufl., C. H. Beck, 2021.

[GMW87] Goldreich, O.; Micali, S.; Wigderson, A.: How to play ANY mental game. In: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing. Association for Computing Machinery, S. 218–229, 1987.

[HT23] Hallweger, K.; Thümmler, R.: Die Beleidigungsstrafbarkeit des sogenannten Deadnamings – Eine Untersuchung de lege lata. In: NStZ. 76, C. H. Beck, 2023.

[Kl22] Klein, J.: Bundesstaat mit Verfolgungseifer, Texanische Transgender-Jagd. Queer.de 21.12.2022, 2022, URL: https://www.queer.de/detail.php?article_id=44158, Stand: 18. 04. 2024.

[Kö23] Köver, C.: Selbstbestimmungsgesetz, Unter Generalverdacht. netzpolitik.org 30.08.2023, 2023, URL: https://netzpolitik.org/2023/selbstbestimmungsgesetz-unter-generalverdacht/, Stand: 17. 04. 2024.

[Li20] Lindell, Y.: Secure Multiparty Computation. Commun. ACM 64 (1), S. 86–96, 2020.

[MAL23] Morales, D.; Agudo, I.; Lopez, J.: Private set intersection: A systematic literature review. Computer Science Review 49, 2023.

[Ne19] Nepper, P.; Nair, K. C.; Sukhanov, V.; Khaneja, V.: Better password protections in Chrome - How it works. Google Security Blog 10.12.2019, 2019, URL: https://security.googleblog.com/2019/12/better-password-protections-in-chrome.html, Stand: 24. 04. 2024.

[Ro19] Roßnagel, A.: DSGVO Art. 5. In: Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I. (Hrsg.): Datenschutzrecht. 1. Aufl., Nomos, 2019.

[Sl24] Slawik, N.: Redebeitrag von Nyke Slawik zur Abstimmung über das SBGG am 12.04.2024, 2024, URL: https://www.gruene-bundestag.de/parlament/bundestagsreden/selbstbestimmung-3, Stand: 17. 04. 2024.

[SZ24] Zahl der queerfeindlichen Straftaten in Bayern verdoppelt. Süddeutsche Zeitung 10.04.2024, 2024, URL: https://www.sueddeutsche.de/bayern/queer-angriffe-straftaten-bayern-genderverbot-sexualitaet-gewalt-1.6538090, Stand: 18. 04. 2024.

[Tr22] Treiber, A.; Müllmann, D.; Schneider, T.; Spiecker genannt Döhmann, I.: Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies. In: Proceedings of the 21st Workshop on Privacy in the Electronic Society. Association for Computing Machinery, S. 69–82, 2022.

[Uz21] Uzun, E.; Chung, S. P.; Kolesnikov, V.; Boldyreva, A.; Lee, W.: Fuzzy Labeled Private Set Intersection with Applications to Private Real-Time Biometric Search. In: USENIX Security Symposium. 2021.

[Ve] VelsPol e.V.: Geschichte der Rosa Listen, o. J. URL: https://www.velspol-nrw.de/html/rosa-listen.html, Stand: 09. 07. 2024.

[Ya86] Yao, A. C.-C.: How to generate and exchange secrets. In: 27th Annual Symposium on Foundations of Computer Science. S. 162–167, 1986.