Teil 3: Landesbericht USA

A. Der verfassungsrechtliche Datenschutz

I. Privacy Protection und Datenschutz

1. Privacy Protection

Das Recht auf *privacy* ist in der US-Verfassung nicht ausdrücklich als ein Recht genannt. Der Begriff „privacy" ist insgesamt schwer zu definieren, da seine Bedeutung vielfach je nach Kontext und der Art und Weise des Gebrauchs variiert und dadurch vage ist.[319] In vielen Ansätzen wurde ver-

---

319 Während die Bedeutung des Begriffs der *privacy* wie oben angeführt relativ vage ist, hat der Begriff der Privatsphäre in der deutschen Rechtsordnung eine auf die verschiedenen Rechtsgebiete übergreifende, relativ einheitliche Bedeutung. Der Begriff der *privacy* wurde durch die Rechtsprechung entwickelt, nachdem Gerichte auf der Ebene des Bundesstaaten *four privacy torts* im Deliktsrecht anerkannt haben: (1) *Intrusion upon Seclusion* (Restatement (Second) of Torts § 652B (1977), this tort allows plaintiffs to seek remedy for the invasion of their „solitude or seclusion" or „private affairs or concerns" if the intrusion is „highly offensive to a reasonable person"); (2) *False Light* (Restatement (Second) of Torts § 652E (1977), this tort allows plaintiffs to seek remedy when they are portrayed in a false light that is „highly offensive to a reasonable person" because the defendant publicly disclosed certain matters or information); (3) *Public Disclosure of Private Facts* (Restatement (Second) of Torts § 652D (1977), this tort allows plaintiffs to seek remedy for the disclosure of a private fact that is „highly offensive to a reasonable person" and not about a matter of public concern); and (4) *Appropriation* (Restatement (Second) of Torts § 652C (1977), this tort allows plaintiffs to seek remedy when their „name or likeness" is appropriated for the defendant's „use of benefit"). Das Restatement of (Second) of Torts versteht unter dem Recht auf *privacy* das Interesse des Einzelnen an der Abgeschiedenheit (unreasonable intrusion upon the seclusion of another) und der Vermeidung der Verwendung seines Namens o. Ä. (appropriation of the other's name or likeness), der unbegründeten Publizität seines privaten Lebens (unreasonable publicity given to the other's private life) sowie der Publizität, die ihn unbegründet in ein falsches Licht der Öffentlichkeit stellt (publicity that unreasonably places the other in a false light before the public). Obwohl die frühzeitige Erfassung des Begriffs der *privacy* durch den US-amerikanischen Obersten Gerichtshof (U. S. Supreme Court) dem Begriff „Privatsphäre" in der deutschen Rechtsordnung nicht zu entsprechen scheint und auch keine Ähn-

sucht, die Bedeutung von *privacy* zu definieren. Ein Entwurf der *privacy* beruhte auf dem „Recht, in Ruhe gelassen zu werden (*the right to be let alone*)", das in der von Richter *Cooley* im Jahr 1880 im Rahmen des Deliktsrechts veröffentlichten Abhandlung formuliert wurde. Zu dieser Zeit wurde der Ausdruck des Rechts auf *privacy* aber noch nicht unmittelbar benutzt.[320] Anlass zu erneuten heftigen Diskussionen um das Thema gab der Aufsatz *The Right to Privacy*,[321] den Samuel D. Warren und Louis D. Brandeis 1890 veröffentlichten. In diesem Aufsatz wird das Thema folgendermaßen erörtert: „Jedem stehen die Sphären von Gedanken, Meinungen und Gefühlen zu, die dann in dem gleichen Maße wie bei Körperverletzungen verletzt werden, wenn seine persönlichen Angelegenheiten öffentlich bekannt gegeben werden."[322]

Der Supreme Court führte in seiner *Griswold v. Connecticut*-Entscheidung aus, dass das Recht auf *privacy* in den Penumbras und Emanationen anderer verfassungsmäßiger Schutzmaßnahmen zu finden sei, wie etwa der Selbstbelastungsklausel des fünften Verfassungszusatzes, obwohl die *Bill of Rights* den Begriff der *privacy* nicht explizit erwähnt. Damit entschied das Gericht, dass die US-Verfassung durch die *Bill of Rights* ein Grundrecht auf *privacy* beinhaltet.[323] Die Rechte, die aus diesen von der Entsprechung als

---

lichkeit zur Idee der informationellen Selbstbestimmung oder dem Datenschutz besteht, scheint die Übersetzung von „privacy" mit „Privatsphäre" deshalb zutreffend zu sein, weil das *Restatement of Torts* den Begriff der *privacy* so ähnlich fasst wie der Begriff „"Privatsphäre" im deutschen Recht verwendet wird und weil die Erfassung des Supreme Courts mit der Zeit erweitert wird und sogar „Information Privacy" im Kontext der *privacy* diskutiert wird.

320 *Cooley*, A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract, 2nd ed., 1888: "The right to one's person may be said to be a right of complete immunity: to be let alone."

321 *Warren/Brandeis*, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5., 1890, 193.

322 *Warren/Brandeis*, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5., 1890, 193, 205: "These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed."

323 Der US-amerikanische Supreme Court hat erst in der *Griswold*-Entscheidung anerkannt, dass sich das verfassungsrechtliche Recht auf *privacy* im Halbschatten (Penumbra) und der Ausstrahlung (Emanation) einiger Verfassungszusätze – Art. 1, 3, 4, 5 und 9 – befindet (Griswold v. Connecticut, 381 U. S. 479 (484)).

Ursprung für die *privacy* genannten Verfassungszusätzen erfasst werden, stehen im Hinblick auf den bedeutenden und umfassenden Schutz der *privacy* jedoch weitaus stärker hinter den Rechten des vierten Verfassungszusatzes zurück und bieten somit keinen allgemein verbindlichen und verlässlichen Schutz. Es soll daher bei der Untersuchung des Privatsphären- und Datenschutzes der vierte Verfassungszusatz im Vordergrund stehen, der ein staatliches Organ dazu ermächtigt, den Lebensraum des Einzelnen zu durchsuchen und seine Sachen in Beschlag zu nehmen. In der *Boyd v. United States*-Entscheidung brachte der Supreme Court den vierten Verfassungszusatz und das Recht auf *privacy* in einen unmittelbaren Zusammenhang.[324] Der vierte Verfassungszusatz wurde eigentlich in Verbindung mit der Due-process-Anforderung des fünften Verfassungszusatzes berücksichtigt.[325] Der grundsätzliche Schutz gegen die staatliche rechtswidrige Nutzung der Technik stammt also aus dem vierten Verfassungszusatz, der dem Schutz des Einzelnen gegen unbegründete Durchsuchungen und Beschlagnahmungen dient.

Das Recht auf *privacy* wird von der Rechtsprechung im Kontext des vierten Verfassungszusatzes zunehmend erweitert anerkannt und steht damit in einer Konkretisierung seiner Konturen. Der Verfasser des vierten Verfassungszusatzes interessierte sich primär für die körperlichen Durchsuchungen von Personen, Häusern, Papieren und Vermögenswerten.[326] Dement-

---

324 *De Busser*, Data Protection in EU und USA Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities, S. 223; Boyd v. United States, 116 U. S. 616 (630): "constitutional liberty and security apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence."

325 Das erklärte der Richter Joseph P. Bradley in der *Boyd v. United States*- Entscheidung: "They throw great light on each other. For the 'unreasonable searches and seizures' condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man 'in a criminal case to be a witness against himself', which is condemned in the fifth amendment, throws light on the question as to what is an 'unreasonable search and seizure' within the meaning of the fourth amendment." (Boyd v. United States, 116 U. S. 616 (633)).

326 Drapper v. United States, 358 U. S. 307.

sprechend entschied der Supreme Court im *Olmstead*-Fall,[327] in dem es um die Verfassungskonformität staatlicher Abhörmaßnahmen bei privaten Fernsprechern ging, dass eine immaterielle Abhörmaßnahme nicht unter den Schutzgegenstand des vierten Verfassungszusatzes fällt. *Brandeis* äußerte eine hiervon abweichende Meinung und betonte, dass der Schutz der *privacy* auch bezüglich immateriellen Maßnahmen besteht.[328] Beispielsweise werden Wohnungen als wichtige private Lebensräume beim Privatsphärenschutz verfassungsrechtlich geschützt. Der Schutz des Lebensraums, der unter dem Privatsphärenschutz von großer Bedeutung ist, wurde zu Beginn lediglich am Maßstab eines unbegründeten physischen Betretens eines privaten Lebensraums im Kontext des vierten Verfassungszusatzes gemessen. Zum Lebensraum gehören Wohnungen, Büros oder auch Hotelzimmer.[329] Die Erfassung der Begriffe „unbegründete Eingriffe" und „privater Raum" durch die Rechtsprechung erfährt eine allmähliche Änderung. Den Zugriff auf Informationen innerhalb eines verfassungsrechtlich geschützten Lebensraums rechtfertigt ausschließlich eine gerichtliche Anordnung, eine Einwilligung eines Betroffenen oder bestimmte Umstände wie ein dringender Fall. Der Schutz des Brief-, Post- sowie Fernmeldegeheimnisses wird gegen eine unbegründete Durchsuchung und Beschlagnahme im Kontext des vierten Verfassungszusatzes gewährt. Bis zu diesem Zeitpunkt war der Schutzgegenstand auf etwas Materielles und auf Räume beschränkt. Dem entspricht der *Olmstead*-Fall, in dem der Schutz deshalb verneint wurde, weil die Informationen, die bei einem Telefonanruf ausgetauscht werden, nichts Materielles sind und ein Strom von elektronischen Impulsen kein Raum ist.[330] Dem Supreme Court wurde die Gelegenheit gegeben, den *Ex Parte Jackson*-Fall[331] hierauf anzuwenden. Das hat er je-

327 Olmstead v. United States, 277 U. S. 438.

328 Olmstead v. United States, 277 U. S. 438 (478 f.): Brandeis äußerte die abweichende Meinung, dass der Verfassungsgeber Amerikaner in ihrem Glauben, ihren Gedanken und Gefühlen schützen wolle, dass das Recht, in Ruhe gelassen zu werden (*the right to be let alone*) das umfassendste und würdigste Recht sei und dass es sich bei allem unbegründeten staatlichen Eindringen in die Privatsphäre um die Verletzung des vierten Verfassungszusatzes handle, unbenommen der eingesetzten Mittel.

329 Katz v. United States, 389 U. S. 347 (359).

330 Olmstead v. United States, 277 U. S. 438.

331 Ex Parte Jackson, 96 U. S. 727 (733): "Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection. […] The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."

doch nicht getan. Nach der Entscheidung des Supreme Court würden die USA keine ähnliche Betreuung der telegraphischen oder telefonischen Mitteilung wie die der versandten versiegelten Briefe gewährleisten.[332] Die *Olmstead*-Entscheidung hat den Schutz der *privacy* im Sinne des vierten Verfassungszusatzes als streng materiellen Bereich verankert.

Demzufolge sah der Supreme Court ursprünglich nur im physischen Betreten des Raums einen Eingriff in den Raum und forderte damit den *due process* als einen Rechtfertigungsgrund, während er ein staatliches Handeln, das kein physisches Betreten ähnlich einer technisch unterstützten Beweiserhebung voraussetzt, ohne Einschränkungen erlaubte. Im *Olmstead*-Fall hat die Strafverfolgungsbehörde die Telefonleitung der Wohnungen und Arbeitsplätze von Verdächtigen überwacht und auf diese Weise einen Beweis gewonnen, der zur Verurteilung der Verdächtigen führte. Der Supreme Court erklärte das als keine verfassungswidrige Durchsuchung. Die gerichtliche Entscheidung gründete sich darauf, dass die Strafverfolgungsbehörde den verfassungsrechtlich geschützten Raum nicht physisch betreten hat und die Telefonleitung kein Teil der Wohnung oder des Büros sei.[333] Auch beim Diktaphon, mit dem ein gesprochener Text (einschließlich der Anrufe) innerhalb eines Raums ohne physisches Betreten aufgenommen und wiedergegeben werden kann, wird keine gerichtliche Anordnung zur Rechtfertigung gefordert.[334] Diese Logik führte in einem anderen Fall hingegen zu einer gegensätzlichen Schlussfolgerung. Im *Silvermann*-Fall entschied das Gericht, dass die Verwendung der *spike mike* ohne gerichtliche Anordnung einen unbegründeten Eingriff darstelle.[335] Denn die Polizisten seien in den verfassungsrechtlich geschützten Raum physisch eingetreten, indem sie das elektronische Gerät am Heizrohr der Wohnung des Angeklagten befestigten. Daraus lässt sich ableiten, dass das geschützte Rechtsgut nicht das Recht ist, vor staatlichen Eingriffen oder staatlicher Kenntnis über etwas, was in einer Wohnung geschieht, sicher zu sein, sondern der Raum als solcher.

Der Supreme Court war jedoch aus doppeltem Grund dazu gezwungen, seine Auffassung über den vierten Verfassungszusatz im Hinblick darauf zu ändern, was als verfassungsrechtlich geschützter Raum und als ein Ein-

---

332 Olmstead v. United States, 277 U. S. 438 (464).

333 Olmstead v. United States, 277 U. S. 438 (464 f.): Der Richter Taft führt aus, dass eine Abhörmaßnahme von elektronischen Informationen außerhalb eines privaten Raums dem Wesen nach etwas ganz Anderes als das physische Betreten eines Raums zum Zwecke einer Gesprächsabhörung sei.

334 Goldmann v. United States, 316 U. S. 129.

335 Silvermann v. United States, 365 U. S. 505.

griff darin angesehen werden soll: Da einerseits die Technik fortschreitet und der Staat in der Lage ist, auch ohne physisches Betreten in verfassungsrechtlich geschützte Sphären einzudringen, lässt sich die frühere gerichtliche Auffassung über den vierten Verfassungszusatz nicht mehr rechtfertigen. Andererseits wurde das verfassungsrechtliche Recht auf *privacy* vom Supreme Court ausdrücklich anerkannt[336] und verschiedene Ausprägungen der *privacy* wurden danach von der Rechtsprechung entwickelt.[337] Die Anerkennung des Rechts auf *privacy* durch den Supreme Court schuf eine neue Lage. Von der Rechtsprechung wurde nachfolgend konkretisiert und erweitert, was das Recht auf *privacy* umfasst.

Die Rechtsprechung, die sich beim Schutz des privaten Raums ursprünglich nur auf ein physisches Betreten des Raums durch staatliche Organe bezogen hatte, erfuhr in der *Katz*-Entscheidung eine wichtige Änderung. Das Gericht stimmte hier dem Widerspruch des Richters *Brandeis* in der *Olmstead*-Entscheidung[338] zu und stellte fest, dass der vierte Verfassungszusatz auch für das Abhören gilt. Der Richter *Harlan* etablierte in seiner zustimmenden Meinung im *Katz*-Urteil eine Überprüfung „der begründeten Erwartung auf *privacy*".[339] Der Supreme Court hat aus dem vierten Verfassungszusatz eine begrenzte Sphäre des verfassungsrechtlichen Schutzes des Rechts auf *privacy* abgeleitet: Das Recht auf *privacy* und Freiheit vor staatlichem Eindringen besteht überall dort, wo eine Person eine begründete Erwartung auf *privacy* (*reasonable expectation of privacy*) hat.[340] Ob es dabei ein physisches Betreten eines privaten Raums gibt, spielt keine bedeutende Rolle mehr. Der Supreme Court führte daher statt einer Prüfung eines physischen Betretens ein neues Kriterium ein: die begründete Erwartung auf *privacy*. Das Kriterium besteht aus zwei Teilen: zum einen aus einem subjektiven Teil, bei dem es darum geht, ob ein Einzelner eine Erwartung auf *privacy* hat *(personal agency)* und zum anderen aus einem objektiven Teil, wobei die Erwartung gesellschaftlich als begründet zu erkennen ist. In der *Katz*-Entscheidung hat *Katz* eine öffentliche Telefonkabine zum Glücksspielanruf benutzt, obwohl die Nutzung von Draht-Fernmeldeeinrichtungen zum Glücksspiel nach dem das *Federal*

336 Griswold v. Connecticut, 381 U. S. 479.
337 Das Kontrazeptionsrecht des Unverheirateten (Eisenstadt v. Baird, 405 U. S. 438), das Abtreibungsrecht (Roe v. Wade, 410 U. S. 113) und das Homosexualitätsrecht (Lawrence v. Texas, 539 U.S. 558) wurden als Ausprägungen des Rechts auf Privatsphäre bestätigt.
338 Zu seiner abweichenden Meinung siehe oben Fn. 328.
339 Katz v. United States, 389 U. S. 347 (360 f.).
340 Katz v. United States, 389 U. S. 347.

Statute verboten ist. Die Strafverfolgungsbehörde hatte an der Außenwand der Telefonkabine ein Abhörgerät befestigt, um Katz' Stimme beim Anruf aufzunehmen. Sie hatte so einen Beweis gewonnen, der zur Verurteilung von *Katz* führte. Die Behörde behauptete mit Verweis auf den *Olmstead*-Fall, dass es keine physische Beeinträchtigung gab und eine Telefonkabine deshalb keinen verfassungsrechtlich geschützten privaten Raum darstelle, weil ihre Nutzung von jedem wahrgenommen werden kann. Der Supreme Court lehnte die *Olmstead*-Entscheidung ab und entwarf eine neue Regelung, die besagt, dass der Einzelne das *Privacy*-Interesse im Kontext des vierten Verfassungszusatzes nicht in einem physischen Raum, sondern in der Geheimhaltung von bestimmten Informationen und Materialien hat. Nach dem Gericht waren das Schließen der Telefonkabinentür und die Bezahlung für den Anruf ausreichende Aktivitäten, um die Erwartung auf *privacy* zu begründen.[341] Die *Katz*-Entscheidung ist deshalb von Bedeutung, weil hierbei keine Unerreichbarkeit der Öffentlichkeit, sondern die begründete Erwartung auf Privatsphäre im Vordergrund steht und der Schutz des Rechts auf *privacy* damit nicht mehr von der räumlichen Sicht abhängt. Der vierte Verfassungszusatz bietet daher in dem Fall Schutz, in dem eine Person eine begründete Erwartung auf *privacy* hat. Er erfordert einen *warrant*, der durch einen *probable cause* gestützt wird, damit die Strafverfolgungsbehörden eine Durchsuchung durchführen können. Auf die Schutzgewährleistung durch den vierten Verfassungszusatz wirken einige Doktrinen ein, die seine Anwendung ausschließen können:

1. *Third Party Doctrine* – Wenn eine Person Informationen einmal an Dritte weitergibt, kann sie keine *privacy* für diese Informationen mehr erwarten.[342]
2. *Misplaced Trust Doctrine* – Eine Person hat keinen Schutz vor Verrat durch einen Informanten oder einen verdeckten Ermittler, da die Person die Verantwortung für die Gefahr des Verrats zu übernehmen hat.[343]
3. *Plain View Doctrine* – Wenn etwas als zwecklos betrachtet wird, handelt es sich nicht um eine Durchsuchung und löst keinen Schutz durch den vierten Verfassungszusatz aus.[344]

341 Katz v. United States, 389 U. S. 347 (361).
342 United States v. Miller, 425 U. S. 435 (*bank records*); Smith v. Maryland, 442 U. S. 735 (*phone numbers*).
343 Hoffa v. United States, 385 U. S. 293.
344 Harris v. United States, 390 U. S. 234.

4. *Special Needs Doctrine* – Unter bestimmten Umständen, nämlich in der Regel bei Durchsuchungen durch Staatsbeamte (z. B. Schulbeamte, Regierungsangestellte), die keine Strafverfolgungsbehörden sind, kann eine Durchsuchung nur *reasonable* sein.[345]

Der Supreme Court hat im Rahmen der objektiven Prüfung der begründeten Erwartung auf *privacy* die *Third-Party-Doctrine* angewendet, nach der die mit Dritten – wie Banken, Telefongesellschaften, Internet-Service-Providern (ISPs) und E-Mail-Servern – geteilten Informationen nicht mehr privat sind.[346] Die *Katz*-Prüfung findet auch in dem *Smith v. Maryland*-Fall Anwendung, in dem es um die Verwendung einer Technik (*Pen Register*) geht, die von Telefongesellschaften verwendet wird, um die von einem bestimmten Telefon gewählten Telefonnummern aufzuzeichnen. Das Gericht entschied, dass *Smith* einen Teil seiner *privacy* gegenüber der Telefondienstleistung preisgegeben hat. Es führte ferner aus, dass er zugunsten eines Briefversands auf das Telefon hätte verzichten müssen, wenn er seine Kommunikation hätte vollständig privat halten wollen.[347] Da es keine Möglichkeit gibt, die gewählten Telefonnummern selbstständig zu verschleiern und er sie mit Dritten geteilt hat, bestehe keine unbegründete Durchsuchung.[348] Hiernach zog der Supreme Court beim *Ciaolo*-Fall mit Hilfe der *Katz*-Prüfung den Schluss, dass einerseits alles, was von jedem wahrgenommen werden kann, mit der Öffentlichkeit geteilt wird und somit nicht privat sein könne und dass andererseits der Bau eines Zauns nicht genug sei, um eine Erwartung auf *privacy* zu schaffen.[349] Demzufolge wurde die begründete Erwartung auf *privacy* verneint.[350] Bei Müllsäcken, die am Straßenrand für die Abholung abgestellt wurden, wird die Erwartung auf *privacy* zwar festgestellt, sie ist jedoch unbegründet.[351] Denn laut

345 O'Connor v. Ortega, 480 U. S. 709.
346 Smith v. Maryland, 442 U. S. 735 (749).
347 Smith v. Maryland, 442 U. S. 735 (742).
348 Smith v. Maryland, 442 U. S. 735 (749): In einer abweichenden Meinung äußerte der Richter *Marshall* seine Ablehnung der bestehenden *Third-Party-Doctrine* des Gerichtshofs. Nach seiner Auffassung kann man seine Informationen mit einer, deshalb aber nicht notwendigerweise auch mit anderen Parteien teilen wollen.
349 California v. Ciaolo, 476 U. S. 207 (213).
350 California v. Ciaolo, 476 U. S. 207: Das Gericht begründet, dass etwas außerhalb der Wohnung, das von einem öffentlichen Raum mit dem bloßen Auge gesehen werden kann, nicht als private Information in Betracht kommt. Das Gericht behandelt leider nicht das Problem der technischen Maßnahme der polizeilichen Nutzung von *aircraft*.
351 California v. Greenwood, 486 U. S. 35 (40).

der *Third-Party-Doctrine* sind die Müllsäcke zum Zwecke der Abholung im Rahmen der Müllabfuhr in die Öffentlichkeit gestellt worden.[352]

Der technische Fortschritt führt wiederum zu einer wichtigen Änderung der *Katz*-Prüfung. Er macht es erforderlich, die Bedeutung des Ausdrucks der begründeten Erwartung auf *privacy* und des physischen Raums beim Schutz der *privacy* wieder abzuschwächen. Bezüglich des Einsatzes von Wärmebildkameras[353] wurde z. B. die Frage gestellt, ob der Einzelne eine bestimmte Tätigkeit ausüben kann, die eine Erwartung auf *privacy* schafft, auch wenn er die neuartige Überwachungstechnologie nicht kennt. Daraufhin hat der Supreme Court ein weiteres Kriterium vorgelegt: die Gewöhnlichkeit einer eingesetzten Technologie im Hinblick auf *personal agency*. Werden der Allgemeinheit unbekannte Geräte genutzt, um den verfassungsrechtlich geschützten Raum ohne physisches Betreten zu durchsuchen, macht die Nutzung dieser Geräte zu Zwecken einer Durchsuchung im Sinne des vierten Verfassungszusatzes eine gerichtliche Anordnung erforderlich. Das Gericht hebt hervor, dass im Kontext des vierten Verfassungszusatzes nicht die Fläche eines Raums geschützt wird, sondern eine staatliche Kenntnisnahme von etwas, was im Raum geschieht. Das Recht auf *privacy* sei eher das Recht, eine staatliche Kenntnisnahme zu verhindern, als das Recht, staatliches Eindringen ohne den *due process* zu vermeiden.[354]

Zusammenfassend lässt sich feststellen, dass ein privater Lebensraum verfassungsrechtlich zunächst gegen das physische Betreten des Raums durch staatliche Organe im Kontext des vierten Verfassungszusatzes geschützt wird. Dieser Schutz des Rechts auf *privacy* wurde durch die *Katz*-Prüfung erweitert und hängt nunmehr nicht ausschließlich von der räumlichen Sicht ab, sondern wird über die subjektive und die objektive Prüfung des Rechts festgelegt. Dies bedeutet, dass sich das Recht auf *privacy* vom Schutz eines Raums als solchem hin zum Schutz vor der staatlichen Kenntnisnahme von etwas, was im Raum geschieht, ändert. Außerdem wendet der Supreme Court nach der *Katz*-Entscheidung die *Third-Party-Doctrine* an, nach der die mit Dritten geteilten Informationen nicht mehr als privat angesehen werden. Darüber hinaus wurde mit der Rechtsprechung die Möglichkeit dafür eröffnet, den verfassungsrechtlich geschützten Raum gegen technikgestützte Maßnahmen zu sichern, wenn

352 California v. Greenwood, 486 U. S. 35 (40).
353 Kyllo v. United States, 533 U. S. 27.
354 Kyllo v. United States, 533 U. S. 27 (35 f.).

dieser Schutz außerdem noch davon abhängt, ob man sich an die eingesetzten technischen Mittel gewöhnt.

2. Die Bedeutung des Datenschutzes für die Privacy Protection

Das Datenschutzrecht und das allgemeine Persönlichkeitsrecht als Ursprung für das Datenschutzrecht firmieren weitestgehend gemeinsam unter dem allgemeinen *Privacy*-Begriff. Da es in den USA außerdem an verfassungsrechtlich ausdrücklichen, datenschützenden Regelungen mangelt, ist es erforderlich, das wenig ausdifferenzierte Recht auf *privacy* im Hinblick auf den Datenschutz zu untersuchen. Dabei erscheint es sinnvoll, den weiten Begriff der *privacy protection* auf eine Unterkategorie des Datenschutzes zu reduzieren und diesen zu untersuchen.

Nach zahlreichen Versuchen, den Begriff der *privacy* zu definieren, konnten die informationelle Privatheit, die Privatheit der Kommunikation und die körperliche Privatheit als Hauptelemente dieses Begriffs herausgefiltert werden.[355] Mit der Zeit begannen die Gerichte, sich neben dem verfassungsrechtlichen Privatsphärenschutz im Allgemeinen auch mit dem Recht auf informationelle Privatsphäre im Besonderen zu befassen.

Im Folgenden soll daher erörtert werden, ob und gegebenenfalls wie das Recht auf die informationelle Privatheit, nämlich die *privacy* im engeren Sinne im verfassungsrechtlichen Kontext – im Rahmen des Gesetzes- und Fallrechts zur vollständigen und ganzheitlichen Rechtsvergleichung[356] – geschützt wird.

3. Der verfassungsrechtliche Datenschutz

Der verfassungsrechtliche Schutz personenbezogener Daten, sprich der *privacy* im engeren Sinne, wird nach der *Katz*-Entscheidung mit dem Prüfungskriterium „begründete Erwartung auf *privacy*" in der Rechtsprechung diskutiert und entwickelt. In der *NAACP v. Alabama*-Entscheidung[357] er-

355 *Genz*, Datenschutz in Europa und den USA, S. 41.

356 Denn das US-amerikanische Rechtssystem basiert auf unterschiedlichen Rechtsquellen und der *Doktrin* des amerikanischen Richterrechts. Das sog. *common law* spielt dabei eine bedeutende Rolle. Daher könnte eine Nachforschung und Analyse von Rechtsprechungsveränderungen im Hinblick auf den Privatsphären- und Datenschutz von großer Bedeutung sein.

357 NAACP v. Alabama, 357 U. S. 449.

fuhr ein spezifischer Bereich der Datenverarbeitung einen frühen verfassungsrechtlichen Schutz.[358] Hier hat der Supreme Court positiv das Recht politischer Gruppen festgestellt, ihre Mitgliederlisten vor staatlichen Stellen geheim zu halten. Erst im Jahr 1976 beschäftigte sich der Supreme Court zum ersten Mal mit dem Schutz personenbezogener Daten als solcher.[359] Hierbei ging es darum, dass von der Polizei an mehr als 800 Einzelhändler Flyer verteilt wurden, auf denen der Name und das Foto einer Person zu sehen waren, die verhaftet, jedoch noch nicht für schuldig erklärt worden war. Der Supreme Court stellte in dieser Entscheidung fest, dass die verfassungsrechtlichen Grundsätze der *privacy* die Datenverbreitung mittels des amtlichen Handelns der Strafverfolgungsbehörden nicht eingrenzen. Das Gericht verneinte hierbei demnach, dass diese Daten eng mit der Persönlichkeit des Einzelnen zusammenhängen. Gemäß der Entscheidung seien die in Frage kommenden Informationen lediglich beschämender Natur, sodass der *due process* im Kontext des vierten Verfassungszusatzes nicht gefordert werde. Jedoch wurden unter dem Verweis auf die *Roe v. Wade*-Entscheidung[360] Leitlinien in Bezug darauf vorgelegt, welche Art von Informationen verfassungsrechtlich geschützt werden soll. Die Leitlinien lauten wie folgt:

1. Der Einzelne hat das Recht, die Offenlegung von persönlichen Angelegenheiten durch staatliche Behörden zu vermeiden.
2. Mit diesem Recht ist auf Seiten des Staates die Pflicht verbunden, die Informationen zu schützen, zu deren Preisgabe dieser den Einzelnen zwingt.
3. Die Informationen, die eng mit den *fundamental areas* verbunden sind, werden durch das Selbstbestimmungsrecht geschützt und rechtfertigen einen stärkeren Schutz des verfassungsrechtlichen Rechts auf informationelle Privatheit.

358 *Genz*, Datenschutz in Europa und den USA, S. 46.

359 Paul v. Davis, 424 U. S. 693.

360 Roe v. Wade, 410 U. S. 113: Das Gericht wies darauf hin, „dass sich die persönlichen Rechte in dieser Garantie der *privacy* darauf beschränken sollen, was fundamental oder implizit im Konzept der geordneten Freiheit sei". Nach der *Paul*-Entscheidung seien die detaillierten Aktivitäten, die unter diese Definition fallen, Angelegenheiten, die mit Ehe, Zeugung, Schwangerschaftsverhütung, Familienbeziehungen und Kindererziehung sowie -bildung im Zusammenhang stehen (Paul v. Davis, 424 U. S. 693 (713)).

Ein Jahr nach der *Paul v. Davis*-Entscheidung stellte der Supreme Court in seiner *Whalen v. Roe*-Entscheidung[361] fest, dass unter dem Recht, in Ruhe gelassen zu werden, das individuelle Interesse an einer Vermeidung der Offenlegung persönlicher Angelegenheiten zu verstehen sei. Im Rahmen dieser Feststellung erkannte der Supreme Court das Recht auf die informationelle Privatheit und den verfassungsrechtlichen Freiheitsschutz an. Die Verfassung erkenne demnach ein berechtigtes Interesse der *privacy* an sensiblen persönlichen Informationen an. Der Fall wurde vom Gericht verhandelt, damit die Verfassungskonformität des Landesgesetzes in New York überprüft werden kann. Nach dem Gesetz sollten die Rezepte eingebracht werden, in denen bestimmte von der Landesregierung als gefährlich eingeordnete Arzneimittel gelistet sind. Das Amtsgericht hatte festgestellt, dass das Gesetz unnötig in die Arzt-Patient-Beziehung eingreife, die als eine der verfassungsrechtlich schutzwürdigsten Zonen der *privacy* gilt.[362] Hierbei unterschied der Supreme Court zunächst zwischen Vertraulichkeits- und Selbstbestimmungsinteressen im Rahmen des Rechts auf informationelle Privatheit und entschied dann, dass das direkte Eingreifen des Landes New York in die Arzt-Patient-Beziehung keine Gefährdung des Selbstbestimmungsinteresses sei, da der Zugang zu Medikamenten nicht von der Zustimmung eines staatlichen Beamten oder sonstiger Dritter abhängt.[363] Eine Gefährdung der Vertraulichkeit wurde hingegen vom Gericht akzeptiert. Um solche Herausforderungen im Rahmen des Rechts auf informationelle Privatheit zu überwinden, wandte das Gericht einen Abwägungsansatz an.[364] Der Abwägung zwischen dem öffentlichen Interesse am Zugriff auf die personenbezogenen Daten als einem Teil der *privacy* und dem gefährdeten individuellen Interesse wurde eine Begleitungspflicht des Staates als eine neue Variable hinzugefügt.[365] Der Supreme Court erkannte hierbei zwar an, dass im *Privacy*-Schutz zwei unterschiedliche Interessen enthalten sind, nämlich zum einen das Interesse des Einzelnen an der Vermeidung der Bekanntmachung seiner persönlichen Angele-

361 Whalen v. Roe, 429 U. S. 589.
362 Roe v. Ingraham, 403 F. Supp. 931 (D. C. N. Y. 1975).
363 Whalen v. Roe, 429 U. S. 589 (598 f. und 602, 603).
364 Der Ansatz wurde seit der *Griswold v. Connecticut*-Entscheidung im Autonomie-Zweig der Privatsphäre verwendet, damit die Verfassungsmäßigkeit von Gesetzen entschieden wird, die eine selbstbestimmte Entscheidung verhindern.
365 Der Richter Stevens behauptet, „die Befugnis, Daten für die öffentlichen Zwecke zu sammeln und zu nutzen, ist in der Regel von einer gleichzeitigen gesetzlichen oder behördlichen Pflicht zur Vermeidung von unberechtigten Angaben begleitet" (Whalen v. Roe, 429 U. S. 589 (605)).

genheiten und zum anderen das Interesse an der Selbstbestimmung bei wichtigen Entscheidungen; das Gericht entschied jedoch, dass bei diesem Fall keine unbegründete Verletzung der beiden Interessen vorliegt. Denn soweit die Sicherheitsverfahren nach dem Gesetz eingehalten werden, sei die Möglichkeit der Bekanntmachung der gespeicherten Daten relativ gering. Auch die Ablehnung des Eingriffs in das Selbstbestimmungsrecht sei auf die Statistik über die Anzahl der ausgestellten Rezepte nach dem Inkrafttreten des Gesetzes gestützt.[366]

Kurz nach der *Whalen*-Entscheidung verfocht der frühere Präsident *Nixon* die Verfassungsverletzung des Presidential Recordings and Materials Preservation Act in der *Nixon*-Entscheidung. Nach dem Gesetz sollte die GSA (*General Services Administration*) alle Dokumente und Tonbänder während seiner Amtszeit als Präsident speichern. Der Kläger behauptete deshalb die Verletzung des Rechts auf *privacy*, da ein Teil der eingezogenen Dokumente sowie Tonbänder private Unterlagen darstelle, die das Amt keineswegs betreffen. Der Richter *Brennan* stellte fest, dass auch der frühere Präsident das verfassungsrechtliche Recht auf seine *privacy* beanspruchen konnte[367] und er eine legitime Erwartung auf *privacy* hatte.[368] Der Abwägungsansatz führte zu keiner Verletzung des Rechts auf Geheimhaltung der persönlichen Angelegenheiten, da das hier involvierte archivische Überprüfungsverfahren eher dem „wichtigen öffentlichen Interesse" und dem „wichtigen Staatsinteresse" und weniger dem Privatheitsinteresse diente.[369] Entsprechend der *Whalen*-Entscheidung sieht der Supreme Court das Interesse des Einzelnen an der Vermeidung der Bekanntmachung persönlicher Angelegenheiten als einen Teil der *privacy*. Das Interesse des Einzelnen habe bei diesem Fall einer Abwägung gegen das öffentliche Interesse an der Unterwerfung der präsidentiellen Materialien unter die archivalische Überprüfung bedurft. Der Gerichtshof ent-

366 Whalen v. Roe, 429 U. S. 589 (599 ff.).
367 Nixon v. Administrator of General Services, 433 U. S. 425 (457).
368 Nixon v. Administrator of General Services, 433 U. S. 425 (465).
369 Nixon v. Administrator of General Services, 433 U. S. 425 (464 ff.).

schied unter Berücksichtigung der gesetzlichen Sicherungsmaßnahme im Gesetz,[370] dass das öffentliche Interesse überwiege.[371]

Nach den Bewertungen der Circuit Courts hat der Supreme Court zwar deutlich gemacht, dass das Interesse des Einzelnen an der Vermeidung der Offenlegung persönlicher Angelegenheiten zum einen und zum anderen das Interesse an der Selbstbestimmung bei bedeutungstragenden Entscheidungen in der Verfassung wurzeln, er hat jedoch keine nachvollziehbaren Leitlinien vorgelegt, die bei Überprüfungen der mit der informationellen Privatheit in Zusammenhang stehenden Fälle anwendbar sind.[372] Die nachvollziehbaren Leitlinien werden eher von den Circuit Courts entwickelt. Wie der Supreme Court prüfen auch sie die Verfassungskonformität im Rahmen eines Eingriffs in persönliche Daten als solche mit Hilfe des Abwägungsansatzes.[373] Mit dem äußerst vagen Wegweiser des Supreme Court haben die Circuit Courts eine nützliche Abwägungsgleichung entwickelt, mit der Fälle lösbar sind, die die informationelle Privatheit betreffen. Werden ihre Entscheidungen zusammengefasst, kann die ähnlich angewandte Abwägungsgleichung so formuliert werden:[374]

> Individuelles Privatsphäreninteresse = (Informationstyp – Klägerkategorie) – staatliche Sicherungsmaßnahme

---

370 Siehe Nixon v. Administrator of General Services, 433 U. S. 425 (458 ff.): Der Richter *Brennan* erklärt, dass das Gesetz nicht nur Maßnahmen vorsieht, die darin bestehen, die übermäßige Verbreitung von privaten Materialien zu verhindern, sondern dass der Staat im Gegensatz zum *Whalen*-Fall eine langfristige Kontrolle über solche privaten Informationen nicht einmal behalten wird.

371 Bei einer abweichenden Meinung behauptet der Präsident des Supreme Court *Burger*, dass das öffentliche Interesse, das die Regierung genannt hat, aus Mangel an konkreten Zielsetzungen nicht mehr als ein generalisierter Bedarf sei und demnach das Interesse des Präsidenten an seiner Privatsphäre überwiege (Nixon v. Administrator of General Services, 433 U. S. 425 (528 ff.)).

372 So alle Circuit Courts außer dem 6. Circuit Court. Vgl. Barry v. City of New York, 712 F. 2d. 1554 (1559) (2nd Cir. 1983): Obwohl der Supreme Court anerkannte, dass das Recht des Einzelnen auf das Vermeiden der Bekanntmachung persönlicher Angelegenheiten seine Wurzeln in der Verfassung hat, bedauert der Richter *Wilfred Feinberg*, dass das Wesen und der Umfang des Interesses sowie die entsprechenden Prüfungsmaßstäbe für angebliche Verletzungen dieses Interesses nach wie vor unklar sind.

373 Vgl. Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978); Fadjo v. Coon, 633 F. 2d. 1172 (5th Cir. 1981); Barry v. City of New York, 712 F. 2d. 1554 (1559) (2nd Cir. 1983); Tavoulareas v. Washington Post, 724 F. 2d. 1010 (D. C. Cir. 1984).

374 *Kuhn*, Federal Dataveillance: Implications for Constitutional Privacy Protections, S. 130.

Individuelles Privatsphäreninteresse (>, <) staatliches Interesse an Informationen = Entscheidung

Auf den jeweiligen Informationstyp wird der Grundsatz angewendet, dass umso mehr Schutz gewährt wird, je enger die Informationen mit dem fundamentalen Interesse und mit dem Selbstbestimmungsrecht verbunden sind. Die Informationen, die der Staat nach einer Verabredung der Vertraulichkeit erhebt und sammelt – unabhängig davon, ob die Vertraulichkeit durch eine ausdrückliche Verabredung oder durch ein Gerichtsverfahren gesichert ist –, genießen meist hochgradigen Schutz.[375] Daneben sind die sexuelle Orientierung[376] und das Selbstbestimmungsrecht in Ehebeziehungen[377] oder homosexuellen Partnerschaften[378] dazu geeignet, höchsten Schutz zu gewähren. Medizinische Informationen werden hingegen unterschiedlich behandelt. Informationen, die z. B. mit einem Schwangerschaftsstatus[379] oder dem HIV-Status[380] im Zusammenhang stehen, werden als intime Informationen angesehen; der Schutz für die übrigen allgemeinen medizinischen Informationen wird dagegen abgelehnt, etwa wie die vom Gericht bestellte psychiatrische Beurteilung.[381] Die Circuit Courts gewähren den finanziellen Informationen einen mittelgradigen Schutz, da diese nicht eng genug mit fundamentalen familiären Interessen im Zusammenhang stünden.[382] Nach der *Paul*-Entscheidung wird der Einzelne nicht gegen die Offenlegung persönlicher Daten geschützt, wenn diese lediglich

375 S. Fadjo v. Coon, 633 F. 2d. 1172 (5th Cir. 1981); Tavoulareas v. Washington Post, 724 F. 2d. 1010 (D. C. Cir. 1984); James. v. City Douglas, 941 F. 2d. 1539 (11th Cir. 1991).

376 Sterling v. Borough of Minersville, 232 F. 3d. 190 (3rd Cir. 2000): In diesem Fall hatte sich ein Teenager umgebracht, nachdem die regionale Polizei ihm damit gedroht hatte, seinen Großeltern zu verraten, dass er homosexuell ist. Das Gericht stellte fest, dass selbst die einfache Bedrohung einen Verstoß gegen das Recht auf Privatsphäre darstellt („the essence of the right to privacy is in avoiding disclosure of personal matters", S. 197).

377 Griswold v. Connecticut, 381 U. S. 479.

378 Eisenstadt v. Baird, 405 U. S. 438.

379 Gruenke v. Seip, 225 F. 3d. 290 (3rd Cir. 2000).

380 Herring v. Keenan, 218 F. 3d. 1171 (10th Cir. 2000).

381 Borucki v. Ryan, 827 F. 2d. 836 (842) (1st Cir. 1987): Die Entscheidung beruht darauf, dass die Inhalte dieser Berichte keine intime Informationen darstellen: „the contents of such reports did not rise to the level of the more intimate information indicated in Paul and nor did the justification for protecting such a privacy interest reside in the penumbra of any specific amendment mentioned in Griswold."

382 Vgl. Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978); Barry v. City of New York, 712 F. 2d. 1554 (2nd Cir. 1983).

beschämender Natur sind.[383] Außerdem genießt das *Privacy*-Interesse an persönlichen Daten beim öffentlichen Eintrag, z. B. beim Verhaftungsdaten, den niedrigsten Schutz.[384] Der vierte Verfassungszusatz wurde sowohl auf personenbezogene Daten unter der Herrschaft Dritter als auch auf sog. Daten ohne Inhaltwie beispielsweise Telefonnummern als unanwendbar angesehen.[385]

Im Rahmen der sog. Klägerkategorie wird geprüft, ob eine bestimmte Qualität das individuelle Interesse schwächt, beispielsweise die mit Steuergeld verdiente[386] oder die ein öffentliches Vertrauen erfordernde Stellung[387] oder die Stellung als Gefangener.[388]

Bei einer staatlichen Sicherungsmaßnahme wird danach gefragt, ob (und wie) der Staat seine Pflicht erfüllt, die von ihm bestellten Informationen zu schützen. Je ausgeprägter die staatlichen Garantien in den Augen des Gerichts erscheinen, desto geringer ist das wahrgenommene Risiko. Das Gericht stellte fest, dass z. B. in der *Barry*-Entscheidung die Sicherungsmaßnahme bereits ausreichend sei, da das gesetzliche Verfahren den Mitarbeitern der Stadt eine Klagemöglichkeit eröffne, um bestimmte Typen von Informationen gegen die Offenlegung vor der Öffentlichkeit zu schützen.[389] Darüber hinaus sei der *coding process* für die erforderlichen Sicherungsmaßnahmen geeignet, um die Informationen von Patienten zu schützen.[390]

Das staatliche Interesse an Informationen als das letzte Element der Abwägungsgleichung teilt sich grob in drei Stufen: das berechtigte, das wesentliche und das zwingende Interesse. Ein berechtigtes Interesse kann die Prüfung bestehen und ein wesentliches Interesse wird unter der intermediären Prüfung gewährleistet, während ein zwingendes Interesse einer strikten Prüfung unterzogen werden soll. Je enger eine bestimmte Information mit fundamentalen Werten verbunden ist, desto zwingender

383 Siehe Alexander v. Peffer, 993 F. 2d. 1348 (8th Cir. 1993).
384 Siehe Eagle v. Morgan, 88 F. 3d. 620 (8th Cir. 1996); Russell v. Gregoire, 124 F. 3d. 1079 (1094) (9th Cir. 1997).
385 *Schwartz*, Zur Architektonik des Datenschutzes in den USA, in: *Stern/Pfeifer/Hain*, Datenschutz im digitalen Zeitalte, S. 113 f.
386 Vgl. Barry v. City of New York, 712 F. 2d. 1554 (2nd Cir. 1983); Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978).
387 Vgl. Nat. Fed'n of Fed. Employers v. Greenberg, 983 F. 2d. 286 (D.C. Cir. 1993).
388 Vgl. Eagle v. Morgan, 88 F. 3d. 620 (8th Cir. 1996); Russell v. Gregoire, 124 F. 3d. 1079 (1094) (9th Cir. 1997).
389 Barry v. City of New York, 712 F. 2d. 1554 (1561 ff.) (2nd Cir. 1983).
390 Schacter v. Whalen, 581 F. 2d. 35 (37) (2nd Cir. 1978).

soll das staatliche Interesse sein, um einen Verstoß gegen das Recht auf informationelle Privatsphäre zu rechtfertigen. Die Circuit Courts erklären das staatliche Interesse an der Verbesserung des Wahlprozesses mit der Begründung für wesentlich, dass durch die Transparenz bei den Wählern das Vertrauen erhöht wird.[391] Die Förderung der öffentlichen Sicherheit und Wohlfahrt wird ebenfalls als ein wesentliches Interesse angesehen.[392] Der Staat verliert dann einen Prozess, wenn kein staatliches Interesse vorhanden ist.[393]

Nach fortdauernden Entscheidungen der Circuit Courts wurde dem Supreme Court erst wieder im Jahr 2011 ein Anlass gegeben, um eine endgültige Entscheidung über die Verletzung des Rechts auf informationelle Privatheit zu treffen. In diesem Fall ging es darum, ob die Hintergrundüberprüfung des Vertragspersonals durch die NASA das Recht auf die informationelle Privatheit verletzte.

Entsprechend der leitenden Weisung des damaligen Präsidenten *George W. Bush*, die neuen gleichförmigen Identifizierungsstandards für das Bundespersonal einschließlich des Vertragspersonals zu gestalten, ordnete das Handelsministerium an, dass das Vertragspersonal, das schon lange Zugang zu Bundeseinrichtungen hatte, bis zum Oktober 2007 die Hintergrundüberprüfung vollenden musste. Das *Jet Propulsion Laboratory (JPL)* ist eine Einrichtung der NASA, die das *California Institute of Technology (Caltech)* unter staatlichem Vertrag führt. Im Januar 2007 änderte die NASA den mit Caltech abgeschlossenen Vertrag. Nach dem neuen Vertrag musste das gesamte Personal des JPL die neue Hintergrundüberprüfung rechtzeitig ausführen.

Aus diesem Grund erhoben die Beklagten eine Klage unter Berufung darauf, dass das Hintergrundüberprüfungsverfahren das verfassungsrechtli-

391 Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978): Floridas *Sunshine Amendments* liefern den Wählern mehr Informationen über Kandidaten und die finanziellen Offenlegungsvorschriften zielen darauf ab, die Wahrscheinlichkeit von Korruption oder Interessenkonflikten zu verringern (1134 ff.). Obwohl der Richter *Wisdom* Zweifel an der Effektivität der Amendments zur Abschreckung vor Korruption gezeigt hat, erkannte er die potenzielle Effektivität an und erklärte die Amendments für legitim. Für eine ähnliche Begründung siehe auch Barry v. City of New York, 712 F. 2d. 1554 (1560 ff.) (2nd Cir. 1983).

392 Schacter v. Whalen, 581 F. 2d. 35 (37) (2nd Cir. 1978); Zum Schutz der Gesundheit und Sicherheit von Arbeitskräften, S. Westinghouse, 638 F. 2d. 570 (579) (3rd. Cir. 1980).

393 Vgl. Fadjo v. Coon, 633 F. 2d. 1172 (5th Cir. 1981); Tavoulareas v. Washington Post, 724 F. 2d. 1010 (D. C. Cir. 1984); James. v. City Douglas, 941 F. 2d. 1539 (11th Cir. 1991); Gruenke v. Seip, 225 F. 3d. 290 (3rd Cir. 2000).

che Recht auf die informationelle Privatheit verletzt. Während das Amtsgericht eine einstweilige Verfügung leugnete, wies das *Ninth Circuit Court* die Anordnung des Amtsgerichts ab. Es entschied, dass einige Teile des Formulars zur Hintergrundüberprüfung wahrscheinlich verfassungswidrig sind, z. B. die Bekanntgabe von Drogenbehandlungen oder Beratungen u. a. Die Regierung beantragte daher eine Revision.

Die Grundannahme des Supreme Court vor der konkreten Überprüfung lautet, dass die Verfassung das Recht auf die informationelle Privatheit schütze, das in beiden oben genannten Entscheidungen, *Whalen* und *Nixon*, erwähnt wurde.[394] Der Supreme Court entschied danach, dass die Hintergrundüberprüfung der NASA ein solches Recht nicht verletzt habe. Der Schutz der *privacy* umfasse gemäß dem Supreme Court tatsächlich mindestens zwei unterschiedliche Arten des Interesses: zum einen das Interesse an der Vermeidung der Offenlegung persönlicher Angelegenheiten, zum anderen das Interesse an der Selbstbestimmung ohne staatliche Intervention.[395] Die Regierung habe ein Interesse an der Durchsetzung der Hintergrundüberprüfung zur begründeten Einstellung und dieses Interesse hänge nicht von der Stellung als Bundespersonal oder Vertragspersonal ab. Die Erhebung persönlicher Daten durch den Staat zu öffentlichen Zwecken könne das Problem der Bedrohung der Privatsphäre verursachen. Das Problem sollte durch eine gesetzliche oder behördliche Verpflichtung gelöst werden, um die unbefugte Veröffentlichung zu vermeiden.[396] Dabei wird die Frage, ob das Recht in der amerikanischen Verfassung existiert, offengelassen. Die Richterin *Scalia* stimmt dieser Auffassung, nach der die Hintergrundüberprüfung kein bestimmtes verfassungsrechtliches Recht verletzt, zwar zu, sie behauptet jedoch, dass der Gerichtshof die Frage des verfassungsrechtlichen Rechts auf informationelle Privatheit negativ hätte lösen müssen.[397]

---

394 NASA v. Nelson, 131 S. Ct. 746 (753 f.); *Fan*, Constitutionalizing Informational Privacy by Assumption, 14 U. Pa. J. Const. L. 953, 2012 (954); *Olivito*, Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy, Ohio State Law Journal, vol. 74, no. 4 669, 2013 (689 f.); *Moniodis*, Moving from Nixon to NASA: Privacy's Second Strand – A Right to Informational Privacy, 15 YALE J. L. & Tech. 139, 2012 (148).

395 Whalen v. Roe, 429 U. S. 589 (599); NASA v. Nelson, 131 S. Ct. 746 (753); *Azarchs*, Informational Privacy: Lessons from Across the Atlantic, 16 U. Pa. J. Const. L. 805, 2014 (807).

396 NASA v. Nelson, 131 S. Ct. 746 (753); Whalen v. Roe 429 U. S. 589 (600 f.).

397 Sie verneint bei der Zustimmungsmeinung das Konzept des verfassungsrechtlichen Rechts auf die informationelle Privatsphäre. Ihre Ansicht stützt auch der

Daher lässt sich feststellen, dass der Supreme Court den verfassungsrechtlichen Schutz des Rechts auf informationelle Privatheit nur vermutet und entsprechend der *Whalen*- und der *Nixon*-Entscheidung das Recht in zwei Teile differenziert, und dass auch die staatliche Pflicht, die vom Staat erhobenen Informationen zu schützen, in Betracht gezogen wurde. Es ist jedoch unklar, ob die von Circuit Courts entwickelte konkrete Abwägungsgleichung vom Supreme Court bei der Abwägung beider kollidierender Interessen verwendet wurde. Nach der Abwägungsgleichung der Circuit Courts wird das Schutzniveau zuerst danach festgelegt, wie privat oder intim eine bestimmte Information ihrem Wesen nach ist. Unter Berücksichtigung des Klägerelements, das den Schutz verringert, wird der Umfang des Rechts auf informationelle Privatheit wiederum gemäß dem Kriterium festgelegt, ob eine gesetzliche oder prozedurale Sicherungsmaßnahme vorgesehen ist. Ist das individuelle Interesse einmal auf diese Weise festgesetzt, kann die Verletzung der angegriffenen Vorschriften oder des staatlichen Handelns mit Hilfe der Abwägung geprüft werden. Das Gericht gewährt in der Regel den höchsten Schutz für die Informationen, die den Autonomiebereich berühren oder die medizinische Informationen von intimem Charakter (z. B. Schwangerschafts- oder HIV-Status) darstellen, während, relativ gesehen, allgemeine medizinische, finanzielle oder beschämende Informationen aufgrund der Tatsache, dass es sich bei ihnen nicht um höchstpersönliche Informationen handelt, weniger geschützt werden. Die staatliche Pflicht zum Vertraulichkeitsschutz wird konkret, aber gegebenenfalls vordergründig bewertet.

Es lässt sich folgern, dass die persönlichen Daten als solche durch den Staat unterschiedlich, nämlich je nach Art ihrer Sensibilität, dann erhoben und verwertet werden dürfen, wenn die Sicherungsmaßnahmen vorgesehen sind – wobei es keine Rolle spielt, ob sie hinreichend sind, um die personenbezogenen Daten vor der unbefugten Erhebung oder Verwertung zu schützen – und wenn das staatliche Handeln der Abwägungsprüfung standhalten kann. Umgekehrt wird die staatliche Erhebung und Verwertung von persönlichen Daten, die der Abwägungsprüfung nicht standhalten, als eine Verletzung des Rechts auf *privacy* angesehen.

Richter Thomas mit seiner kurzen zustimmenden Stellungnahme. (NASA v. Nelson, 131 S. Ct. 746 (757)); *Azarchs*, Informational Privacy: Lessons from Across the Atlantic, 16 U. Pa. J. Const. L. 805, 2014 (806): „Ohne eine klare Textgrundlage haben die Gerichte wenig Befugnis, ein solches Recht zu verteidigen, wenn es von den beiden anderen Regierungszweigen verletzt wird, und wenig Richtlinien zur Festlegung seiner Grenzen".

Obwohl der Supreme Court das Recht auf informationelle Privatheit nicht ausdrücklich feststellt, sondern nur implizit von dessen Existenz ausgeht, garantiert die US-amerikanische Verfassung für einen engen, inneren und speziellen Bereich den Schutz der *privacy* zumindest vor hoheitlichen Eingriffen. Es ist bemerkenswert, dass der Schutz der *privacy* mit Hilfe des Kriteriums „begründeter Erwartung auf *privacy*" erweitert wird und dass das Recht auf informationelle Privatheit unter der Differenzierung zwischen dem Vertraulichkeitsinteresse und dem Autonomieinteresse diskutiert wird. Bezüglich der Frage nach dem Schutz des Rechts auf informationelle Privatheit liegt die erhebliche Schwäche darin, dass das Gericht lediglich vor der Offenlegung Schutz gewährt, nicht aber bezüglich aller Verarbeitungsvorgänge von personenbezogenen Daten wie deren unbefugter Erhebung, Speicherung, interner Übermittlung innerhalb der öffentlichen Stellen sowie deren Verwertung.

Angesichts des Umstands, dass es nach US-amerikanischer Dogmatik keine Idee von einer Schutzpflicht des Staates gibt, aktive Maßnahmen zum Schutz der *privacy* von Individuen zu ergreifen, und daher die aus der US-Verfassung ableitbaren Rechte ausschließlich als Abwehrrechte gegenüber dem Staat zu verstehen sind, erscheint der Datenschutz durch ein generelles und fundamentales Recht auf informationelle Selbstbestimmung als sehr unwahrscheinlich.

II. Übersicht des einfachgesetzlichen Datenschutzsystems

Auch wenn die personenbezogenen Daten verfassungsrechtlich nicht ausdrücklich geschützt werden können, kann das Bundesgesetz Schutzmaßnahmen vorschreiben und dem Staat, der die Informationen anfordert, Prozessanforderungen auferlegen. Das US-amerikanische Recht kennt kein allgemeines Datenschutzrecht, welches die Privatsphäre eines Einzelnen und seine personenbezogenen Daten umfassend schützt und für alle staatlichen Organe Geltung hat. Beim Datenschutz wird in den USA ein bereichsspezifischer Regelungsansatz gewählt. Damit ist grundsätzlich jeder Datenverarbeitungsvorgang zulässig, soweit gesetzlich nichts anderes bestimmt ist. Da in vielen Einzelfällen politische Notwendigkeiten den Gesetzgeber zum Handeln trieben, konnte daraus nur eine bereichsspezifische Sondergesetzgebung entstehen. Dabei können grundsätzlich die folgenden Bundesgesetze gelten: 1. der Electronic Communications Privacy Act (ECPA), das aus dem Wiretap Act (18 U. S. C. §§ 2510–2522), das eine strenge Kontrolle für das „interception" der Kommunikationen

bietet, dem Stored Communications Act (18 U. S. C. §§ 2701–2711), der vorschreibt, dass die Behörden mit *subpoena*,[398] *court order* oder *warrant*[399] auf gespeicherte Daten im elektronischen Speicher zugreifen müssen und dass die Behörden *warrant* oder *court order* einholen müssen, um auf bestimmte Kundendaten von ISPs zugreifen zu können, und dem Pen Register Act (18 U. S. C. §§ 3121–3127) besteht, der vor der Installation des Pen Registers ein *court order* erfordert; 2. der Privacy Act (5 U. S. C. § 552a), der einen Code of Fair Information Practice festlegt, der die Erhebung, Verwendung und Übermittlung von personenbezogenen Daten über Personen regelt, die von Bundesbehörden geführt werden; 3. der Privacy Protection Act (PPA) (42 U. S. C. § 2000aa), der Mediendokumente und Arbeitsprodukte vor behördlichen Durchsuchungen und Beschlagnahmen schützt; 4. der Right to Financial Privacy Act (RFPA) (12 U. S. C. §§ 3401–3422), der den Kunden von Finanzinstituten das Recht auf ein gewisses Maß an *privacy* bei behördlichen Durchsuchungen gibt und verhindert, dass Banken und andere Finanzinstitute die Finanzinformationen einer Person an die Behörden weitergeben, es sei denn, die Daten werden aufgrund einer *subpoena* oder eines Durchsuchungsbefehls veröffentlicht[400] und 5. der Foreign Intelligence Surveillance Act (50 U. S. C. §§ 1801–1811), der Standards und Verfahren für die Verwendung

398 Eine *subpoena* ist eine Anordnung für eine Einholung von Zeugnissen oder Unterlagen. Zahlreiche Gesetze ermächtigen die Bundesbehörden zur Ausstellung von *subpoenas*. Die Ausstellung einer *subpoena* setzt einen „Grund zu der Annahme voraus, dass die angeforderten Daten für eine rechtmäßige Strafverfolgungsuntersuchung relevant sind." Wenn der Betroffene, der eine *subpoena* erhält, Einwände hat, kann er eine Klage einreichen, um die *subpoena* aufheben oder ändern zu lassen. Das Gericht kann die *subpoena* aufheben oder ändern, wenn ihre Einhaltung unvernünftig oder unterdrückend erscheint (Fed. R. Crim. P. 17 (c) (2)).

399 Eine *court order* und ein *warrant* unterscheiden sich durch ihre Anforderungen. Ein *warrant* wird durch einen wahrscheinlichen Grund (probable cause) gestützt, während eine *court order* konkrete und klar umrissene Tatsachen erfordert, aus denen hervorgeht, dass Grund zu der Annahme besteht, dass die gesuchten Informationen für die strafrechtliche Ermittlung relevant sind.

400 United States v. Dionisio, 410 U. S. 1: Eine *subpoena* der *Grand Jury* löst keinen Schutz des vierten Verfassungszusatzes aus; Gonzales v. Google, 234 F. R. D. 674 (N. D. Cal. 2006): Die Behörde stellte eine *subpoena* für die Suchanfragendaten von Google aus, um die Wirksamkeit der *content filtering software* zu untersuchen. Das Gericht gestattete der Behörde nicht, Informationen über Suchanfragen zu erhalten, da „der Verlust des Goodwills von Google eine potenzielle Belastung darstellt, wenn Google gezwungen ist, Suchanfragen an die Behörden weiterzuleiten".

der elektronischen Überwachung durch die Behörden zum Sammeln von Auslandsnachrichten in den USA festlegt.

Die Gesetzgebung auf Bundesebene beruht auf einer Unterstützung selbstregulativer Verfahrensweisen der US-Handelsaufsicht *FTC*. Gemäß der Rechtspolitik der Selbstregulierung ist die Regulierung wesentlicher Bereiche im gesellschaftlichen Leben den Betroffenen selbst überlassen. Der Staat fördert zwar (mehr oder minder stark) Leitlinien „guten" selbstregulativen Datenschutzes, die Form der Selbstregulierung bleibt jedoch den betroffenen gesellschaftlichen Kräften überlassen. So stützen sich die USA im Rahmen des Datenschutzes auf den Flickenteppich eng fokussierter sektoraler Gesetze und freiwilliger Selbstregulierung.[401] Die gesetzlichen spezifischen Datenschutzvorschriften in den USA können in zwei Kategorien nach Normadressaten aufgeteilt werden: zum einen Datenschutz im öffentlichen Sektor – für den Staat und seine Organe –, zum anderen Datenschutz im privaten Sektor – hinsichtlich des Schutzes Privater gegenüber Privaten.

1973 veröffentlichte das *U. S. Department of Health, Education & Welfare* (HEW) einen einflussreichen Bericht,[402] in dem eine Reihe von fair information practices (FIPs) empfohlen wurden:

1. Es darf keine Systeme zur Aufbewahrung personenbezogener Daten geben, deren Existenz geheim ist.
2. Es muss dem Einzelnen eine Möglichkeit gegeben werden, herauszufinden, welche Informationen über ihn in einem Datensatz enthalten sind und wie sie verwendet werden.
3. Es muss für den Einzelnen eine Möglichkeit bestehen, zu verhindern, dass für einen bestimmten Zweck erhaltene Informationen ohne seine Zustimmung für andere Zwecke verwendet oder zur Verfügung gestellt werden.
4. Der Einzelne muss identifizierbare Informationen über sich korrigieren oder ändern können.
5. Jede Organisation, die die Datensätze identifizierbarer personenbezogener Daten erstellt, verwaltet, verwendet oder übermittelt, muss die Zuverlässigkeit der Daten für ihren beabsichtigten Gebrauch gewähr-

401 Daneben haben die Einzelstaaten auch Gesetze, die die elektronische Überwachung und den Zugang zu Computern regeln. In einigen Staaten sehen diese Gesetze strengere Datenschutzbestimmungen vor als die Bundesgesetze.

402 *U. S. Department of Health, Education & Welfare*, Records, Computers, and the Rights of Citizens: Report of the Secretary´s Advisory Committee on Automated Personal Data Systems, 1973.

leisten und angemessene Vorkehrungen treffen, um einen Missbrauch der Daten zu verhindern.

Diese FIPs wurden in verschiedenen US-Datenschutzbestimmungen verkörpert. Aufgrund der Vielzahl von Gesetzen ist es unmöglich, sie alle übersichtlich vorzustellen. Unter diesen Gesetzen ist jedoch beispielsweise der Privacy Act[403] nennenswert. Das Gesetz legt eine Reihe von fair information practices fest, die die Erhebung, Verwaltung, Verwendung und Übermittlung personenbezogener Daten über Personen regeln, die von Bundesbehörden in Datenspeicherungssystemen geführt werden. Das Gesetz schützt als direkte gesetzgeberische Folge der sog. Watergate-Affäre die Privaten gegen hoheitliche Eingriffe in ihre Privatsphäre. Für die Daten, die von Bundesbehörden geführt werden, gelten nach dem Privacy Act folgende Grundsätze: das Übermittlungsverbot ohne Zustimmung der Betroffenen, der Zweckbindungsgrundsatz, die Datenvermeidung und -sparsamkeit, die Benachrichtigungspflicht, die Datensicherheit usw. Sein wesentlicher Grundsatz ist, die Datensammlung soweit möglich bei der betroffenen Person durchzuführen.[404] Nach diesem Gesetz darf keine Behörde Daten, die in einem Datenspeicherungssystem enthalten sind, auf beliebige Art und Weise an eine Person oder eine andere Behörde weitergeben, es sei denn, dies erfolgt auf schriftliche Anfrage oder mit vorheriger schriftlicher Zustimmung der Betroffenen.[405] Die Behörden dürfen nur jene Daten über eine Person speichern und verwalten, die relevant und notwendig sind, um einen Zweck der Behörde zu erfüllen, der gesetzlich oder auf Anordnung des Präsidenten zu erfüllen ist.[406] Eine Person muss auf Anfrage darüber benachrichtigt werden, wie ihre personenbezogenen Daten verwendet werden.[407] Die Behörden sind darüber hinaus auch dazu verpflichtet, angemessene administrative, technische und physische Schutzmaßnahmen zu treffen, um die Sicherheit und Vertraulichkeit der Daten zu gewährleisten.[408] Außerdem wird das Recht der Betroffenen auf Einsichtnahme und gegebenenfalls Berichtigung der über sie gesammelten Daten gewährleistet.[409] Der Privacy Act enthält jedoch viele Möglichkeiten bezüglich der Ausnahmen für die Daten, die nicht unter die Anforderun-

403 5 U. S. C. § 552a von 1974.
404 5 U. S. C. § 552a (e).
405 5 U. S. C. § 552a (b).
406 5 U. S. C. § 552a (e) (1).
407 5 U. S. C. § 552a (e) (3).
408 5 U. S. C. § 552a (e) (10).
409 5 U. S. C. § 552a (d).

gen des Gesetzes fallen. Diese Ausnahmen umfassen unter anderem: (1) die Daten zu Strafverfolgungszwecken; (2) die Daten, die gemäß dem FOIA offengelegt werden müssen; (3) die Daten, die für eine routine use offengelegt werden, wenn die Offenlegung mit dem Zweck vergleichbar ist, für den die Behörde diese Daten gesammelt hat; (4) die Offenlegung von Daten gegenüber dem *Census Bureau*; (5) die Offenlegung von Daten gegenüber einer Person aufgrund eines Nachweises zwingender Umstände, die sich auf ihre Gesundheit oder Sicherheit auswirken; (6) die Offenlegung gegenüber dem Kongress; (7) die Offenlegung gegenüber dem *Comptroller General*; (8) die Offenlegung aufgrund eines Gerichtsbeschlusses; (9) die Offenlegung gegenüber einer *credit reporting agency*.[410] Das Gesetz ist deshalb von Bedeutung, weil es das erste gesamtstaatliche Gesetz zum Schutz Privater gegen hoheitliche Eingriffe in deren Privatsphäre ist. Es findet allerdings nur bei Regierungsstellen der Bundesbehörden Anwendung, jedoch nicht bei Regierungsstellen in den einzelnen föderalen Staaten. Neben dem Schutz der Privatsphäre vor hoheitlichen Eingriffen dienen verschiedene Normen zum Datenschutz für den privaten Bereich, etwa der Fair Credit Reporting Act oder der Gramm-Leach-Billey-Act bei Finanzdienstleistern sowie der Electronic Communications Privacy Act oder der Children's Online Privacy Protection Act im Bereich der Telekommunikation und der neuen Medien.

Demnach fehlt in den USA ein allgemeines und bereichsübergreifendes Gesetz zum Schutz personenbezogener Daten sowohl für den öffentlichen als auch den privaten Sektor. Auch wenn es im öffentlichen Sektor ein gesamtstaatliches Gesetz gibt, ist dieser Schutz nur begrenzt.

B. Datenschutz bei den konkreten Maßnahmen

Der vierte Verfassungszusatz schützt eine Person gegen unbegründete Durchsuchung und Beschlagnahme, wenn eine Person begründete Erwartung auf *privacy* hat. Ein *warrant*, der auf einen wahrscheinlichen Grund (*probable cause*) gestützt wird, kann eine Durchsuchung durch den Staat rechtfertigen. In den USA wird das Recht auf die informationelle Privatheit zwar verfassungsrechtlich mit Hilfe der Unterscheidung zwischen Vertraulichkeits- und Selbstbestimmungsinteressen überprüft und geschützt, aber die konkreten Vorkehrungen zum Zweck des Schutzes dieses Rechts werden aus den verfassungsrechtlichen Entscheidungen nicht abgeleitet.

410 5 U. S. C. § 552a (b).

Die konkreten Kriterien bzw. Schutzmaßnahmen im Hinblick auf das Recht auf informationelle Privatheit werden eher durch die FIPs[411] oder andere bundesrechtliche Einfachgesetze empfohlen oder ergriffen. Da die *privacy* zwar im Rahmen des vierten Verfassungszusatzes geschützt ist, aber darunter verschiedene Ausnahmen und *privacy doctrines* gelten, ist es sinnvoll zu betrachten, wie die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch den Staat im Rahmen bestimmter Einfachgesetze geregelt werden.

In diesem Zusammenhang soll zuerst untersucht werden, wie das Strafregister, die Rasterfahndung und die Vorratsdatenspeicherung als die für die vorliegende Arbeit ausgewählten Bereiche gesetzlich bestimmt sind und welche Daten darunter auf welche Weise erhoben, gespeichert, verwendet und weitergegeben werden dürfen. Anschließend soll eingeschätzt werden, welche Maßnahmen zum Zweck des Schutzes personenbezogener Daten gegen den unbefugten oder übermäßigen Zugriff darauf getroffen werden und ob die Vorkehrungen hinreichend sind, um den Einzelnen unter den modernen automatisierten Datenverarbeitungsbedingungen zu schützen.

I. Strafregister

Die *criminal history records*[412] spielen eine bedeutsame und oft entscheidende Rolle in jeder Phase des Strafverfahrens.[413] Die USA haben kein national zentralisiertes Strafregister. Vielmehr betreibt jeder Staat ein eigenes zentrales Strafregister, das die Fallverarbeitungsinformationen erhält, zu denen die Strafverfolgungsbehörden, die Gerichte und die Vollstre-

411 Fair Information Practices, in: *U. S. Department of Health, Education & Welfare*, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973.

412 Der United States Code definiert die *criminal history records* als „information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release" (42 U. S. C. § 14616).

413 Die Daten fördern die Entscheidungsfindung in jeder Phase des Strafverfahrens: "to keep track of arrestees; to identify and apprehend absconders; to assess risk of flight and future criminality for purposes of pretrial and post-trial detention; to make prosecutorial decisions on diversion, charging, and plea bargaining; to determine appropriate sentences; and to administer probation, jails, prisons, and parole."

ckungsbehörden des jeweiligen Staats beigetragen haben. Das Strafregister wird den Strafverfolgungsbehörden um legitimer Zwecke willen durch landesweite Telekommunikationssysteme zugänglich gemacht. Infolge des tendenziell zunehmenden Zugangs zu den im Strafregister gespeicherten Daten und der wachsenden Anzahl privater Informationsvermittler mit eigenen Strafregisterdatenbanken wird die Frage des Datenschutzes im Bereich des Strafregisters öfter als je zuvor gestellt.

Bis 1967 betrieb das FBI eine zentralisierte Strafregisterdatei, die als primäre Quelle für den zwischenstaatlichen Datenaustausch bei nationalen Strafregisteranfragen diente. Das FBI behielt in seiner eigenen Datenbank Kopien der *rap sheets*[414] aller Staaten, damit eine Strafverfolgungsbehörde in einem Staat herausfinden konnte, ob eine bestimmte Person in einem Strafregister eines anderen Staates registriert war. Als eine Reaktion auf den Vorschlag der *President's Commission on Law Enforcement and Administration of Justice*[415] gründete das FBI 1967 das *National Crime Information Center* (NCIC) unter der *Criminal Justice Information Services Division* (CJISD), um eine bundesweite, benutzerorientierte Computerauskunft aus dem Strafregister zur Verfügung zu stellen. Daraufhin führte das NCIC ein zwischenstaatliches computergestütztes Strafregistersystem – *an interstate computerized criminal history record system* (CCH-System) – ein, das Angaben über Personen enthält, die wegen Verbrechen und schwerer Vergehen unter dem Gesetz des Bundes- bzw. Einzelstaats verhaftet wurden. Der National Crime Prevention and Privacy Compact Act von 1998 sah vor, dass das Informationssystem des FBI verschlankt und damit in einen effizienteren *Interstate Identification Index* (Triple I-System oder III-System) umgewandelt wird. Die Besorgnis über die Idee, ein nationales zentralisiertes Strafregister zu etablieren, sowie die Besorgnis um seine Praktikabilität und die Kosten führten nämlich dazu, dass das FBI das CCH-Programm zugunsten des dezentralisierten nationalen III-Systems[416] beendete.

---

414 Das bedeutet eine Chronologie der Handlungen des Strafjustizsystems in Bezug auf eine bestimmte Person, einschließlich Verhaftungen, Anklagedaten, Urteilen und Verurteilungen (*Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 392).

415 President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society (Washington D. C.: Government Printing Office, February 1967).

416 Das *Interstate Identification Index System* oder das III-System ist das kooperative *federal state system* für den Austausch von Angaben aus dem Strafregister und umfasst den *National Identification Index*, die Nationale Fingerabdruck-Datei und die *criminal history record repositories* der Einzelstaaten in dem Ausmaß ihrer

1. Organisationsstruktur

Das III-System ist ein zwischenstaatliches Computernetzwerk, das unter anderem dem Datenaustausch zwischen dem Bund und den Einzelstaaten dient und das die Mittel zur Verfügung stellt, mit denen beim nationalen Strafregister angefragt wird, um festzustellen, ob eine Person in einem der Bundesstaaten registriert ist.[417] Das NCIC pflegte bis vor Kurzem in der eigenen Datenbank Kopien von *rap sheets* aller Einzelstaaten, sodass eine Strafverfolgungsbehörde in einem Staat herausfinden konnte, ob ein Verhafteter oder eine Person von Interesse (wie ein Verdächtiger) in einem anderen Staat eine Eintragung in einem staatlichen Strafregister hatte.[418] Die Sorge um die Kosten sowie die Effizienz aufgrund des doppelten nationalen Registers von einzelstaatlichen Täterdatensätzen,[419] die Notwendigkeit zur Schaffung eines dezentralisierten nationalen Strafregistersystems mit gemeinsamer Verantwortung und gegenseitiger Verpflichtung[420] und der erhebliche technische und organisatorische Fortschritt, der ein dezentralisiertes nationales Strafregister unterstützen kann, führten dazu, dass das III-System das zentralisierte Datenbanksystem ersetzte.

Das III-System ist dazu gedacht, die automatisierten Datenbanken der staatlichen zentralen Strafregister und des FBI durch einen *Index-Pointer-Ansatz* in ein nationales System zusammenzuführen. Das FBI führt nun in erster Linie ein 51. Strafregister und stellt dabei Informationen über Bundesstraftäter zur Verfügung. Staatliche Strafregister, die als Datenanbieter für nationale III-Suchzwecke funktionieren, übernehmen die Verantwortung für die Bereitstellung von *criminal history records* online in Re-

---

Teilnahme an diesem System und das *criminal history record repository* des FBI (28 C. F. R. § 20.3 (m)).

417 Über das dezentrale III-System siehe unten Schaubild 1.

418 Zur frühen Entwicklung dieses Programms siehe U. S. Dept. of Justice v. Reporter's Committee for Freedom of Press.

419 Dies ist vor allem darauf zurückzuführen, dass die Einreichung von Verhaftungs- und Verfügungsinformationen an die staatlichen *repositories* durch staatliche und örtliche Justizbehörden in den meisten Staaten gesetzlich vorgeschrieben ist, während die Einreichung dieser Informationen beim FBI durch diese Behörden freiwillig ist.

420 28 C. F. R. § 20.37: "It shall be the responsibility of each criminal justice agency contributing data to the III System and the FIRS to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred."

aktion auf III-Datenanfragen für Strafverfolgungszwecke. Dafür erlauben alle staatlichen Gesetzgebungen bezüglich *criminal history records* den zwischenstaatlichen und den zwischen dem Bund und den einzelnen Staaten stattfindenden Datenaustausch.

Das Verfahren der Mitteilung und Speicherung von Datensätzen im dezentralen III-System ist je nach den am NFF teilnehmenden oder nicht teilnehmenden Staaten unterschiedlich.[421] Im Fall von NFF-Staaten leitet deren Strafregister dem FBI bei der Verhaftung einer Person, die noch nie zuvor im Staat verhaftet wurde, die Fingerabdrücke der Person zusammen mit den Textdokumenteninformationen weiter. Die Identifikationsinformationen werden verwendet, damit die Person zum NII hinzugefügt oder der Index aktualisiert werden kann. Wenn die Person bereits im Index ist, dienen die Daten zur Festlegung eines Pointer, der angibt, dass das Repository einen *criminal history record* über die für berechtigte III-Zwecke zur Verfügung stehende Person enthält. Die Fingerabdrücke werden dem NFF hinzugefügt. Die Einzelstaaten senden also nur die erste Verhaftungseintragung elektronisch an das FBI, die im *Interstate Identification Index* der Aktualisierung der Liste von Tätern und Staaten dient, die weitere konkrete Registrierungen haben.[422] Weitere strafrechtlich relevante Daten, die sich auf die Täter beziehen, speichern die Staaten selbst. Damit stellen sie die Strafregistrierungen und die damit zusammenhängenden Informationen für eventuelle Anfragen aus anderen Einzelstaaten oder von zugelassenen Bundesbehörden zur Verfügung. Wenn eine Person verhaftet wird, die bereits zuvor in dem jeweiligen Staat verhaftet wurde, und wenn für die Übermittlung der staatlichen Verurteilungsdaten zum III-Zwecke das staatliche Repository zuständig ist, werden die Fingerabdrücke oder

421 NFF (*National Fingerprint File*) ist eine Datenbank von Fingerabdrücken oder anderen eindeutigen persönlichen Identifizierungsinformationen, die sich auf eine verhaftete oder angezeigte Person beziehen. Die darin enthaltenen Daten werden vom FBI gepflegt, um eine positive Identifizierung von Daten, die im III-System indiziert sind, zu pflegen (28 C. F. R. § 20.3 (o)). Die Staaten, die die Verantwortung für die Bereitstellung ihrer III-indizierten *criminal history records* sowohl für nicht strafjustizielle Zwecke als auch für Strafjustizzwecke übernommen haben, werden als „NFF-Staaten" bezeichnet, weil sie dem FBI dem *National Fingerprint File-Konzept* gemäß Fingerabdrücke und Anzeigen- sowie Dispositionsinformationen von Straftätern vorlegen. Bis zum Jahresende 2016 haben 20 Staaten am NFF teilgenommen (http://www.search.org/states-participation-in-national-systems-and-programs-that-facilitate-interstate-exchange-of-criminal-history-records/, abgerufen am 29. Juni 2018).

422 Zurzeit nehmen alle fünfzig Staaten und der District of Columbia am III-System teil.

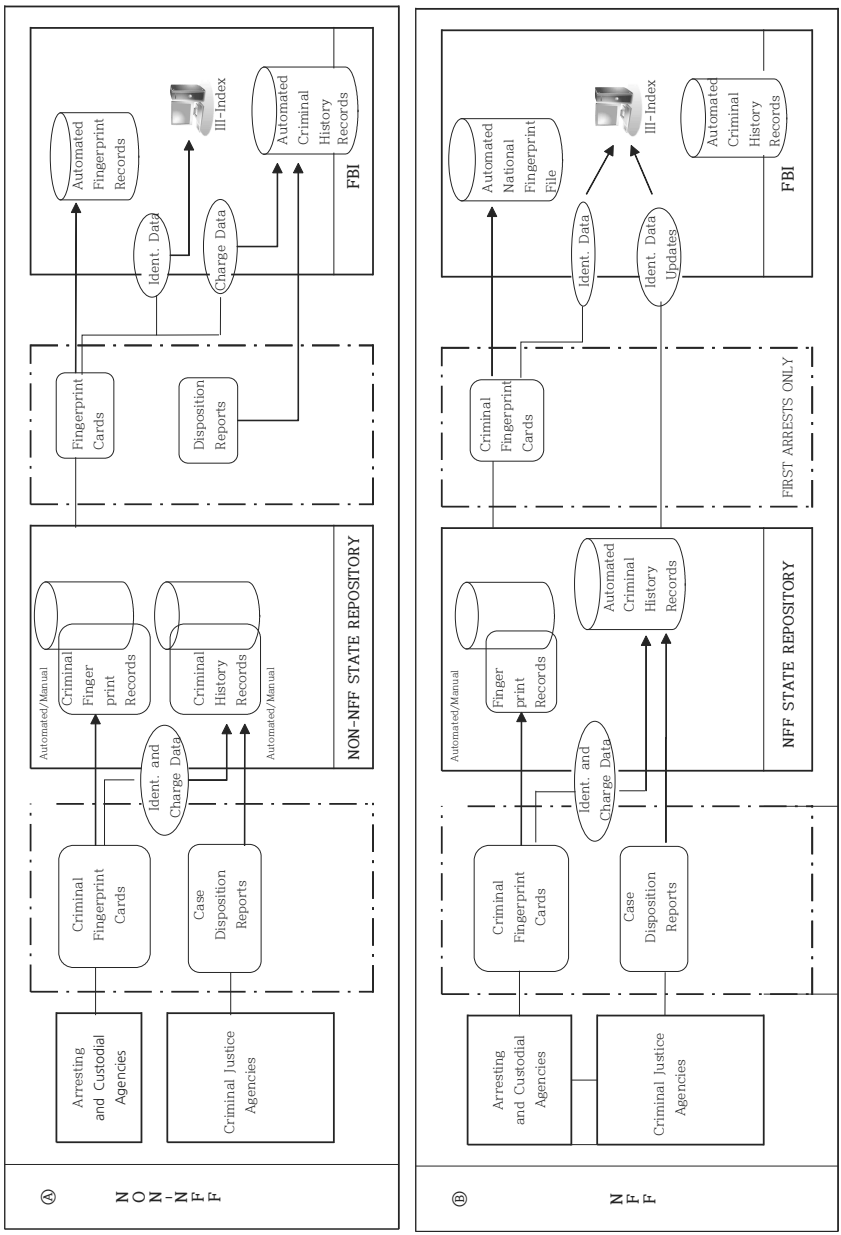
Anzeigen-/Dispositionsdaten nicht an das FBI weitergeleitet. Wenn eine Person verhaftet wird, die zwar bereits zuvor in dem jeweiligen Staat verhaftet wurde, aber für die Übermittlung ihrer staatlichen Eintragungen im Repository zum III-Zwecke das FBI verantwortlich ist,[423] leitet das einzelstaatliche Register die Fingerabdrücke oder Anzeigen-/Dispositionsdaten nach Vor-NFF-Praktiken weiter, sodass das FBI seine Eintragungen aktuell halten kann. Die Nicht-NFF-Staaten leiten ähnlich wie beim dritten Verfahren alle Fingerabdrücke oder Anzeigen-/Dispositionsdaten an das FBI weiter.

Unter diesem Ansatz unterhält das FBI einen automatisierten Master-Name-Index (MNI),[424] den *National Identification Index* (NII), der Namen und Identifikationsdaten enthält, die alle Personen betreffen, deren automatisierte Registrierungen über das III-System verfügbar sind.

423 Während sich einige III-Staaten darauf verständigt haben, nur die Aufzeichnungen von Personen zur Verfügung zu stellen, die als Ersttäter im Staat nach dem Zeitpunkt verhaftet und/oder angezeigt wurden, ab dem die Teilnahme am III-System stattfand, übernahmen die anderen Strafregister die Verantwortung für neue erstmalige Strafregistrierungen sowie für einige bereits vorhandene Aufzeichnungen von In-State-Straftätern. Das FBI stellt weiterhin einige Aufzeichnungen von Personen in III-Staaten zur Verfügung, deren Aufzeichnungen nicht auf staatlicher Ebene automatisiert wurden (vor allem ältere Personen, die vor Kurzem nicht kriminell tätig waren).

424 The master name index (MNI) is a key element of the criminal history system of the National Instant Criminal Background Check System (known as *NICS*) used for point-of-sale background checks of potential gun purchasers because it permits the user to identify a felony flag on a record of a named offender.

Schaubild 1: Berichterstattung und Pflege von Strafregistrierungen in einem dezentralen III-System[425]



2. Inhalt des Registers

Nach dem US-Code umfasst der Begriff der *criminal history records* nicht nur die strafgerichtlichen Verurteilungsdaten, sondern auch die Daten von Verhaftungen, die nicht zu einer Verurteilung führten, etwa in Fällen, in denen das Hauptverfahren nicht eröffnet wurde[426] oder in denen der Angeklagte vor Gericht freigesprochen wurde.[427] Alle Staaten speichern danach neben den strafgerichtlichen Verurteilungsdaten auch die Verhaftungsdaten in ihren Strafregistern, obwohl sich die in ihr Strafregister einzutragenden Inhalte gesetzlich unterschiedlich gestalten.

In den USA sieht kein Bundesgesetz vor, was in die staatlichen Strafregister eingetragen werden soll. Unabhängig von den einzelnen staatlichen Regelungen über die Inhalte des Registers werden auf bundesgesetzlicher Ebene nur die unter dem III-System zur Verfügung stehenden Zielverbrechen und die konkreten Angaben vorgesehen. Die *criminal history record information*, die im III-System und im *Fingerprint Identification Records System* (FIRS) gepflegt wird, umfasst in der Regel nur schwere und/oder erhebliche Straftaten von Erwachsenen und Jugendlichen. Das heißt, das FBI akzeptiert nach dem geltenden Recht keine Fingerabdrücke und Verhaftungsdaten für weniger schwere Straftaten wie z. B. Trunkenheit, Vagabundentum, Friedensstörungen, Bummeln, falsche Feueralarme und

425 Siehe *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 86.

426 Während in Deutschland nach dem Legalitätsprinzip die Strafverfolgungsbehörde dazu verpflichtet ist, ein Ermittlungsverfahren zu eröffnen, sobald sie Kenntnis von einer (möglichen) Straftat erlangt hat, können die Strafverfolgungsbehörden in den USA auf ein Opportunitätsprinzip zurückgreifen. Die Hauptaufgabe des Staatsanwalts im Vorverfahren besteht darin, die Flut der von der Polizei weitergeleiteten Fälle in einer nach der Verurteilungswahrscheinlichkeit und Verfolgungswürdigkeit gerichteten Prüfung zügig und wenn möglich ohne Durchführung einer nach dem amerikanischen Recht sehr aufwendigen Hauptverhandlung zu erledigen. Dabei kann sich der Staatsanwalt zur Bewältigung dieser Aufgabe ebenfalls auf einen weiten, kaum überprüfbaren Ermessensspielraum berufen. Er kann Anklage erheben oder eine der vielen ihm zur Verfügung stehenden Arten der vorzeitigen, bedingten oder endgültigen Verfahrenseinstellung wählen (siehe *Lützner*, USA, in: *Gropp* (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, S. 743).

427 Siehe auch oben Fn. 412.

Verkehrsverstöße.[428] Auf der einzelstaatlichen Ebene werden die Fingerabdrücke oder *criminal records* von Personen, die wegen solcher Straftaten verhaftet wurden, in einigen Staaten[429] gesammelt, aber in anderen nicht.[430] Auch wenn ein staatliches Register die *criminal records* der wegen minder schwerer Straftaten verhafteten Personen enthalten haben könnte, können die nicht in demselben Staat ansässigen Justizbehörden die Daten nicht durch eine Suche in der NCIC herausfinden.[431] Die einzelstaatlichen sowie das bundesstaatliche Strafregister speichern in der Regel die folgenden Informationen: Identifizierungsinformationen von Personen, auf die sich Angaben beziehen, sowie Informationen bezogen auf aktuelle und frühere Strafjustizverfahren (einschließlich Verhaftungen oder anderer formaler Strafanzeigen und Verfügungen, die von diesen Verhaftungen oder formellen Anklagen geführt werden). Erstere umfassen in der Regel die folgenden Angaben: Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Geschlecht, ethnische Zugehörigkeit, physikalische Eigenschaften wie Haar- und Augenfarbe, Größe, Gewicht und auffällige Narben oder Tattoos, insbesondere auch die Fingerabdrücke.[432] Letztere enthalten Informationen über alle Verhaftungen mit den verfügbaren Dispositionsdaten.

Das FBI führt kein gesondertes Strafregister für Jugendliche, es sei denn, dass sie als Erwachsene vor Gericht stehen. Bis 1992 wurden Gerichtsentscheidungen über Jugendliche nicht in der NCIC-Datenbank des FBI gespeichert. Ein dramatischer Anstieg der Jugendkriminalität führte allerdings dazu, dass der Generalstaatsanwalt eine Regel implementiert hat, die das FBI dazu ermächtigt, die *criminal records* für schwere Straftaten von

428 28 C. F. R. § 20.32 (a) und (b). Das FBI schlug jedoch vor, in das NCIC alle Verhaftungen einschließlich der weniger schweren Straftaten und der Vergehen im jugendlichen Alter einzubeziehen. Es vertrat die Erweiterung des Strafregisterumfangs aus zwei Gründen: erstens, um eine einheitliche nationale Politik zu schaffen, sodass Strafverfolgungsbehörden und Arbeitgeber, die ein FBI-criminal-history-record suchen, in einem anderen Staat die gleichen Informationen erhalten wie Strafverfolgungsbehörden und Arbeitgeber in dem Staat, in dem das Strafregister registriert wurde; und zweitens, um den öffentlichen und privaten Arbeitgebern wertvolle Informationen über potenzielle Mitarbeiter zu geben (*Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 188 und m. w. N.).

429 Siehe z. B. Ohio Rev. Code Ann. § 109.60.

430 Siehe z. B. N. Y. Crim. Proc. Law § 160.10.

431 28 C. F. R. § 20.32 (b).

432 Daneben dürfen auch Arbeitsplatzadresse, Automobilregistrierung und andere relevante Informationen gespeichert werden.

Jugendlichen in einzelstaatliche Strafregister einzutragen. Im Dezember 1992 kündigte das FBI an, dass die Jugendkriminalitätsangaben gemäß der neuen Regel unter den gleichen Standards übermittelt werden, die für die Verbreitung von normalen Strafregisterangaben (Erwachsene) gelten.

Ein Problem bezüglich der Datenspeicherung in einzelstaatlichen Strafregistern lösen die schlichten Strafverfahrensdaten – *arrest records* – aus, die nicht zur Verurteilung geführt haben. Die Daten werden zwar unter dem III-System zwischen einem die Daten erhaltenden Staat und einem anderen Staat nicht ausgetauscht. Die Speicherung der Strafverfahrensdaten ohne Verurteilung erfolgt jedoch auch dann, wenn ein Hauptverfahren gegen einen bestimmten Beschuldigten nicht eröffnet oder er für unschuldig erklärt wird, was für den ehemals zu Unrecht Beschuldigten zu nachteiligen Folgen führt.[433]

3. Verwendung der Daten aus dem Register

Im Grunde genommen sind die Bundesbehörden gesetzlich und verfassungsrechtlich dazu verpflichtet, sowohl die Daten der Öffentlichkeit zugänglich zu machen als auch die *privacy* personenbezogener Daten über die Personen in den Datenbanken zu schützen.[434] Die Entscheidung über den Schutz der *privacy* von Gerichtsdaten liegt im Allgemeinen im Ermessen der Richter und es besteht die Vermutung des öffentlichen Zugangs zu diesen Gerichtsdaten. Es liegt auch im Ermessen der Gerichte, bestimmte Gerichtsverfahren oder Teile von Gerichtsverfahren vor der Öffentlichkeit zu schützen. Die *privacy* anderer staatlicher Daten wird in erster Linie durch den Freedom of Information Act (FOIA), das zur Förderung der Transparenz in nationalen Datenspeicherungssystemen dient, und durch die einzelstaatlichen vergleichbaren Gesetze geregelt. Nach diesen Gesetzen kann jede Person Daten von Bundesbehörden anfordern.[435] Parallel

433 Siehe unten 4. über die möglichen Nachteile der Strafverfahrensdatenspeicherung.

434 *Solove/Schwartz*, Privacy Law: Fundamentals, S. 55 f.

435 Viele dieser Gesetze sehen Ausnahmen für die Offenlegung vor, um die *privacy* zu schützen. Das FOIA enthält neun Ausnahmen zur Offenlegung: (1) als vertraulich eingestufte Daten; (2) interne Personalregeln und -praktiken; (3) gesetzlich ausgenommene Daten; (4) Geschäftsgeheimnisse und vertrauliche Daten; (5) bestimmte Verhandlungsmaterialien; (6) Personal- und Krankenakten sowie ähnliche Akten, deren Offenlegung eine ungerechtfertigte Verletzung der *privacy* darstellen würde; (7) Strafverfolgungsdaten, die Rechtsstreitigkeiten stören,

dazu regelt der Privacy Act die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch die Bundesbehörden. Das Gesetz erstreckt sich aber nicht auf den privaten Sektor oder einzelstaatliche Behörden.

Die Gerichte haben jedoch entschieden, dass verfassungsrechtliche Privacy-Grundsätze nur geringe Auswirkungen auf die Erhebung, Speicherung oder Übermittlung von *criminal history record information* durch Strafverfolgungsbehörden haben.[436] Die Verfassung erkennt zwar ein berechtigtes Interesse an der *privacy* sensibler persönlicher Daten an,[437] der U. S. Supreme Court hat später jedoch festgestellt, dass die verfassungsrechtlichen Privacy-Grundsätze die Übermittlung von Daten über offizielle Handlungen durch Strafverfolgungsbehörden wie etwa eine Verhaftung nicht einschränken.[438] *Common Law Privacy Doctrines* haben sich daraufhin als weitgehend irrelevant für die Verwaltung von *criminal history record information* erwiesen.[439] Das führt zu einem Flickenteppich einer Vielzahl von Bundes- und Landesgesetzen und -rechtsverordnungen, die die Erhebung, Speicherung, Verwendung und Weitergabe von Strafregistrierungen regeln. Auf Bundesebene haben das Parlament mit einem Gesetz[440] und das Justizministerium mit einer Verordnung[441] Mindestanforderungen für die Verwaltung von *criminal history record systems* festgelegt, wobei es den Einzelstaaten überlassen wird, spezifischere Gesetze und Vorschriften zu entwickeln, um sicherzustellen, dass die staatlichen *criminal history records* vollständig, genau, für berechtigte Nutzer leicht zugänglich und vertrauenswürdig sind. Zur Sicherstellung der Vollständigkeit, der Genauigkeit und der Sicherheit von Strafregistrierungen, die die Strafregister erheben,

---

in die *privacy* eindringen, vertrauliche Quellen preisgeben oder die Sicherheit von Personen gefährden würden; (8) bestimmte Daten im Zusammenhang mit der Beaufsichtigung von Finanzinstituten; (9) geologische und geophysikalische Daten in Bezug auf *wells*.

436 Siehe *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 45.

437 Whalen v. Roe, 429 U. S. 589.

438 Paul v. Davis, 424 U. S. 693 (713).

439 *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 45.

440 Omnibus Crime Control and Safe Streets Act of 1968, 42 U. S. C. § 3789g (b), as amended by § 524 (b) of the Crime Control Act of 1973, Pub. L. No. 93-83, 87 Stat. 197 (1973).

441 28 C. F. R. § 20.21 (a) (1).

speichern und übermitteln, wurden mehrere gesetzliche Maßnahmen getroffen. Um die Vollständigkeit, die Genauigkeit und die Sicherheit der Daten sicherzustellen, werden per Gesetz und Verordnung einige Maßnahmen auf Bundesebene gefordert. Die gesetzliche Befugnis des Federal Bureau of Investigation (FBI) zur Verwaltung von Strafregistrierungen findet sich vor allem in 28 U. S. C. § 534. Insbesondere wird der Generalstaatsanwalt gemäß den Absätzen (a) (1) und (a) (4) dazu ermächtigt, Personalien sowie die kriminalistisch relevanten und andere Daten zu erheben, zu speichern, zu klassifizieren und aufzubewahren sowie solche Daten mit den befugten Behörden zu teilen.[442]

Die Daten, die von einem *Central State Repository* gepflegt werden, sind zu ihrer Vollständigkeit innerhalb von 90 Tagen nach den Verfügungen zu erheben und zu speichern. Auf einzelstaatlicher Ebene ist die obligatorische Mitteilung von Verhaftungs- und Verfügungsdaten in allen Einzelstaaten geregelt, damit die Datenqualität sichergestellt werden kann. Zur Genauigkeit sollen Strafverfolgungsbehörden einen Prozess der systematischen Prüfung im Rahmen der Datenerhebung, der Eintragung und der Speicherung einleiten, der die Möglichkeit der Aufzeichnung und Speicherung ungenauer Informationen minimiert, und sie sollen alle Strafverfolgungsbehörden, die bereits solche Informationen erhalten haben, auch nachträglich benachrichtigen, wenn sie unzutreffende Informationen finden.[443] Teile der Verordnung wurden in den nationalen Gesetzen aller Länder umgesetzt, doch das gilt nicht für alle Teile. Manche wurden nur in den nationalen Gesetzen einiger, aber nicht aller Länder umgesetzt.[444]

Unter dem dezentralen Strafregisterwesen mit dem III-System unterscheiden sich die Regelungen über den Zugang zu und der Auskunftserteilung von Daten aus dem Strafregister von Staat zu Staat. Das Verfahren

---

442 Weitere bundesstaatliche Gesetze und Verordnungen, die den Generalstaatsanwalt zur Übermittlung von Strafregistern ermächtigen, sind PL 99 -169, as amended by PL 99 – 569 and PL 101 – 246, 5 U. S. C. § 9101; Executive Orders 10450 and 12968; PL 91 – 452; PL 101 – 647; PL 92 – 544, 86 Stat. 1115; PL 100 – 413; 102 Stat. 1101; PL 94 – 29, as amended by PL 100 – 181, 15 U. S. C. § 78q (f)(2); PL 97 – 444, 7 U. S. C. §§ 12a, 21 (b)(4)(e); PL 99 – 399, 42 U. S. C. § 2169; PL 101 – 604, 49 U. S. C. 44936; 28 C. F. R. 0.85 (b); U. S. Dep´t of Justice Order 556 – 73, 28 C. F. R. 16.30 – 16.34; 5 C. F. R. 732 & 736; PL 103 – 159; PL 103 – 209; PL 103 – 322.

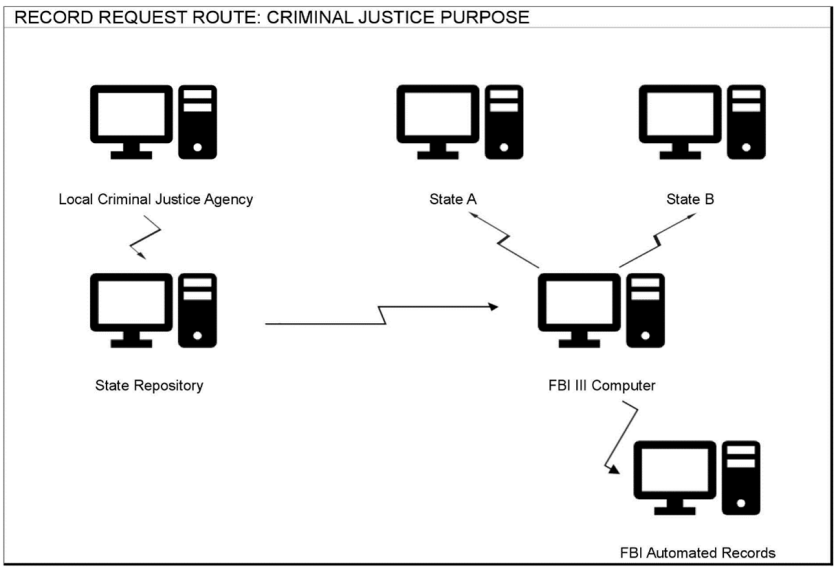
443 28 C. F. R. § 20.21 (a).

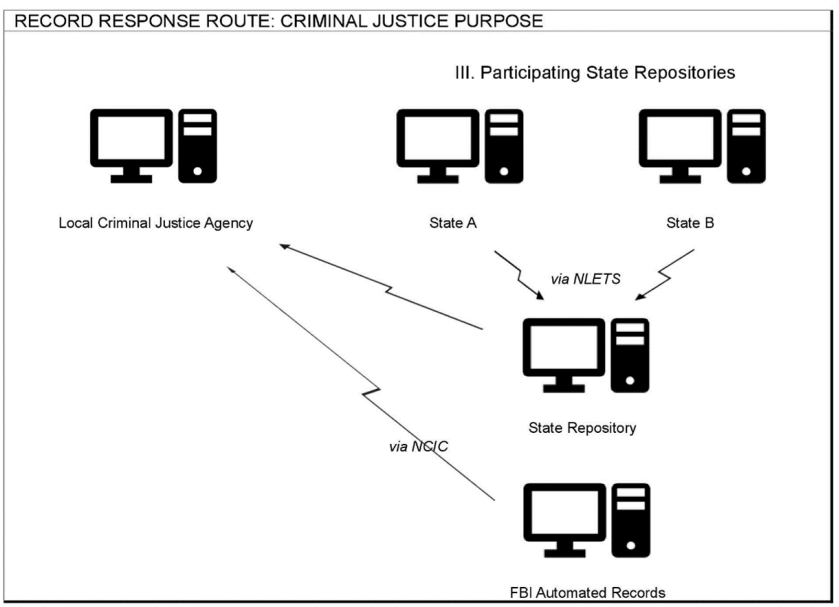
444 *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 49 ff.

einer Anfrage und Auskunft läuft grundsätzlich jedoch wie folgt ab:[445] Eine lokale Justizbehörde überträgt die Anfrage über das staatliche Telekommunikationsnetz an das staatliche Register. Das Register leitet die Anfragenachricht über das NCIC-Netzwerk an den III-Computer weiter. Der III-Computer schaltet die Meldungen entweder auf das staatliche Strafregister um, das Strafregistrierungen über die die Anfrage betreffenden Personen beinhaltet, und/oder auf das FBI, wenn es bezüglich der fraglichen Personen einen Datensatz auf Bundesebene oder in einem oder mehreren Staaten gibt, die nicht am III-System teilnehmen. Wenn das Ergebnis einer Suche nach diesem Index zeigt, dass das Suchthema eine III-indizierte Registrierung hat, wird der Index auf die anfragende Behörde an das FBI und/oder an eine oder mehrere der staatlichen Strafregister verweisen, von denen der Datensatz oder die Datensätze dann übermittelt werden. Die anfragende Behörde kann die Registrierungen dabei mit Hilfe des NCIC-Netzwerks und des *National Law Enforcement Telecommunications System* (NLETS Network) direkt aus den angegebenen Quellen erhalten. Genauer gesagt werden Angaben, die von den automatisierten Dateien des FBI geliefert werden, über das NCIC-Netzwerk an das anfragende staatliche Register zurückgegeben. Die am III-System teilnehmenden staatlichen Strafregister nutzen das NLETS-Netzwerk, um Auskünfte zu erteilen. Das die Auskünfte erhaltende staatliche Strafregister gruppiert, falls erforderlich, mehrstaatliche Angabenkomponenten und übermittelt eine Antwort an die anfragende Behörde. Der gesamte Prozess dauert in der Regel weniger als eine Minute.

445 Über das Verfahren einer Datenanfrage und -auskunft für strafjustizielle Zwecke siehe unten Schaubild 2.

Schaubild 2: Datenanfragen und -antworten für strafjustizielle Zwecke[446]





Für die Übermittlung personenbezogener Daten gelten je nach der über sie Auskunft erhaltenden Behörde und den Zwecken unterschiedliche Einschränkungen.[447] Nach 28 C. F. R. § 20.21 (b) und (c) gibt es Beschränkungen nur bei der Übermittlung von *nonconviction data* (Verhaftungsdaten, die nicht zu einer Verurteilung führen) und bei der Übermittlung an die *noncriminal justice agencies*. Die Beschränkung gilt also weder für die Übermittlung von Verurteilungsdaten noch für die Übermittlung von *criminal history records* an Strafjustizbehörden. Dementsprechend stellen die Staaten in der Regel nur wenige oder keine Beschränkungen für die Übermittlungen von Verurteilungsdaten vor, und eine Reihe von Staaten beschränken auch nicht die Übermittlung von *open arrest records*, die weniger als ein Jahr alt sind.[448] Die Mehrheit der strafjustiziellen Anfragen an staatliche Strafregister für *criminal history records* wird von entfernten Computer-Terminals online empfangen. Solche Online-Remote-Terminals bieten einen direkten Zugriff auf das MNI des Repository für die Durchführung von Suchvorgängen und für die Führung von *criminal history files* zum Zweck der Erlangung von c*riminal history records*. Hierbei wird auf der föderalen Ebene die Führung der staatlichen Strafregister nur unter dem Aspekt der Vollständigkeit, der Genauigkeit und der Sicherheit von Daten kontrolliert, die von staatlichen Registern gespeichert und gepflegt werden, nicht aber unter dem Aspekt des Datenschutzes. Generell gibt es so gut wie keine datenschutzrechtlichen Regelungen in diesem Bereich.

Neben der Nutzung der Daten aus dem Strafregister zu strafrechtlichen Zwecken wurde der Zugriff auf die Datensätze aus dem Strafregister erweitert. Die *criminal records* werden nicht nur den lokalen, staatlichen und föderalen Strafverfolgungsbehörden zur Verfügung gestellt, sondern

446 Siehe *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 78.

447 28 C. F. R. § 20.33 (a).

448 *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 55.

sind auch anderweitig verfügbar.[449,450] Eine zunehmende Anzahl von Staaten erleichtert es jeder Person, für irgendeinen Zweck die Daten über irgendjemanden aus dem Strafregister zu erhalten.[451] Der hauptsächliche Grund dafür ist die Gesetzgebung, die die durch den Bund veranlassten *background checks* (Hintergrundprüfungen) für nichtstrafrechtliche Zwecke ermöglicht oder erfordert, und Megans Gesetze. Insbesondere für Sexualstraftäter stehen aufgrund der Verbreitung von Megans Gesetzen und des *Adam Walsh*-Gesetzes personenbezogene Daten aus dem Strafregister kostenlos online zur Verfügung.[452] Darüber hinaus wurde die Vertraulichkeit einzelner Strafregisterdaten durch die Verabschiedung von Gesetzen zu Hintergrundprüfungen erheblich beeinträchtigt.

Megans Gesetze, die die Identitäten, Adressen und Straftaten von Sexualstraftätern über das Internet öffentlich zugänglich machen, haben ebenfalls zu einem rascheren Zugang zu staatlichen Strafregistern geführt.[453]

---

449 Die staatlichen Strafregister machen ihre *criminal records* nicht nur der staatlichen und lokalen Polizei, Bewährungsbehörde, Strafvollzugsbehörde und den anderen Strafjustizbehörden, sondern auch einigen Arbeitgebern und Verbänden verfügbar: S. Colo. Rev. Stat. § 24-72-303 (2007); *U. S. Department of Justice*, Survey of State Criminal History Information Systems, 2003, Bureau of Justice Statistics.

450 Die Verurteilungsdaten stehen gegen eine Gebühr zur Verfügung oder sind sogar frei online zugänglich. So veröffentlicht z. B. Colorado alle Verurteilungen im Internet und ermöglicht gegen eine geringe Gebühr die Durchführung einer Strafregistersuche über das Internet. Connecticut macht Verurteilungsdaten für die Öffentlichkeit allgemein zugänglich. Kansas, Montana und Oklahoma verlangen bereits von bestimmten gewalttätigen Tätern, sich bei der Strafvollzugsbehörde oder einer lokalen Strafverfolgungsbehörde anzumelden. Ein in Illinois verabschiedetes Gesetz weist staatliche Feuerwehrstationen an, auf ihrer Webseite Daten über Brandstifter zu veröffentlichen. Tennessee stellt jeder Person gegen eine Gebühr eine Kopie aller Verurteilungsdaten in seinem Strafregister zur Verfügung. Viele Staaten, einschließlich Florida, bieten den Online-Zugang zu einem Namensverzeichnis von aktuellen und ehemaligen staatlichen Gefangenen (vgl. *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 399 f.).

451 *U. S. Department of Justice*, Report of the National Task Force on Privacy, Technology, and Criminal Justice Information, 2001, Bureau of Justice Statistics, S. 1.

452 Ein obligatorisches Anmelde- und Gemeinschaftsmeldungsgesetz, das von Personen, die wegen Sexual- und Kindermissbrauchsdelikten verurteilt oder wegen seelischer Störung freigestellt wurden, verlangte, sich bei den örtlichen Strafverfolgungsbehörden anzumelden (N. J. Stat. Ann. §§ 2C:7-1-17 (2006).

453 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 399.

Im Jahr 1990 verabschiedete der US-Bundesstaat Washington den ersten Community Protection Act, mit dem die Registerbehörden dazu ermächtigt wurden, Auskünfte über Sexualstraftäter an die Öffentlichkeit zu geben.[454,455] Darüber hinaus garantiert der Adam Walsh Child Protection and Safety Act,[456] dass jeder Staat ein Online-Sexualstraftäterregister haben wird. Das Gesetz sieht vor, dass der US-amerikanische Generalstaatsanwalt die Richtlinien für staatliche Sexualstraftäterregister verkündet, und es droht Staaten an, die die Anforderungen der Registrierungspflicht bis 2009 nicht erfüllen, mit dem Verlust von Bundesförderungen.[457] Das Gesetz fordert ferner, dass das FBI ein nationales Register für Sexualstraftäter einrichtet und führt, das alle staatlichen Register vereint.[458]

Die Vertraulichkeit der *criminal history records* wurde mit der Verabschiedung von Gesetzen, die die föderal-initiierten *background checks* für nicht strafrechtliche Zwecke ermöglichten oder erforderten, ernsthaft erodiert.[459] Die Anzahl der Übermittlung von Fingerabdrücken an das FBI zum Zweck der nicht strafrechtlichen Kontrolle übersteigt nun die Anzahl derer zum Zweck der strafrechtlichen Kontrolle. Im Jahre 2005 wurden etwa zehn Millionen nicht strafrechtliche Kontrollen durchgeführt.[460] Das FBI behandelte die *criminal history records* historisch als so vertraulich, dass sie nur mit lokalen einzelstaatlichen und bundesstaatlichen Strafverfolgungsbehörden geteilt werden sollten.[461] In den letzten Jahren hat das

454 Wash. Rev. Code Ann. § 4.24.550 (West 2005).

455 Nachdem New Jersey als Reaktion auf die Vergewaltigung und Ermordung der siebenjährigen Megan Kanka durch einen zuvor zweimal verurteilten Sexualstraftäter ein Gesetz zur Registrierung von Sexualstraftätern und zur Benachrichtigung der Gemeinschaft verabschiedet hatte, galten Megans Gesetze im ganzen Land. Heute haben alle fünfzig Staaten Megans Gesetze, die es jedem ermöglichen, auf einer Webseite der staatlichen Strafregister für Sexualstraftäter nach einem Namen oder einem Wohnsitz zu suchen (Siehe *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 205 m. w. N.).

456 Pub. L. No. 109-248, 120 Stat. 587 (2006) (codified as amended in scattered sections of 18 and 24 U. S. C.).

457 Adam Walsh Child Protection and Safety Act §§ 112, 125, 120.

458 Adam Walsh Child Protection and Safety Act § 119.

459 Das Gesetz, das das Parlament im Jahre 1972 erlassen hat, ermöglicht den Bundesstaaten darüber hinaus, dass ihre Strafregister im Namen privater Arbeitgeber die FBI-Hintergrundkontrolle (FBI *background checks*) anfordern: Pub. L. No. 92-544, 108 Stat. 1109, 1115 (1972).

460 *U. S. Department of Justice*, Attorney General's Report on Criminal History Background Checks, 2006, S. 3.

461 28 C. F. R. § 20.1 (2007).

Parlament jedoch eine Reihe von Gesetzen verabschiedet, die die Vertraulichkeit dieser Daten vermindern, indem sie die Hintergrundprüfungen für nicht strafrechtliche Zwecke nicht nur erlaubt, sondern auch beauftragt. Während der Kongress zuvor den Zugang zu den *criminal records* nur erlaubt hatte, begann er nunmehr, durch andere neue Rechtsvorschriften *background checks* sogar zu verlangen.[462] Nach den Terroranschlägen vom 11. September 2001 verabschiedete der Kongress mehrere Gesetze, die Hintergrundprüfungen für etwa eine Million Arbeiter fordern, einschließlich Gepäckprüfern, Hafen- und Chemiearbeitern, Beschäftigten in der Transportindustrie und des privaten Sicherheitspersonals und Personen, die bestimmte biologische Mittel behandeln. Diesbezüglich stellen die staatlichen Strafregister ihre Daten einigen Arbeitgebern und freiwilligen Vereinigungen zur Verfügung.[463] In diesem Zusammenhang stellen sich zwar viele Datenschutzfragen, in der vorliegenden Arbeit kann jedoch nicht konkret auf all diese Frage eingegangen werden; stattdessen beschränkt die Autorin sich auf die Datenschutzfrage bezüglich der Verwendung der Strafregistrierungen im Strafverfahren. Denn die *background checks* privater Unternehmen weichen vom Untersuchungsumfang der vorliegenden Arbeit ab.

Um einen unbefugten oder unverhältnismäßigen Zugriff auf Strafregistrierungen zu vermeiden, veranlassten mehr als die Hälfte der Bundesstaaten ihre Strafverfolgungsbehörden dazu, bei Datenanfragen Protokolle zu behalten, die die Benennung der Empfänger der *criminal history record information* und das Anfragedatum enthalten.[464] Einige Bundesstaaten stellen außerdem gewisse Ausbildungsanforderungen an das Personal, das an dem Eintragen von Daten in die *criminal history record systems* beteiligt ist. Die Tendenz geht dahin, einzelne personenbezogene Daten aus dem Strafregister leichter zugänglich zu machen. Die öffentliche Politik scheint darauf hinzuwirken, dass die Daten im Strafregister allgemein zugänglicher werden, sodass Behörden, Vereinigungen und Einzelpersonen, wenn

462 Zum Beispiel führten die Terroranschläge vom 11. September 2001 zu einer Gesetzgebung, die für Millionen Menschen die kriminalgeschichtlichen Hintergrundchecks fordert.

463 Siehe z. B. *U. S. Department of Justice*, Survey of State Criminal History Information Systems, 2003, Bureau of Justice Statistics, S. 8.

464 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 57 f.

sie dies wollen, kriminalgeschichtliche Daten über beliebige Personen bei geschäftlichen und anderen Entscheidungen berücksichtigen können.[465]

Die datenschutzrechtliche Einschränkung der Auskunftserteilung aus dem Strafregister ist aus zwei Gründen weniger wirksam: den in Gerichten gespeicherten und von ihnen geführten Daten und der ansteigenden Anzahl privater Informationsvermittler mit eigenen Strafregisterdatenbanken. Ein großer Teil der *criminal history record information* über eine bestimmte Person ist öffentlich in *court dockets*[466] und *court records* zugänglich. Bis vor Kurzem waren jedoch die Strafregister einer Person nicht leicht abrufbar, da Suchende nicht Kenntnis darüber erlangen konnten, welche Gerichte die relevanten Daten besaßen. Die jüngste landesweite Zentralisierung und Automatisierung von Gerichtsaktensystemen haben die Identifizierung und Zugänglichkeit von Daten aber erheblich verbessert. Mit dem E-Government-Gesetz von 2002 wurde versucht, die Daten aus dem Strafregister über die Computersuche zugänglich zu machen.[467] Das Gesetz schreibt vor, dass Bundesbehörden und Bundesgerichte ihre Daten entweder per Fernzugriff oder alternativ durch Computerterminals vor Ort elektronisch zur Verfügung stellen.[468] Der zweite Grund für die weniger wirksame oder sogar unwirksame Einschränkung der Auskunftserteilung aus dem Strafregister liegt in der Existenz von sog. *criminal information brokers*. Nach dem ersten Verfassungszusatz kann niemand bestraft werden, wenn der Staat Daten an die Öffentlichkeit weitergibt.[469] Einige Unternehmen bauen ihre eigenen Datenbanken auf, indem sie in großen Mengen Strafregisterauszüge von Gerichten und staatlichen Strafregistern kaufen.[470,471] Sie entsenden in der Regel ihr Personal an die zuständigen

---

465 Es gibt zwar einige Einschränkungen, die sich jedoch darin erschöpfen, dass es Arbeitgebern verboten ist, Daten aus dem Strafregister in Arbeitsentscheidungen zu verwenden.

466 Ein *docket* enthält die Daten über Anklagen, Entscheidungen, Strafen und andere gerichtliche Ereignisse. Jedes Gericht verwaltet die Daten über jene Ereignisse (die *dockets* genannt werden), die vor dem jeweiligen Gericht stattgefunden haben.

467 Pub. L. No. 107-347. 116 Stat. 2889 (2002).

468 Pub. L. No. 107-347. 116 Stat. 2889 (2002), §§ 204–05.

469 *Solove/Schwartz*, Privacy Law: Fundamentals, S. 55: Der Staat kann aber die Daten nur unter der Bedingung zur Verfügung stellen, dass man zustimmt, deren Übermittlung einzuschränken.

470 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 185 f.

471 In der Regel kommen die US-amerikanischen Gerichte zu dem Schluss, dass Informationen, die der Öffentlichkeit einmal zugänglich gemacht wurden, nicht

Gerichte in der Gegend, in der das Subjekt einer Hintergrundsuche gelebt hat, um die Strafregisterdaten über diese Person zu erhalten. Durch eine Internetsuche nach Strafregistern können die *criminal history records* den Privaten zur Überprüfungen der Beschäftigung oder der Wohnungsvermietung oder zu anderen Zwecken gegen eine geringe Gebühr übergeben werden. So erhöht sich das Bedürfnis nach Datenschutz durch eine einheitliche Regulierung der Strafregister immer weiter, weil die Daten, die von Gerichten oder von privaten Informationsanbietern in ihren Datenbanken geführt werden, der Öffentlichkeit leicht zugänglich gemacht werden.

4. Speicherdauer

Außer einiger Ausnahmevorschriften gibt es keine föderale Gesetzgebung, die zu einer allgemein verfügbaren Tilgung (*expungement*)[472] von Eintragungen im Strafregister ermächtigt. Die Speicherdauer ist also bundesgesetzlich nicht vorgesehen. Obwohl das Parlament keine föderale Begünstigungsgesetzgebung erlassen hat, die in den meisten Staaten zur Verfügung

---

mehr privat sein können. Zu einem anderen Verständnis der *privacy* siehe U. S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U. S. 749: Das Gericht stellt fest, dass es auch dann, wenn die Daten in einer öffentlichen Domain stehen, einen großen Unterschied zwischen öffentlichen Daten, die erst nach einer sorgfältigen Recherche der Gerichtsakten, Landesarchive und örtlichen Polizeibehörden im ganzen Land gefunden werden können, und einer computergestützten Zusammenfassung in einer Datenbank in einer einzigen Informationsstelle gibt. Dieses Verständnis von *privacy* unterscheidet sich stark von der Art und Weise, wie die meisten Gerichte *privacy* verstehen.

472 *Expungement* bedeutet wörtlich, dass eine Aufzeichnung oder ein Verfahren vollständig gelöscht wird und *sealing*, dass eine Aufzeichnung oder ein Verfahren „nur" versiegelt, aber nicht zerstört wird. In Bezug auf den Gebrauch in vielen staatlichen Gesetzen über die Behandlung strafrechtlich relevanter Daten werden die beiden Begriffe jedoch häufig synonym verwendet. *Expungement* wird im Sinn von *expunging* oder *sealing* einer Aufzeichnung oder *annulling* einer Verurteilung verwendet. Unabhängig vom verwendeten Begriff ist die Rechtsfolge im Allgemeinen dieselbe: Behördliche Daten, die einen strafgerichtlichen Fall identifizieren, werden für die Öffentlichkeit nicht zugänglich gemacht. Der Zugriff auf die Daten durch die Strafverfolgungsbehörden kann auch bei – nur in Bezug auf die Terminologie – getilgten Daten gesichert werden. Das Ausmaß, in dem die Daten tatsächlich vernichtet werden, ist unterschiedlich, aber typischerweise wird vom Strafjustizsystem ein Mindestmaß an Daten aufbewahrt.

stehen kann, und nicht einmal eine gesetzliche Speicherdauer existiert, können die Straftäter aufgrund bestimmter Gesetze ausnahmsweise unter bestimmten Umständen eine Tilgung genießen. Ein Beispiel dafür ist 18 U. S. C. § 3607 (c). Die Vorschrift sieht einen Umstand vor, in dem das Parlament der Judikative das Tilgungsermessen ausdrücklich erteilt.[473] Die Tilgungsermächtigung der Exekutive ist in 42 U. S. C. § 14132 (d) vorgeschrieben.[474] Außerdem wird der *Secretary of Veterans Affairs* dazu

---

473 18 U. S. C. § 3607 (c): "Expungement of Record of Disposition. – If the case against a person found guilty of an offense under section 404 of the Controlled Substances Act (21 U. S. C. § 844) is the subject of a disposition under subsection (a), and the person was less than twenty-one years old at the time of the offense, the court shall enter an expungement order upon the application of such person. The expungement order shall direct that there be expunged from all official records, except the nonpublic records referred to in subsection (b), all references to his arrest for the offense, the institution of criminal proceedings against him, and the results thereof. The effect of the order shall be to restore such person, in the contemplation of the law, to the status he occupied before such arrest or institution of criminal proceedings. A person concerning whom such an order has been entered shall not be held thereafter under any provision of law to be guilty of perjury, false swearing, or making a false statement by reason of his failure to recite or acknowledge such arrests or institution of criminal proceedings, or the results thereof, in response to an inquiry made of him for any purpose."

474 42 U. S. C. § 14132 (d): "Expungement of records –
(1) By Director
(A) The Director of the Federal Bureau of Investigation shall promptly expunge from the index described in subsection (a) the DNA analysis of a person included in the index—
(i) on the basis of conviction for a qualifying Federal offense or a qualifying District of Columbia offense (as determined under sections 14135a and 14135b of this title, respectively), if the Director receives, for each conviction of the person of a qualifying offense, a certified copy of a final court order establishing that such conviction has been overturned; or
(ii) on the basis of an arrest under the authority of the United States, if the Attorney General receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.
(B) For purposes of subparagraph (A), the term "qualifying offense" means any of the following offenses:
(i) A qualifying Federal offense, as determined under section 14135a of this title.
(ii) A qualifying District of Columbia offense, as determined under section 14135b of this title.
(iii) A qualifying military offense, as determined under section 1565 of title 10.

ermächtigt, Daten über disziplinarische Angelegenheiten zu tilgen, die sich auf die beruflichen Verhaltensweisen oder Kompetenzen von *Veterans Health Administration*-Mitarbeitern beziehen.[475] Hierbei vertraten zahlreiche *Courts of Appeal* die Auffassung, dass es keine gerichtliche Befugnis gibt, Bundesstrafregistrierungen ohne eine bestimmte Gesetzgebung oder außerordentlich selten vorliegende und außergewöhnliche Umstände zu tilgen.[476] Die Bundesgerichte haben entschieden, dass die Tilgung dennoch aufgrund der einem Gericht innewohnenden Befugnisse oder vorbehaltlich der Ausübung der Nebenhoheit gewährt werden kann.[477] Aufgrund der Entscheidung des Supreme Courts im Jahr 1994, mit der die

---

(C) For purposes of subparagraph (A), a court order is not "final" if time remains for an appeal or application for discretionary review with respect to the order.
(2) By States
(A) As a condition of access to the index described in subsection (a), a State shall promptly expunge from that index the DNA analysis of a person included in the index by that State if—
(i) the responsible agency or official of that State receives, for each conviction of the person of an offense on the basis of which that analysis was or could have been included in the index, a certified copy of a final court order establishing that such conviction has been overturned; or
(ii) the person has not been convicted of an offense on the basis of which that analysis was or could have been included in the index, and the responsible agency or official of that State receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.
(B) For purposes of subparagraph (A), a court order is not "final" if time remains for an appeal or application for discretionary review with respect to the order."

475 38 U. S. C. § 7462 (d) (1). "After resolving any question as to whether a matter involves professional conduct or competence, the Secretary shall cause to be executed the decision of the Disciplinary Appeals Board in a timely manner and in any event in not more than 90 days after the decision of the Board is received by the Secretary. Pursuant to the board's decision, the Secretary may order reinstatement, award back pay, and provide such other remedies as the board found appropriate relating directly to the proposed action, including expungement of records relating to the action."

476 Siehe auch *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 2.

477 Nur ein Bundesgericht stimmte zu, dass das Gesetz Bundesgerichte dazu befugt, Strafregistrierungen zu tilgen (United States v. Bohr, 406 F. Supp. S. 1218).

Nebenhoheit der Untergerichte begrenzt wurde,[478] sind die Circuit Courts in ihrer Ansichten darüber, ob die Tilgung nur aus gerechten Gründen in Betracht gezogen werden kann, gespalten. Der Supreme Court hatte inzwischen zwei Gelegenheiten, die Standpunktverschiedenheit der Circuit Courts zu lösen. Er hat sie jedoch nicht genutzt.[479]

Es herrscht jedenfalls Einigkeit darüber, dass auf der einzelstaatlichen Ebene keine gesetzliche Bestimmung über die bestimmte Speicherdauer von Strafregistrierungen existiert. Die *criminal history records* können jedoch auf staatlicher Ebene die Tilgung in irgendeiner Form genießen, obwohl die Gesetze je nach Einzelstaat unterschiedlich sind. In der Tat bietet jeder Staat unter bestimmten Umständen in irgendeiner Weise eine Form des *expungement*, wenn auch nur in begrenztem Ausmaß.[480] Insgesamt 36 Einzelstaaten gestatten es Einzelpersonen, dass ihre Strafverfahrensdaten ohne Verurteilung aus dem Strafregister gelöscht werden, wenn die Anklagen gegen sie fallengelassen oder sie im Strafverfahren freigesprochen wurden. Eine beträchtliche Anzahl von Einzelstaaten (24) sieht ferner die Löschung von Verurteilungen vor.[481] Die Strafverfahrensdaten ohne Verurteilungen allein haben ein beträchtliches Potenzial für nachteilige Folgen in den Bereichen der privaten Beschäftigung, der staatlichen Beschäftigung, der staatlichen Leistungen, der Zulassung zum Militär und des Erwerbs von Krediten. Ein ehemaliger Angeklagter verliert unter anderem seinen guten Ruf und hat Schwierigkeiten bei der Erlangung einer Anstellung, selbst wenn die Anklage fallen gelassen wurde. Eine Person, über die es Strafverfahrensdaten gibt, kann darüber hinaus Nachteile in verschiedenen weiteren Bereichen erfahren: die Vertreibung aufgrund einer Verhaftung vor einer Verurteilung oder die permanente Sperrung für den öffentlichen Wohnungsbau aufgrund einer Verurteilung;[482] Schwierigkeiten bei der Rückkehr in die Schule, als Konsequenz von *Federal Student Aid Ineligibi-*

478 Kokkonen v. Guardian Life Ins. Co. of Am., 511 U. S. 375 (1994).

479 Siehe *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, 2013, S. 10 m. w. N (Rowlands v. United States, 127 S. Ct. 598 (2006) (cert. denied); United States v. Coloian, 128 S. Ct. 377 (2007) (cert. denied).

480 Wenn ein *criminal history record* versiegelt wird, hat die Öffentlichkeit keinen Zugang dazu, es sei denn, dass dies vom *district court* aus gutem Grund angeordnet wird. Bestimmte Strafjustizbehörden haben jedoch Zugang zu versiegelten Strafregistrierungen in ihrer Gesamtheit. Wenn die Daten demgegenüber getilgt werden, werden sie endgültig gelöscht.

481 *McAdoo*, Creating an expungement statute for the District of Columbia: A Report and Proposed Legislation, S. 1.

482 Department of Housing and Urban Development v. Rucker, 535 U. S. 125.

lity aufgrund bestimmter Verurteilungen;[483] ein lebenslanges Verbot von *Food Stamps* und *Temporary Assistance to Needy Families*;[484] Hindernisse für ein Familienleben wie ein Verbot von Pflege- und Adoptionsprogrammen.[485] Die Tilgung ist deshalb von Bedeutung, weil kollaterale Konsequenzen für die nicht gelöschten und damit ewig aufbewahrten Strafregistrierungen die Wiedereingliederung und die Rehabilitation von Straftätern (auch von ehemaligen Angeklagten) vereiteln und Rückfälligkeit fördern könnten.

Die Staaten haben unterschiedliche Mechanismen, um die Eintragungen in ihrem Strafregister zu tilgen. Zum Beispiel erlaubt der *California Penal Code* die Tilgungsbegünstigung von *Strafverfahrensdaten ohne Verurteilungen* für Verbrechen nur unter bestimmten Voraussetzungen: Wenn keine Anklage eingereicht wird, kann eine Person bei einer zuständigen Strafverfolgungsbehörde beantragen, ihre Daten löschen zu lassen. Die Behörde kann die Daten dieser Person nach der Feststellung der tatsächlichen Unschuld mit der Zustimmung der Staatsanwaltschaft versiegeln. Das Gleiche gilt, wenn ein Hauptverfahren eröffnet, aber der Angeklagte nicht verurteilt wurde. Das Gericht kann nach einem Freispruch auch von sich aus anordnen, die Daten zu versiegeln.[486] Maryland gewährt die Tilgung demgegenüber nicht nur bezüglich Strafverfahrensdaten ohne Verurteilungen, sondern auch bezüglich Verurteilungsdaten unter bestimmten anderen Voraussetzungen: bei allen Verbrechen außer Gewaltverbrechen, wenn die Verurteilung aufgehoben wird und wenn keine weiteren Verurteilungen (außer geringfügigen Verkehrsverstößen) oder anhängigen Verfahren vorliegen.[487] Die verschiedenen Elemente, die für eine Tilgungsentscheidung bedeutend sind – wie etwa Datenarten, Objektverbrechen, Wartezeiten bei einer entschiedenen Tilgung, die Möglichkeit von Rückfällen, die Beweislast und die Verwertungsmöglichkeit sowie das Schweigerecht des Betroffenen nach einer Begünstigung –, sind je nach Einzelstaat unterschiedlich geregelt. Dies ist besonders beunruhigend, da sich viele Staatsdelikte oder gleichwertige (d. h. ungeordnete) Straftaten mit Bundesdelikten überschneiden, und zahlreiche Verbrechen auf staatlicher Ebene haben fast identische föderale Gegenstücke, aufgrund derer Täter angeklagt werden können. Ob ein einmaliger minderjähriger Täter

483 20 U. S. C. 1091 (r).
484 21 U. S. C. 862a (a).
485 42 U. S. C. 671 (20) (a).
486 California Penal Code sec. 851.8.
487 Maryland Criminal Procedure Code Ann sec. 10-103.

oder ein Angeklagter, der sich als unschuldig erwiesen hat, dauerhaft mit dem Stigma einer Eintragung im Strafregister versehen wird, kann davon abhängen, wo er wegen der Straftat angeklagt wurde und ob er vor einem Einzelstaats- oder vor einem Bundesgericht angeklagt wurde.

Wird ein Blick auf die Tilgungsregelungen je nach Datenart auf einzelstaatlicher Ebene geworfen, kann Folgendes festgestellt werden: 26 Einzelstaaten erlauben die Tilgung von DNA-Daten nach einer Abweisung einer Verurteilung.[488] Jugendregistrierungen können in den meisten Staaten gelöscht werden, nachdem ein Minderjähriger das 18. oder das 21. Lebensjahr vollendet hat und die Person später nicht wegen eines anderen Verbrechens verurteilt wurde. Ein Verbrechen darf nur in einigen Staaten gelöscht werden. In den meisten Staaten können die Verhaftungsdaten, die nicht zu einer Verurteilung oder zu einer *guilty plea* führen, gelöscht werden, wenn für eine bestimmte Zeit keine weiteren Anklagen oder Verurteilungen vorliegen.[489] Die eine Tilgung ersuchende Person muss sich

---

488 ALA. CODE § 36-18-26 (2005); ARIZ. REV. STAT. § 13-610 (2004); CAL. PENAL CODE § 299 (Deering 2005); CONN. GEN. STAT. § 54-1021 (2004); DEL. CODE ANN. tit. 29, § 4713 (2005); GA. CODE ANN. § 24-4-65 (2004); IDAHO CODE § 19-5513 (Michie 2004); 730 ILL. COMP. STAT. § 5/5-4-3 (2005); IND. CODE ANN. § 10-13-6-18 (Michie 2004); KY. REV. STAT. ANN. § 17.175 (Michie 2004); LA. REV. STAT. ANN. § 15:614 (2004); ME. REV. STAT. ANN. tit. 25, § 1577 (2004); MASS. GEN. LAWS ch. 22E, § 15 (2004); MO. REV. STAT. § 650.055 (2004); MONT. CODE ANN. § 44-6-107 (2004); NEB. REV. STAT. § 29-4109 (2004); N.H. REV. STAT. ANN. § 651-C:5 (2004); N.J. REV. STAT. § 53:1-20.25 (2004); N.Y. [EXEC.] LAW § 995-c (Consol. 2005); N.C. GEN. STAT.§ 15A-148 (2004); N.D. CENT. CODE § 31-13-07 (2004); 44 PA. CONS. STAT. ANN.§ 2321 (West 2004); R.I. GEN. LAWS § 121.5-13 (2004); S.C. CODE ANN. § 23-3-660 (2004); S.D. CODIFIED LAWS § 23-5A-28 (Michie 2003); TEX. GOV'T CODE ANN. § 411.151 (Vernon 2004); VT. STAT. ANN. tit. 20 § 1940 (2004); VA. CODE ANN. § 19.2-310.7 (Michie 2004); W.V. CODE ANN. § 15-2B-11 (Michie 2005); WIS. STAT. ANN. § 165.77(4) (West 2004); WYO. STAT. ANN. § 7-19-405 (Michie 2004). Die Tilgung von DNA-Daten kommt meistens bei der Umkehrung von Verurteilungen, der fehlgeschlagenen Anklageerhebung und beim Ablehnungsbeschluss der Eröffnung des Hauptverfahrens aufgrund der Anklage vor.

489 ALASKA STAT. § 12.55.085 (Michie 2004) (conviction may be set aside if person was discharged by court without imposition of a sentence); ARK. CODE ANN. § 16-93-303 (Michie 2005) (first-time offender who completed probation, without a judgment of guilty, may have his record expunged); CAL. PENAL CODE § 851.85 (Deering 2005) (person acquitted of charge, if found factually innocent by the court, may have his records sealed); CONN. GEN. STAT. § 54-142a (2004) (person found not guilty of a charge, or if his charge is dismissed, may have his records erased upon expiration of time period for appeal);

in der Regel bei einer zuständigen Behörde melden und von sich aus Unterlagen zur Unterstützung der gewünschten Maßnahme vorlegen. In einigen Staaten muss eine Person, die eine Tilgung ersucht, die tatsächliche Unschuld beweisen.[490] Nebraska verlangt, dass Einzelpersonen durch klare und überzeugende Beweise zeigen, dass sie versehentlich verhaftet wurden,

---

DEL. CODE ANN. tit. 10, § 1025 (2005) (person may request expungement of criminal records if charge is dismissed or not otherwise prosecuted); GA. CODE ANN. § 353-37 (2004) (person arrested for an offense but not prosecuted, or if charges are dismissed, may request expungement of records); 20 ILL. COMP. STAT. § 2630/5 (2005) (person acquitted or released without being convicted may request expungement of records upon showing good cause); IND. CODE ANN. § 35-38-5-1 (Michie 2004) (person may request expungement of arrest record if no charges filed, charges dropped due to mistake, no offense was committed, or upon an absence of probable cause); KAN. STAT. ANN. § 22-2410 (2005) (person may request expungement of arrest record); KY. REV. STAT. ANN. § 431.076 (Michie 2004) (person charged but found not guilty, or against whom charges were dismissed, may request expungement of all records, including arrest records, fingerprints, photographs and other data); MD. CODE ANN. [CRIM. PROC.] § 10-103 (LexisNexis 2004) (person may request expungement of arrest record if no charges filed); MISS. CODE ANN. § 99-15-57 (2004 (records shall be expunged if case dismissed or otherwise not prosecuted); N.J. REV. STAT. § 2C:52-6 (2004) (if arrest does not result in conviction, record may be expunged); N.C. GEN. STAT. § 15A-146 (2004) (arrest that does not result in conviction may be expunged); OHIO REV. STAT. ANN. § 2953.52 (Anderson 2005) (person may request sealing of records anytime after found not guilty or charges dismissed, or after two years from the return of no bill by a grand jury); OKLA. STAT. tit. 22 § 18 (2004) (person arrested with no charges filed, or upon reversal of conviction, may request expungement); 18 PA. CONS. STAT. ANN. § 9122 (arrest records expunged after eighteen months from date of arrest upon order or certification of no proceedings); S.C. CODE ANN. § 17-1-40 (2004) (arrest records expunged if acquitted or charges dismissed); TENN. CODE ANN. § 40-32-101 (2004) (expungement of arrest records available at no cost if acquitted, charges dismissed, arrested without charges, or no bill returned by a grand jury); UTAH CODE ANN. §§ 77-18-9 – 15 (2005) (expungement of arrest records available if released without charges filed, charges dismissed or acquitted); VA. CODE ANN. § 19.2-392.2 (Michie 2004) (person may request expungement if charged and acquitted, pardoned, or charges dismissed); W. V. CODE ANN. § 61-11-25 (Michie 2005) (person found not guilty or charged dismissed may apply for expungement of arrest records if no previous felony convictions); WYO. STAT. ANN. § 7-13-1401 (Michie 2004) (person may request expungement if at least 180 days since arrested and no charges filed or charges dismissed).

490 *Diehm*, Federal Expungement: A Concept in Need of a Definition, St. John's Law Review, Vol 66. No. 1, 1992, 73, 74.

um ihre Verhaftungsdaten löschen zu lassen.[491] Im Gegensatz dazu hält Maine die Informationen automatisch geheim, wenn keine Verurteilung erfolgt.[492]

Die Löschung von Verurteilungsdaten wird in der Regel dem Ermessen des Gerichts überlassen, wenn der Angeklagte nicht innerhalb einer bestimmten Frist weitere Verurteilungen erhält, nachdem er aus der Haft oder aus der Bewährung entlassen wurde. Fast jedes Gericht erlaubt die Tilgungsbegünstigung für ein erstmaliges Vergehen, insbesondere wenn es von einem Minderjährigen begangen wurde, solange über einen bestimmten Zeitraum hinweg – in der Regel zwei bis fünf Jahre – keine weiteren Verurteilungen vorliegen.[493] Verurteilungen, die rückgängig gemacht oder abgelehnt wurden, werden auf Anfrage oft gelöscht. Darauf muss der Angeklagte jedoch je nach Schwere des Verbrechens zwischen einem und zehn Jahren warten.[494] Die Verhaftungsdaten können in den meisten Staaten gelöscht werden, wenn sie nicht zu einer Verurteilung führten.[495] Die Löschung der Strafregistrierungen bezüglich sexueller Verbrechen ist hingegen meistens nicht möglich. Dies erlauben nur einige Staaten unter bestimmten Umständen.[496] Die Tilgung der Sexualstrafregistrierungen gestaltet sich deshalb schwierig oder ist sogar unmöglich, weil Sexualstraftä-

---

491 NEB. REV. STAT. § 29-3523 (2004) (person may have erroneous arrest record expunged upon showing of clear and convincing evidence).

492 ME. REV. STAT. ANN. tit. 16, § 613 (2004).

493 KY. REV. STAT. ANN. § 431.078 (Michie 2004) (person convicted of a misdemeanor or other minor violation may request expungement after five years); MISS. CODE ANN. § 99-15-59 (2004) (first-time misdemeanor offender may have conviction expunged).

494 N. H. REV. STAT. ANN. § 651.5 (2004).

495 Der Zugang zu den gelöschten Daten durch öffentliche Behörden wird in Nebraska aber außerordentlich gesichert: NEB. REV. STAT. § 29-3523 (2004) („Arrest records may be sealed, except for public officials or candidates for public office, if prosecution is inactive or completed within one year").

496 In Idaho können Sexualstraftäter nach zehn Jahren eine Tilgung ihrer Strafregistrierungen und die Befreiung von ihrer Pflicht zur Registrierung in der staatlichen Datenbank beantragen, wenn sie durch eindeutige und überzeugende Nachweise belegen, dass sie nicht in Gefahr sind, erneut straffällig zu werden, und dass keine ähnlichen Anklagen anhängig sind. Für Sexualverbrechen der Personen, die wegen einer schweren Straftat verurteilt wurden, ist keine Tilgung möglich. In ähnlicher Weise können Sexualstraftäter in Nebraska eine Tilgung beantragen, wenn sie nicht mehr dazu verpflichtet sind, sich in der staatlichen Datenbank anzumelden, wenn sie durch eindeutige und überzeugende Beweise nachweisen können, dass ihnen kein Risiko einer Rückfälligkeit droht und dass keine ähnlichen Anklagen erhoben werden. Zur lebenslangen Registrierung in der staatlichen Datenbank verurteilte Straftäter können ihre

ter einem höheren Rückfallrisiko ausgesetzt sind als diejenigen, die andere Straftaten begehen, und weil die Gesellschaft Sexualstraftaten für besonders abscheulich hält. Die Staaten erlauben daher für Sexualdeliktsdaten keine Löschungsbegünstigung, selbst wenn keine Verurteilung vorliegt. Der Grund hierfür könnte darin liegen, dass die Staaten die Daten für mögliche zukünftige, damit verbundene Anklagen gegen denselben Straftäter behalten wollen. Eine solch rigorose Haltung gegenüber bestimmten Verbrechen kann zudem bei häuslicher Gewalt[497] festgestellt werden. An die Tilgung von Strafregistrierungen im Zusammenhang mit häuslicher Gewalt werden tendenziell strengere Anforderungen gestellt als an die Tilgung üblicher Verbrechen; die Tilgung ist hier im Allgemeinen aber leichter als bei Sexualstraftaten.[498]

Die Tilgung scheint dennoch höchst problematisch zu sein, nicht nur wegen ihrer begrenzten Natur, sondern auch wegen Schwierigkeiten in der Durchsetzung. Aufgrund des Systems, in dem die Daten von Gerichten geführt werden und für die Öffentlichkeit leicht zugänglich sind, und wegen der starken Verbreitung kommerzieller Informationsanbieter mit eigenen Strafregisterdatenbanken wird das einheitliche Datenmanagement schwierig. Denn es ist schwer sicherzustellen, dass die unter bestimmten Umständen schon gelöschten Datensätze vollständig, also aus allen Datenbanken gelöscht werden. Auch wenn die Tilgungsvorschrift auf staatlicher Ebene getroffen wurde, liegt das Problem darin, alle in verschiedenen Systemen gespeicherten Daten effektiv zu verwalten oder die Wirksamkeit des Informationsmanagements zu gewährleisten, da es kompliziert ist, die Strafregisterdatenbank der privaten Informationsvermittler gesetzlich einzuschränken.

Außerdem scheinen die versiegelten Daten im Strafregister dafür, dass sichergestellt wird, dass sie später, möglicherweise gemäß einer gerichtlichen Anordnung, geöffnet werden können, zwar praktischer zu sein,

---

Daten nicht löschen lassen (*McAdoo*, Creating an Expungement Statute for the District of Columbia: a Report and Proposed Legislation, S. 8).

497 Der Begriff der häuslichen Gewalt umfasst den Kindesmissbrauch, den Ehegattenmissbrauch und den Missbrauch von abhängigen Erwachsenen.

498 Vgl. N. Y. [FAM. CT. ACT] § 1051 (2005); ALA. CODE § 26-14-3 (2005); ARK. CODE ANN. § 5-28-220 (Michie 2005); COLO. REV. STAT. § 19-3-505 (2004); GA. CODE ANN. § 49-5-184 (2004); HAW. REV. STAT. ANN. § 350-2 (Michie 2004); IDAHO CODE § 39-5304 (Michie 2004); 325 ILL. COMP. STAT. § 5/7.14 (2005); ME. REV. STAT. ANN. tit. 22, § 4008 (2004); S.C. CODE ANN. § 22-5-910 (2004); R.I. GEN. LAWS § 12-1-12 (2004); S.D. CODIFIED LAWS § 26-8A-11 (Michie 2003); VT. STAT. ANN. tit. 33 § 4916 (2004).

unterliegen jedoch dem erheblichen Risiko einer absichtlichen oder versehentlichen Offenlegung. Vor dem Aufkommen des Internets konnten die Daten vielleicht erfolgreich versiegelt werden. Unter den Bedingungen der modernen Informationsverarbeitung ist eine wirksame Versiegelung jedoch weniger wahrscheinlich. Sobald bestimmte Daten für einen bestimmten Zeitraum auf einer Webseite veröffentlicht werden, können diese öffentlich verbreiteten Daten nicht mehr effektiv geheim gehalten oder vertraulich behandelt werden. Die staatliche Registerbehörde wird bei der Verwaltung ihrer Ver- oder Entsiegelungsaufgaben auf Schwierigkeiten stoßen. Zudem bleibt die Frage, ob die Arbeitgeber nach versiegelten Strafregistrierungen fragen können, und wenn sie es tun, ob eine Person, deren Daten in einem Strafregister versiegelt wurden, die Tatsache wahrheitsgemäß beantworten muss,[499,500] weil die Tilgung oder die Versiegelung gesetzlich nicht mit einem sogenannten Verwertungsverbot verbunden ist.

Neben der vielfältigen Art und den wachsenden Volumina der *criminal history records* hat sich auch der Zugang zu diesen dramatisch erweitert. Nicht nur die fortgeschrittene Informationstechnik und die zunehmende Rolle der Strafregistereintragungen im Strafverfahren, sondern auch die einzelstaatlich ermächtigten, vom Parlament zugelassenen oder sogar beauftragten *criminal background checks*, die Entstehung der blühenden Privatwirtschaft, die den *criminal background checking service* für Kunden bietet, die aggressive Übermittlung der *criminal records* für Sexualstraftäter infolge der Verbreitung der Megans Gesetze drängen darauf, angemessene Schutzmaßnahmen für hochsensible Daten einzuführen. In den USA scheint das Bewusstsein für den Schutz personenbezogener Daten im Strafverfahren aber noch unzureichend zu sein. Angesichts dessen sollten vermehrt politische Überlegungen über den effektiven und angemessenen Datenschutz im Strafverfahren angestellt werden.

---

499 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 412.

500 Insgesamt 28 Staaten erlauben es Einzelpersonen, deren Eintragungen im Strafregister gelöscht wurden, die ehemalige Existenz solcher Daten zu verschweigen, wenn sie danach gefragt werden. Dies geschieht dadurch, dass eine *Legal Fiction* geschaffen wird, die notwendig ist, um den Zweck der Tilgung zu verfolgen und die Personen von der Stigmatisierung und den lebenslangen kollateralen Konsequenzen solcher Daten zu befreien (*Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 36 m. w. N.).

II. Rasterfahndung

Nach der deutschen Rechtsordnung ist eine Rasterfahndung ein maschineller Abgleich von Daten, die sowohl bei öffentlichen als auch bei privaten Stellen gespeichert sind, um bestimmte Verdächtige festzustellen oder Nichtverdächtige auszuschließen. Der Datenabgleich, der einer Rasterfahndung im Sinne von § 98a in der deutschen StPO funktional vergleichbar ist, wird in den USA unter dem Namen des *Computer Matching* reguliert und verwendet. Seitdem das *Computer Matching* in den frühen 1970er Jahren möglich wurde, wird es heute insbesondere in der Regierungsverwaltung häufig verwendet, vorwiegend, um Gesetzesverstöße im Zusammenhang mit dem Empfang staatlicher Leistungen zu ermitteln. Der Computer Matching and Privacy Act von 1988[501] hat den Privacy Act von 1974 geändert, indem bestimmte Schutzbestimmungen für diejenigen Personen hinzugefügt wurden, deren Datensätze in den automatisierten Matching-Programmen verwendet werden. Das Gesetz schränkt die *Computer Matching*-Programme nicht ein, sondern legt nur Verfahren für Bundesbehörden fest, die sich mit dem *Computer Matching* der Daten befassen.[502] Die Verfahrensregelungen gelten nur für den Datenabgleich von Daten, die bei öffentlichen Stellen gespeichert sind, aber nicht für den Abgleich, der Datenbestände verwendet, die im Besitz Privater sind. Das beruht in den US-amerikanischen Datenschutzgesetzen vor allem auf dem Fehlen eines Konzepts, das der Idee des grundgesetzlichen Verbots mit Erlaubnisvorbehalt entspricht. Denn jede Datenverarbeitung ist in den USA grundsätzlich zulässig, sofern es keine speziellen Bestimmungen gibt, die dagegen sprechen,[503] während die Datenverarbeitung in Deutschland nur auf Basis eines Erlaubnistatbestandes zulässig ist. Die Erhebung und der Abgleich von Daten, die sich im Besitz Privater befinden, werden somit grundsätzlich gesetzlich nicht geregelt. Die gesetzliche Regelung betrifft angesichts der Gefahren staatlicher automatisierter Datenverarbeitung nur den Abgleich von Daten, die bereits bei einer Behörde gespeichert sind. Das *Computer Matching*, das dem Computer Matching and Privacy Act von 1988 unterliegt, ist also ein computergestützter Abgleich maschinen-

501 Computer Matching and Privacy Protection Act of 1988, P. L. 100–503.

502 *Solove/Schwartz*, Privacy Law: Fundamentals, S. 67.

503 Zum Beispiel der Social Security Act (42 U. S. C. § 1320b-7), der Tax Reform Act aus dem Jahr 1976 (Public Law 94–455, Department of Defense Authorization Act of 1983, Public Law 97–252) usw. Die meisten speziellen Gesetze ermächtigen aber nur dazu, einen Abgleich durchzuführen, enthalten jedoch keine weiteren Einzelheiten für die Durchführung der Maßnahme.

lesbarer Datensätze, die nur bei öffentlichen Stellen bereits gespeicherte personenbezogene Daten von vielen Personen enthalten, um Missbrauch staatlicher Leistungen festzustellen.[504] Für die Verwendung der bei einer Bundesbehörde gespeicherten Daten von einer anderen Behörde zum Zweck eines Datenabgleichs wird eine Datenübermittlung von einer Behörde zu der anderen Behörde vorausgesetzt. Dabei ist der Privacy Act von 1974 einschlägig, der allgemeine datenschutzrechtliche Bestimmungen für alle bei Bundesbehörden gespeicherten Daten enthält. Das Gesetz umfasst aber nicht den Abgleich, der bei einer privaten Stelle gespeicherte Daten verwendet.

Gegen das *Computer Matching* werden verfassungsrechtliche Bedenken erhoben, da hierfür kein Tatverdacht erforderlich ist, obwohl polizeiliche Untersuchungen nach den Grundsätzen des vierten Verfassungszusatzes und dem im fünften und sechsten Verfassungszusatz verankerten Prinzip der Unschuldsvermutung normalerweise nur beim Vorliegen eines Tatverdachts zulässig sind. Auch der Umfang der Untersuchungen, bei denen alle Personen in den betroffenen Dateien als mögliche Täter angesehen werden, ist Gegenstand von Kritik.[505] Mit der Entwicklung der Computertechnologie ist nicht nur die Fähigkeit entstanden, große Mengen an Daten zu speichern, sondern auch die Fähigkeit, Daten automatisch zu sortieren, zu extrahieren und abzugleichen. Die Bedenken hinsichtlich des Datenabgleichs werden dann besonders akut, wenn die Regierung viele sensible Daten auf einer einzigen Datenbank besitzt oder besitzen kann.

Nachfolgend soll deshalb zum einen gesondert den Rechtsgrundlagen für den Abgleich nachgegangen werden, der bereits bei öffentlichen Stellen gespeicherte Datenbestände verwendet, und zum anderen auch der Abgleich untersucht werden, der Datenbestände im Besitz Privater verwendet. Anschließend soll durch die Analyse gesetzlich getroffener spezifischer Absicherungsvorkehrungen untersucht werden, ob das Dateninteresse oder die Freiheitsrechte des Einzelnen beim Abgleich sowohl bei öffentlichen als auch bei nicht öffentlichen Stellen gespeicherter Daten entsprechend der Eingriffsintensität der Maßnahme geschützt werden.

504 5 U. S. C. § 552a (a) (8) (A).

505 *Lützner*, USA, in: *Gropp* (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, S. 763 und m. w. N.

1. Organisationsstruktur

a) Datenübermittlung als Vorbedingung eines Datenabgleichs

aa) Überblick

Ein maschineller Datenabgleich besteht vor allem aus der Datenübermittlung von einer Speicherstelle als Voraussetzung eines Abgleichs und dem automatisierten Datenabgleich als dem endgültigen Ziel. Die Einschränkung der Datenübermittlung wirkt unterschiedlich, je nachdem, wo die Daten gespeichert sind, also in den Speichersystemen der Bundesbehörden, der einzelstaatlichen Behörden oder eines privaten Unternehmens. Die Einschränkung eines maschinellen Datenabgleichs gilt nur für den Datenabgleich durch die Bundesbehörden. Wie oben erwähnt, ist in den USA grundsätzlich jede Datenverarbeitung zulässig, sofern es keine speziellen Bestimmungen gibt, die dagegen sprechen. Eine Datenübermittlung und ein computergestützter Datenabgleich sind daher ohne anderslautende Vorschriften grundsätzlich zulässig und werden in den USA nur im Bereich eines Datenabgleichs durch die Bundesbehörden geregelt.

bb) Unterschiedliche Regulierung der Übermittlung der öffentlichen und privaten Daten

Auf Bundesebene sind mehrere Gesetze im Hinblick auf den behördlichen Datenabgleich in Kraft getreten.[506] Diese Gesetze legen wichtige Grundprinzipien für das behördenübergreifende Datenmanagement auf allen Regierungsebenen fest. Das erste Bundesgesetz, das auf den Schutz des Interesses bezüglich der *data privacy* abzielte, war der Privacy Act von 1974, der unter anderem ein Verbot der behördenübergreifenden Offenlegung personenbezogener Daten ohne Zustimmung der betroffenen Person vorsah.[507] Danach dürfen die Behörden nur jene Daten über eine Person speichern und verwalten, die zu einem Zweck, der gesetzlich oder auf Anordnung des Präsidenten zu erfüllen ist, relevant und notwendig sind (5 U. S. C. § 552a (e) (1)). Eine Datenübermittlung zum Zweck eines Datenabgleichs ist grundsätzlich an eine Zustimmung der Betroffenen

506 So der Tax Reform Act of 1976, Public Law 94-455, Department of Defense Authorization Act of 1983, Public Law 97-252.

507 5 U. S. C. § 552a (b).

gebunden. Die Datenübermittlung ist also in der Regel nur dann zulässig, wenn die Datenübermittlung an eine Person oder eine andere Behörde von den Betroffenen schriftlich angefragt oder wenn ihr vorher schriftlich zugestimmt wird. Das Gesetz umfasst keinen Datenabgleich *nach* einer eingeleiteten spezifischen strafrechtlichen oder zivilrechtlichen Ermittlung einer oder mehrerer bestimmter Personen, um Beweise gegen diese Personen zu erheben. Die Auslegung des Wortlauts der Norm spricht dafür, dass die Norm nur auf das *Data Matching* angewendet wird, das zur Identifizierung einiger Verdächtigen *vor* dem Beginn einer konkreten strafrechtlichen Untersuchung durchgeführt wird.

Der Computer Matching and Privacy Protection Act von 1988, ein Änderungsgesetz des Privacy Act, sieht die Regulierung des Datenabgleichs der Bundesregierung vor.[508] Die Gesetzgebung ist zustande gekommen, weil der Privacy Act von 1974 nach der Ansicht des Kongresses für Personen, deren Daten zum Datenabgleich verwendet werden mussten, wenig Schutz bot.[509] Das Gesetz enthält explizitere Richtlinien, die regeln, wie Daten zwischen Regierungsbehörden ausgetauscht werden und inwieweit die Behörden auf der Grundlage von übermittelten und dann ausgeglichenen Daten nachteilige Maßnahmen gegen Einzelpersonen treffen dürfen. Außerdem legt das Gesetz die Standards für das ordnungsgemäße Verfahren fest, die das Ausmaß beschränken, in dem die Behörden auf der Grundlage abgeglichener Daten handeln können. Es sieht vor, dass zwischen Behörden keine Daten ausgetauscht werden dürfen, es sei denn, dies ist unter bestimmten Voraussetzungen schriftlich vereinbart (5 U. S. C. § 552a (o) (1)). Datenabgleichvorgänge unterliegen aber nicht immer, sondern nur in bestimmten Fällen diesem Gesetz. Es ist z. B. dann nicht einschlägig, wenn ein *Matching* im Anschluss an die Einleitung einer bestimmten strafrechtlichen oder zivilrechtlichen Untersuchung gegen eine oder mehrere bekannte Personen von einer Behörde (oder einem Teil davon) durchgeführt wird, die jegliche Tätigkeit im Zusammenhang mit der Durchsetzung des Strafgesetzes als ihre Hauptaufgabe führt, um Beweise gegen diese Person oder diese Personen zu sammeln.[510] Die Auslegung des Wortlauts der Norm spricht dafür, dass die Norm nur auf das *Data*

508 Mit dem Computer Matching and Privacy Protection Act (CMPPA) von 1988 ist der Schutz durch den Privacy Act auf das *matching program* ausgedehnt.

509 Siehe Committee on Government Operations, Computer Matching and Privacy Protection Act of 1988, H.R. Rep. No. 100–802, 100th Cong., 2d Sess. 3107, 1988 (3114).

510 5 U. S. C. § 552a (a) (8) (B) (iii).

Matching angewendet wird, das zur Identifizierung einiger Verdächtigen *vor* dem Beginn einer konkreten strafrechtlichen Untersuchung durchgeführt wird.

Beim EDV-Abgleich, der Datenbestände im Besitz Privater verwendet, verhält sich dies anders. Dieser Unterschied beruht auf der Tatsache, dass im Privacy Act die Unterstützungspflicht einer Speicherstelle, die keine öffentliche Stelle ist, nicht berücksichtigt wird und es im Privatsektor so gut wie keine datenschutzrechtlichen Regelungen gibt.[511] Die datenschutzrechtlichen Belange wurden hier nur in einigen Industriezweigen gesetzlich geregelt, etwa im Finanzsektor, in der Telekommunikationsindustrie, im Hochschulbereich und in der Fernsehindustrie. Unter diesen Bedingungen verfügen die Ermittlungsbehörden über eine Reihe von Instrumenten, um auf die Daten des Privatsektors zugreifen zu können; dies sind zum einen die unverbindlichen und zum anderen die verbindlichen Möglichkeiten. Die Ermittlungsbehörden können Daten unverbindlich auf dem Datenmarkt entgeltlich erwerben. In vielen Staaten verkauft beispielsweise das Verkehrsamt Listen von Führerschein- und Autoinhabern, die unter anderem Geburtsdaten und die gefahrenen Automarken enthalten. Dies beruht auf der Verkürzung des Schutzes der begründeten Erwartung auf *privacy* durch die *third party doctrine*. Dabei können Daten, die einmal an Dritte weitergegeben wurden, keinen Schutz mehr genießen.[512] Können Daten nicht entgeltlich erworben werden, hängt der Zugang der Ermittlungsbehörde zu Daten von der Kooperationsbereitschaft der jeweiligen Datenbesitzer ab. Viele Datenbesitzer wollen Daten für polizeiliche Ermittlungszwecke ohne Vorlage einer *subpoena* oder einer anderen vergleichbaren gerichtlichen Anordnung aber nicht herausgeben.[513] Ohne

511 *Lützner*, USA, in: *Gropp* (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, S. 759 und m. w. N.: „Als Begründung wird angeführt, dass die unterschiedliche Größe und Belange der verschiedenen Industriezweige einen Ausgleich zwischen dem Datenschutz und den legitimen Interessen Dritter an bestimmten Daten in einem einzelnen Gesetz nicht ermögliche."

512 Smith v. Maryland, 442 U. S. 735 (1979); Couch v. United States, 409 U. S. 322 (1973); United States v. Miller, 425 U. S. 435 (1976). Die unteren Gerichte haben die *third party doctrine* in großem Umfang angewandt, etwa auf die Daten über die Internetnutzung einer Person, die durch ISPs gespeichert sind: United States v. Forrester, 512 F. 3d 500 (9th Cir. 2008); Guest v. Leis, 255 F. 3d 325 (6th Cir. 2001).

513 In einer umfassenden Umfrage der University of Illinois über den Umgang mit Daten bei den größten amerikanischen Firmen erklärten 62 Prozent der Befragten, dass Daten nur gegen Vorlage einer *subpoena* einer staatlichen Stelle

subpoena o. Ä. ist also kaum zu erwarten, dass die privaten Datenbesitzer der Strafverfolgungsbehörde willig ihre Daten weiterleiten und den Datenabgleich unterstützen. Der Staat verfügt außerdem über eine Reihe von verbindlichen Instrumenten, um auf die Daten des privaten Sektors zuzugreifen: Gesetze mit Meldepflichten (z. B. der Bank Secrecy Act), *National Security Letters* (NSLs) oder *subpoena* bzw. eine gerichtliche Anordnung. Der Bank Secrecy Act schreibt die Aufbewahrung von Bankunterlagen und die Erstellung von Berichten vor, die für strafrechtliche, steuerliche oder behördliche Ermittlungen oder Verfahren nützlich sind. Erforderlich ist, dass die bundesweit versicherten Banken die Identität der Kontoinhaber sowie Kopien jedes Schecks, Wechsels oder sonstigen Finanzinstruments speichern müssen (12 U. S. C. § 1829b). Viele Bundesdatenschutzgesetze sehen den behördlichen Zugang zu privaten Daten durch eine gerichtliche Anordnung oder *subpoena* vor, die die lockeren Standards für den Zugang zu Daten enthalten, also weniger strikt als *probable cause* sind. Ein Beispiel hierfür ist der Right to Financial Privacy Act (REPA),[514] der vorschreibt, dass die Finanzdaten einer Person nur aufgrund einer *subpoena* oder eines Durchsuchungsbefehls an die staatlichen Behörden weitergegeben werden dürfen. Die *National Security Letters*[515] sind ein weiterer Mechanismus, mit dem die Behörden Daten aus dem privaten Sektor erhalten können. Damit darf das FBI die Vorlage von Daten verlangen, wenn dies für das Sammeln ausländischer Geheimdienste oder eine Terrorismusermittlung von Belang ist. Eine weitere Zugriffsermächtigung des FBI kommt aus den PATRIOT Act *§ 215 Orders*. Diese Vorschriften aus dem PATRIOT Act erlauben es

---

zugänglich gemacht werden. Hierzu ausführlich *Linowes*, Privacy in America: Is Your Private Life in the Public Eye? Urbana [u. a.], Univ. of Illinois Press, 1989, S. 44.

514 Der Right to Financial Privacy Act von 1978, Pub. L. 95 – 630, 29 U. S. C. §§ 3407. Weitere Gesetze, die von den staatlichen Behörden verlangen, eine gerichtliche Anordnung oder *subpoena* zu erhalten, um auf private Daten zuzugreifen, sind z. B. der Cable Communications Policy Act (CCPA), 47 U. S. C. § 551 (h), der Fair Credit Report Act (FCRA), 15 U. S. C. § 1681 f, der Health Insurance Portability and Accountability Act (HIPAA), 45 C. F. R. § 164.512 (f) (1), der Pen Register Act, 18 U. S. C. § 3123(a), der Stored Communications Act (SCA), 18 U. S. C. § 2703 und der Video Privacy Protection Act (VPPA), 18 U. S. C. § 2710 (b) (2) (C).

515 Die National Security Letters (NSLs) sind ein außergewöhnliches Durchsuchungsverfahren, mit dem das FBI die Offenlegung von Kundendaten erzwingen kann, die Banken, Telefongesellschaften, Internet Service Provider und andere bewahren. Zum Beispiel der Stored Communications Act, 18 U. S. C. § 2709; der Right to Financial Privacy Act, 12 U. S. C. § 3414 (a) (5) (A); der Fair Credit Reporting Act, 15 U. S. C. § 1671u.

dem FBI, die Vorlage von materiellen Gegenständen für Ermittlungen zum Schutz gegen internationalen Terrorismus oder Geheimdienstaktivitäten anzuordnen, es sei denn, dass solche Ermittlungen gegen US-amerikanische Bürger ausschließlich auf der Grundlage von Aktivitäten durchgeführt werden, die durch den ersten Verfassungszusatz geschützt werden. Ein Antrag auf eine *Section 215 Order* ist an einen Richter zu richten und es ist anzugeben, dass die Daten für eine befugte Ermittlung eingeholt werden sollen.

Daten, die von Behörden gespeichert oder privat aufbewahrt werden, können, wie oben erklärt, zum Zweck des Datenabgleichs auf unterschiedliche Weise an die Ermittlungsbehörden übermittelt werden. Die übermittelten Daten bilden eine Vorbedingung eines maschinellen Datenabgleichs.

b) Funktionsweise des Datenabgleichs

Der Computer Matching and Privacy Protection Act (CMPPA) begründet die Verfahren für den maschinellen Datenabgleich durch die Bundesbehörden. Das Gesetz schränkt die *matching programs* nicht ein, sondern fordert von den Behörden, die Verfahren zu veröffentlichen und die Betroffenen vor dem Abgleich zu benachrichtigen. Behörden, die einen maschinellen Datenabgleich vornehmen wollen, müssen außerdem ein *data integrity board* einrichten und eine Genehmigung vom *board* erhalten. Dabei kommt es nicht darauf an, ob die Daten bei den öffentlichen Behörden oder bei Privaten gespeichert sind. Wenn die Daten zum maschinellen Datenabgleich an die Bundesbehörden übermittelt werden, gilt dafür das CMPPA. Das Gesetz erfordert eine Benachrichtigung vor dem einzelnen Datenabgleich, um das Recht der Betroffenen zu schützen.

Die auf diese Weise übermittelten Daten werden folgenderweise abgeglichen:

(1) Von jeder Datenbank, die als Quelle für das Datenabgleichprogramm verwendet wird, werden alle verfügbaren Datenelemente aus allen verfügbaren Datensätzen ausgewählt. (2) Gegebenenfalls finden Datenbereinigungsoperationen statt, damit die Organisation, das Format und der Inhalt einer oder mehrerer Dateien in eine für den Abgleichsschritt geeignete Form geändert werden. (3) Danach wird ein Matching durchgeführt, wobei auf die Dateien mit personenbezogenen Daten ein Matching-Algorithmus angewendet wird, um Treffer zu finden. Damit sind übereinstimmende Datensätze gemeint, die sich auf dieselbe Person beziehen. (4)

Es kommt dann zu einer Inferenz, bei der eine Inferenzprozedur auf das Ergebnis des Abgleichprozesses angewendet wird (d. h. entweder auf den Inhalt von übereinstimmenden Datensatzpaaren oder auf das Vorhandensein oder Nichtvorhandensein von Übereinstimmungen). Der Zweck dieses Schritts ist es, Rückschlüsse auf die Person zu erhalten, auf die sich die Daten beziehen, oder auf ihr Verhalten, ihre Handlungen oder Neigungen. (5) Treffer werden in diesem Schritt gefiltert, um einen effizienten Einsatz von Ermittlungsressourcen zu gewährleisten und ungerechtfertigte Verwaltungsmaßnahmen zu vermeiden. (6) Auf Grundlage der Analyse von resultierenden Informationen werden Entscheidungen getroffen und Maßnahmen ergriffen. (7) Gegebenenfalls werden neue Datensätze erstellt oder die bestehenden Datensätze geändert oder erweitert. (8) Eine Qualitätsanalyse kann auf allen Stufen ein Feedback generieren, das eine Rückkehr zu früheren Schritten erfordert.[516]

2. Abgleichbare Daten

5 U. S. C. § 552a (a) (4) erwähnt als für einen Abgleich verfügbare Daten alle Artikel, Sammlungen oder Gruppierungen von Informationen über eine Person, die von einer Behörde geführt werden, einschließlich – aber nicht darauf beschränkt – ihrer Ausbildung, Finanztransaktionen, der medizinischen Vorgeschichte, der Straf- oder Beschäftigungsgeschichte, und Daten, die den Namen der Person oder die identifizierende Nummer, das Symbol oder ein anderes identifizierendes Merkmal enthalten, das der Person zugewiesen werden kann, wie etwa ein Finger- oder Stimmabdruck oder ein Foto. Die Vorschrift sieht also keine Beschränkungen für bestimmte personenbezogene Daten vor, die zum Abgleich verwendet werden dürfen. Es gibt viele Möglichkeiten, wie Daten in den Besitz einer Behörde gelangen können: Sie können von der Behörde erstellt werden oder durch Beobachtung der betroffenen Person oder ihres Verhaltens oder als Nebenprodukt einer Transaktion zwischen der Behörde und der betroffenen Person erstellt werden. Die Behörde kann die Daten auch von der betroffenen Person selbst, von einer anderen Behörde oder erneut von einer Behörde erwerben, an die sie weitergegeben wurden.[517] All

516 *Clarke*, Dataveillance by Governments: The Technique of Computer Matching, Information Technology & People, Vol. 7 No. 2, 1994, 46.

517 *Clarke*, A Normative Regulatory Framework for Computer Matching, Vol. 13 Issue 4, Journal of Computer & Information Law, 1995, S. 598.

die Daten, die bei der Behörde auf verschiedene Weisen erworben oder erstellt und dann gespeichert wurden, können der Gegenstand eines Datenabgleichs sein.

Auch im Falle von Daten im Privatbesitz kann eine Behörde alle personenbezogenen Daten ohne Beschränkung erwerben und sie zum Abgleich verwenden, solange die Datenbesitzer zur Herausgabe von Daten für polizeiliche Ermittlungszwecke bereit sind.

3. Verwendung des Datenabgleichs

Der Privacy Act macht es von der Zustimmung der Betroffenen abhängig, ob Daten, die für einen bestimmten Zweck erhoben wurden, später für einen anderen Zweck verwendet werden dürfen. Grundsätzlich darf keine Behörde ohne Zustimmung des Betroffenen ihre Daten zur Durchführung eines Abgleichs an eine andere Stelle weiterleiten. Ungeachtet dieser Bestimmung kommt der Zustimmung des Betroffenen eine schwache Bedeutung zu. Denn im Falle eines Datentransfers zwischen Behörden derselben Regierungsebene (z. B. zwischen US-Bundesbehörden oder zwischen den Behörden eines bestimmten Staates) nehmen es Regierungsbehörden manchmal zum Vorwand, dass sie Mitglieder eines monolithischen öffentlichen Dienstes sind. Dadurch können sie behaupten, dass alle Datenübertragungen zwischen Regierungsstellen interne und nicht externe Übertragungen sind.[518] Solche totalitären Tendenzen können den Schutz des Rechts auf informationelle Selbstbestimmung mit der Kontrolle durch die verfahrensrechtlichen Vorkehrungen entmachten. Ein weiterer Faktor, der die Zustimmung der betroffenen Personen bedeutungslos macht, ist die

518 *Clarke*, Computer Matching and Digital Identity, 1993: Um dieses Problem in den Griff zu bekommen, sagt Clarke, der Gesetzgeber müsse unbedingt klarstellen, dass Behörden für die Zwecke der Datenübertragung unabhängige Organisationen sind, damit alle Datenübertragungen den Regeln für die Sammlung und Verbreitung unterliegen. Außerdem betont er eine umfassende und universell anwendbare Datenschutzgesetzgebung, die ein ausgewogenes Verhältnis zwischen den verschiedenen wirtschaftlichen und sozialen Interessen erreicht, und er fordert die Errichtung einer Kontrollstelle, die über ausreichende Befugnisse und Ressourcen verfügt, um ein angemessenes Gleichgewicht zwischen der informationellen Privatsphäre und der administrativen Effizienz zu erreichen (*Clarke*, A Normative Regulatory Framework for Computer Matching, Vol. 13 Issue 4, Journal of Computer & Information Law, 1995, S. 611 ff.; zustimmend zur Idee der Einrichtung einer solchen Stelle siehe auch *Laudon*, Computers and Bureaucratic Reform, S. 384).

Ausnahmemöglichkeit unter Verwendung des Begriffs „routine use“[519]. Der Privacy Act lässt die Ausnahmemöglichkeit offen und der Ausnahmetatbestand wird in der Praxis großzügig ausgelegt. Ein Problem liegt also darin, dass viele Abgleichvorgänge im Rahmen des *routine use*-Ausnahmetatbestandes durchgeführt werden. Ein Datenabgleich wird in der Praxis oft einfach als *routine use* von Daten betrachtet. Infolgedessen sind Behörden in der Lage, die Anforderung des Privacy Act zu umgehen, dass Einzelne der Verwendung ihrer Daten für einen anderen als den ursprünglich vorgesehenen Zweck zustimmen müssen. Der Privacy Act sieht vor, dass das *Computer Matching* durchgeführt werden kann, um die Berechtigung oder die fortwährende Einhaltung gesetzlicher oder aufsichtsrechtlicher Anforderungen von Bewerbern, Empfängern oder Begünstigten von oder Teilnehmern an der Erbringung von Dienstleistungen in Bezug auf Geld- oder Sachleistungen oder Zahlungen im Rahmen von Bundesleistungsprogrammen festzustellen oder zu überprüfen, um Zahlungen zurückzuzahlen oder Schulden im Rahmen solcher Bundesleistungsprogramme zu tilgen. Der Hauptanwendungsbereich dieser Maßnahme war bis dato die Identifizierung solcher Personen, die unberechtigt staatliche Leistungen empfangen oder beantragt haben. Die Bedeutung des Verwendungszwecks des Datenabgleichs ist aber gering, weil das *Computer Matching* häufig als Routinemaßnahme durchgeführt wird. Das Gesetz wird aufgrund eines Defekts der großzügigen Auslegung der Ausnahmetatbestände als ein „Papiertiger“ angesehen.[520] Darüber hinaus ist eine Zustimmung der Betroffenen sogar dann nicht erforderlich, wenn eine Strafverfolgungsbehörde eine schriftliche Anfrage an eine Behörde gerichtet hat, die die Daten führt, und in dieser schriftlichen Anfrage der gewünschte Teil dieser Daten und der Zweck angegeben ist, für den die Daten angefragt werden.[521]

Der Computer Matching and Privacy Protection Act von 1988 sieht zusätzliche Verfahren vor, schafft jedoch keine inhaltlichen Leitlinien, um zu bestimmen, wann ein Abgleich akzeptabel ist. Er legt Entscheidungen über einen Datenabgleich in die Hände einzelner Verwaltungsbehörden, die verpflichtet sind, bestimmte Verfahren zu befolgen. Die Durchführung eines Datenabgleichs ist beispielsweise verboten, wenn keine schriftliche

519 5 U. S. C. § 552a (a) (7): *Routine use* bedeutet die Weiterverwendung von erhobenen Daten, wenn die spätere Verwendung mit dem Erhebungszweck vergleichbar ist.

520 Siehe *Carlson/Miller*, Public Data and Personal Privacy, Santa Clara High Technology Law Journal, Vol. 16 Issue 1, 2000, S. 105.

521 5 U. S. C. § 552a (b) (7).

Vereinbarung zwischen der Speicherstelle und der Anfragestelle getroffen wurde. Eine behördenübergreifende Datenübermittlung zum Zweck eines Datenabgleichs ist also nur nach schriftlicher Vereinbarung zwischen der Speicherstelle und der Anfragestelle möglich. Denn das Gesetz sieht vor, dass Daten zwischen Behörden nicht ausgetauscht werden dürfen, es sei denn, dies ist unter bestimmten Voraussetzungen schriftlich vereinbart. Die Matching-Vereinbarungen müssen den Zweck des geplanten Datenabgleichs festlegen, die Datensätze beschreiben, die abgeglichen werden, und Verfahren zur Benachrichtigung über unerwünschte Ereignisse auf der Grundlage eines Datenabgleichs festlegen.[522]

4. Aufbewahrungsdauer der Daten

Trotz Bemühungen auf Bundesebene, die mit dem Datenabgleich verbundenen Privacy-Interessen zu berücksichtigen, gibt es keine Bestimmungen, die Aufbewahrungsdauer für die Ergebnisse eines Datenabgleichs mit sowohl bei öffentlichen als auch bei privaten Stellen gespeicherten Daten zu beschränken. Die Aufbewahrungsdauer der Daten hängt also nur von der schriftlichen Vereinbarung ab, aufgrund derer die Behörden Daten austauschen können.[523] Nach 5 U. S. C. § 552a (o) (1) (I) soll die schriftliche Vereinbarung Verfahren für die Rückgabe der Datensätze an die Speicherstelle oder die Vernichtung von Datensätzen enthalten, die in einem Datenabgleich verwendet werden. Bestimmte Aufbewahrungsfristen, Rückgabezeiten von Daten an eine Speicherstelle oder Löschungs- oder Vernichtungszeiten nach einem Abgleich sind nicht gesetzlich festgelegt. Dies gilt auch für den Abgleich der Daten, die auf dem Datenmarkt entgeltlich gekauft oder von einer privaten Stelle aufgrund einer *subpoena* oder einer gerichtlichen Anordnung erhalten wurden. In diesem Fall ist nicht einmal eine schriftliche Vereinbarung erforderlich.

Es gibt zwar keine Löschungsregelungen für die Daten, die in den Speichersystemen privater Unternehmen gespeichert sind, aber zahlreiche Bundesstaaten haben Gesetze, nach denen ein Unternehmen personenbe-

522 Zu den Einzelheiten der sog. *matching agreements* 5 U. S. C. § 552a (o) (1).

523 Aufgrund dieser fehlenden externen Kontrolle über das *Computer Matching* argumentiert *Laudon*, dass eine Datenschutzgesetzgebung der zweiten Generation erforderlich sei (*Laudon*, Computers and Bureaucratic Reform, S. 400).

zogene Daten sicher und effektiv vernichten muss, wenn es die Daten nicht mehr speichern will.[524]

5. Mitteilungspflicht

Die *vor* dem Abgleich erforderlichen Verfahren werden durch wichtige Schutzmaßnahmen für die Bürger *nach* dem Datenabgleich flankiert. Die notwendigen Schutzmaßnahmen sind in 5 U. S. C. (p) geregelt. Die erste Maßnahme betrifft die Frage, inwieweit eine unabhängige Überprüfung der in einem Abgleich verwendeten personenbezogenen Daten erforderlich ist, bevor die Behörde Maßnahmen in Bezug auf die Person ergreift. Verlangt wird entweder, (1) dass ein Beamter der Behörde eine unabhängige Überprüfung der Daten bezüglich nachteiliger Maßnahmen gegen jede Person unternimmt, deren Daten in *matching programs* verwendet werden, oder (2) dass die Daten auf die Identifizierung und die Höhe der Leistungen beschränkt sind, die von einer Speicherstelle im Rahmen eines staatlichen Leistungsprogramms gezahlt werden, und dass ein hohes Maß an Vertrauen besteht, dass die der Anfragestelle zur Verfügung gestellten Daten zutreffend sind.[525] Der Privacy Act verlangt, dass die Betroffenen eine Mitteilung von der Behörde erhalten, die eine Erklärung ihrer Ergebnisse beinhaltet, und dass sie über die Möglichkeit informiert werden, solche Feststellungen anzufechten. Personen müssen nach dem Gesetz also benachrichtigt werden, wenn Leistungen aufgrund von übereinstimmenden Daten reduziert oder gekündigt werden sollen, und sie können eine Frist von dreißig Tagen haben, um die Ergebnisse anzufechten. Der Computer Matching Act verpflichtet die Behörden dazu, die Benachrichtigungsme-

524 Alaska Stat. § 45.48.500; Ariz. Rev. Stat. § 44-7601; Ark. Code Ann. § 4-110-104; Cal. Civ. Code § 1798.81; Colo. Rev. Stat. § 6-1-713; Conn. Gen. Stat. Ann. § 42-471; Ga. Code § 10-15-2; Haw. Rev. Stat. § 487R-2; 20 ILCS 450/20; Ind. Code §§ 24-4-14-8 und 24-4.9-3-3.5(c); Kan. Stat. Ann. § 50-7a03; Ky. Rev. Stat. § 365.725; Mass. Gen. Laws Ch. 931, § 2; Md. Code, Comm. Law § 14-3507; MCL § 445.72a; Mo. Stat. § 288.360; Mont. Code Ann. § 30-14-1703; Nev. Rev. Stat. § 603A.200; N.J. Stat. § 56:8-162; N.Y. Gen. Bus. Law § 399-H; N.C. Gen. Stat. § 75-64; Ore. Rev. Stat. § 646A.622; R.I. Gen. Laws § 6-52-2; S.C. Code § 37-20-190; Tex. Bus. & Com. Code. Ann. § 72.004; Utah Code Ann. § 13-44-201; 9 Vt. Stat. Ann. § 2445; Wash. Rev. Code § 19.215.020; Wisc. Stat. § 134.97.

525 5 U. S. C. 552a (p) (1) (A). Die zweite Alternative schwächt die Erfordernis einer unabhängigen Verifizierung durch die Forderung nach der generellen Genauigkeit der Daten.

thode der betroffenen Personen in der Vereinbarung anzugeben. Obwohl der Computer Matching Act keine inhaltlichen Anforderungen für die Entscheidung enthält, wann ein Datenabgleich angemessen ist, bietet er einige Verfahrensschutzmaßnahmen für den Einzelnen, einschließlich dieser Möglichkeit, nach dem Datenabgleich der Genauigkeit der Ergebnisse zu widersprechen. Die Benachrichtigungspflicht an Einzelpersonen ist aber nicht mit einem Datenabgleich als solchem, sondern mit den nachteiligen Maßnahmen aufgrund von Ergebnissen eines Datenabgleichs verbunden. Wird also keine nachteilige Maßnahme getroffen, findet auch keine Benachrichtigung statt.

Eine Bundesbehörde darf zur Durchführung eines Abgleichs grundsätzlich nur mit der Zustimmung des Betroffenen dessen Daten an eine andere Stelle weiterleiten. Dass die Bedeutung dieser Beschränkungsvorschrift wegen der großzügigen Auslegung der Ausnahmetatbestände verlorengegangen ist, wurde oben bereits dargelegt. Die spezifische Kontrolle, die der Computer Matching Act zum Datenschutz eines Einzelnen vorsieht, erfolgt in zwei Richtungen: zum einen als Information an den Kongress, zum anderen als die Einrichtung eines Datenaufsichtsausschusses innerhalb einer den Datenabgleich vornehmenden Behörde. Eine Kopie der Vereinbarung, die alle beteiligten Behörden vor der Durchführung des Abgleichs treffen müssen, ist dreißig Tage vor Beginn der Maßnahme an einen Ausschuss des Kongresses zu schicken (5 U.S.C. § 552a (o) (2)). Daneben sieht das Gesetz bei allen am *Computer Matching* beteiligten Behörden die Einrichtung eines Datenaufsichtsausschusses vor, der bei allen Abgleichvorgängen die Einhaltung der gesetzlichen Vorgaben überwachen soll. Ein Datenaufsichtsausschuss muss innerhalb jeder Behörde eingerichtet werden, bevor diese an Matching-Vereinbarungen teilnehmen kann (5 U. S. C. 552a (u)). Der Datenaufsichtsausschuss überwacht und koordiniert unter den verschiedenen Abteilungen einer solchen Behörde die Implementierung dieser Vorschrift durch die Behörde. Er ist dazu verpflichtet, jährlich einen Bericht zu erstellen und diesen dem Leiter der Behörde sowie dem *Office of Management and Budget* vorzulegen.

III. Vorratsdatenspeicherung

1. Geschichtlicher Hintergrund

Das Freiheits- und Persönlichkeitsinteresse der Bürger muss gegen die Verantwortung des Staates abgewogen werden, seine Bürger vor ausländi-

schen Bedrohungen zu schützen, Verbrechen zu ermitteln und das geltende Recht durchzusetzen. Dies ist deshalb nicht einfach, weil im digitalen Zeitalter neue Herausforderungen entstehen, denen mit konventionellen Mitteln schwer oder gar nicht begegnet werden kann. Eines der neuen Ermittlungsmittel ist die Vorratsdatenspeicherung. Hierbei handelt es sich um ein kriminalpolitisches Instrument, das die Kommunikationsdienstanbieter dazu verpflichtet, bestimmte Daten zum Zweck einer eventuellen Ermittlung, Feststellung und Verfolgung bestimmter Straftaten vorrätig und anlasslos zur Verfügung zu stellen. In den USA existiert aber keine Bestimmung, die die Telekommunikationsunternehmen zur vorrätigen und anlasslosen Speicherung bestimmter Daten verpflichtet, obwohl mehr als zwanzig Jahre lang eine ähnliche Praxis herrschte, ohne dass die Bevölkerung davon wusste. Diesbezüglich wurde in den USA im Jahr 2013 durch Snowdens Enthüllungen ein Skandal verursacht. Der Skandal führte dazu, dass die Bevölkerung über die Datenspeicherungspraxis des Staates informiert wurde. An diesem erstaunlichen Ereignis sind die mehrfachen Versuche des Parlaments, die Vorratsdatenspeicherung einzuführen, gescheitert. Der Gesetzgebungsfehlschlag gründet sich nicht nur auf der geschichtlichen Erfahrung der Bevölkerung in Verbindung mit einer Reihe von Ereignissen bezüglich der Metadatensammlung des Staates, sondern auch unmittelbar auf das fehlende Datenschutzgesetz: Es gibt in den USA so gut wie keine Datenschutzgesetze im Privatsektor. Die privaten Unternehmen können deshalb nach Belieben und ohne weitere Einschränkungen Daten speichern. In dieser Situation sorgt sich der Staat bei einer Anforderung der Daten wenig darum, dass die Daten zum Anfragezeitpunkt im Unternehmen verlorengehen und deshalb nicht mehr gespeichert sind.

In diesem Zusammenhang wurden die sog. Quick-Freeze-Verfahren unter dem ECPA (Electronic Communications Privacy Act von 1986)[526] ohne eine Vorratsdatenspeicherung implementiert. Hierbei ist eine anlassbezogene Speicherung der bei den Telekommunikationsunternehmen vorhandenen Daten vorgesehen („einfrieren"). Bei Verdachtsfällen kommt es auf Anordnung der Strafverfolgungsbehörden zu einer „vorübergehenden Sicherung" der Daten. Unter bestimmten Voraussetzungen können diese eingefrorenen Daten den Ermittlungsbehörden zur Verfügung gestellt werden („auftauen"). Der Zugriff auf die Daten ist damit möglich. Im Folgenden soll zuerst der historische Hintergrund näher erläutert werden, der dazu geführt hat, dass die US-amerikanische Datenspeicherungspraxis

526 ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U. S. C § 2510.

sich auf das Quick-Freeze-Verfahren beschränkt; danach soll die aktuelle Datenspeicherung unter dem Quick-Freeze-Verfahren untersucht werden.

a) Die Datensammlung der DEA als eine Vorlage für die Metadatensammlung der NSA

Die Antidrogenbehörde DEA (*Drug Enforcement Administration*) hat zwanzig Jahre lang Milliarden von Telefonverbindungsdaten mit noch weniger demokratischer Kontrolle gespeichert. Die DEA betrieb eine riesige Datenbank mit Telefonverbindungsdaten namens USTO.[527] Anstatt die Telefongesellschaften um Anrufdaten von Personen zu ersuchen, die wegen Drogenverbrechen verdächtig wurden, hatte das Justizministerium Telefonanbietern die Anordnung erteilt, Listen aller Anrufe aus den USA in Länder zu übertragen, in denen nach Ansicht der Regierung Drogenhändler operieren. Die Behörde leitete Informationen von Geheimdienstabhörungen, Informanten und der Datenbank mit Telefonverbindungsdaten an Behörden im ganzen Land weiter, um ihnen dabei zu helfen, strafrechtliche Ermittlungen gegen Amerikaner einzuleiten.[528] Die DEA erhielt die Daten mit administrativen *subpoenas*, die es der Behörde erlaubten, Daten zu sammeln, die für Bundesdrogenuntersuchungen relevant oder wesentlich sind. Es handelte sich zwar um eine weite Auslegung dieser Befugnis, die jedoch wahrscheinlich nicht angefochten wird, da die *subpoenas* im Gegensatz zu Durchsuchungsbefehlen keiner gerichtlichen Anordnung bedürfen.

Um das Programm geheim zu halten, wurden die Verbindungsdaten nie als Beweismittel in Prozessen oder als Grundlage für Durchsuchungsbefehle verwendet. Die Anfangsdaten, die aus den oben erwähnten Quellen stammen, wurden effektiv an einem zentralen Ort der SOD (*Special Operation Division*) bereinigt, bevor sie an Mitarbeiter von Behörden einschließlich der DEA, des *Internal Revenue Service*, des FBI und der *Homeland*

527 In der DEA-Datenbank namens USTO wurden unabhängig davon, ob gegen die Beteiligten ein Verdacht vorlag, Verbindungsdaten zu Gesprächen ins Ausland gespeichert: Die Telefonnummern sämtlicher US-Bürger, die irgendwann einmal in eines von 116 Ländern telefonierten, werden mitsamt der Nummer des Angerufenen, der Uhrzeit und der Gesprächsdauer gespeichert.

528 *Shiffman/Cooke*, Exclusive: U. S. directs agents to cover up program used to investigate Americans, REUTERS v. 5.8.2013, abrufbar unter: https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R.

Security gesendet wurden. Eine Ermittlungsbehörde erhielt von der SOD einen Geheimtipp, nach dem die Anfangsdaten aus der ursprünglichen Quelle nicht als Beweismittel verwendet wurden, führte dann eine separate Untersuchung durch und konstruiert daraus die unabhängigen, im Prozess anzuerkennenden Beweise. Die Methode wird als *parallel construction* bezeichnet. Die *parallel construction* wurde wegen Verstoßes gegen die verfassungsmäßigen Rechte der jeweils Angeklagten auf ein faires Verfahren und wegen der vorgerichtlichen Entdeckungsregelung kritisiert, damit Beweise unterschlagen werden, die sich für die jeweils Angeklagten als nützlich erweisen könnten.[529]

Das USTO-Programm wurde erst nach den Snowden-Enthüllungen im Mai 2013 eingestellt. Seitdem übergab die DEA den Mobilfunkbetreibern jeden Tag eine Liste mit Telefonnummern, deren Anschlussinhaber sie verdächtigte, und verlangte die entsprechenden Verbindungsdaten. Die inzwischen eingestellte Operation, die von der DEA durchgeführt wurde, war die erste bekannte Bemühung der Regierung, Verbindungsdaten von Millionen US-Bürgern in Massen zu sammeln, unabhängig davon, ob sie einer Straftat verdächtigt wurden oder nicht. Es war ein Modell für das massive Telefonüberwachungssystem, das die NSA nach den Anschlägen vom 11. September 2001 einsetzte, um Terroristen zu identifizieren.

b) Metadatensammlung[530] der NSA

aa) Die Anschläge vom 11. September 2001 als Wendepunkt

Ein Großteil dessen, was über das Massenmetadatensammlungsprogramm der NSA bekannt ist, stammt aus Dokumenten, die durch die Snowden-Offenlegung veröffentlicht wurden. Die Praxis der Metadatensammlung der NSA vor den Anschlägen am 11. September 2001 ist daher kaum bekannt.

---

529 *Shiffman/Cooke*, Exclusive: U. S. directs agents to cover up program used to investigate Americans, REUTERS v. 5.8.2013, abrufbar unter: https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R.

530 Metadaten enthalten Informationen zu einem Anruf – wer, wo, wann und wie lang –, aber nicht den Inhalt der Kommunikation.

Die NSA ist gemäß der *executive order* 12333[531] dazu ermächtigt, die Daten ausländischer elektronischer Nachrichtendienste zu sammeln und zu analysieren und die Sicherheit von geheimen US-Computersystemen zu gewährleisten.[532] Die Befugnisse der NSA wurden aber während eines verdeckten Programms von 1956 bis 1971 missbraucht, als die Behörde die Geheimdienstdaten sammelte und verschiedene US-Bürger überwachte.[533] Als Reaktion auf den Missbrauch wurde der Foreign Intelligence Surveillance Act (FISA) erlassen, dessen Ziel die Begrenzung der Massenüberwachung in den USA ist. Gemeinsam mit dem FISA wurde auch der *Foreign Intelligence Surveillance Court* (FISC oder FISA-Court) eingerichtet, dessen Aufgabe es ist, die FISA-Anordnungsanträge zu überprüfen.[534] Die FISA-Anordnungsanträge müssen hinreichend wahrscheinlich (*probable cause*) sein, damit zu der Annahme gelangt werden kann, dass „das Ziel der elektronischen Überwachung eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist"[535] und dass sich die gesuchten Informationen auf die nationale Sicherheit beziehen. Bei einer FISA-Anordnung ist, anders als bei der Title-III[536], kein *probable cause* für die Annahme erforderlich, dass die Zielperson ein Verbrechen begangen hat oder begehen wird.

---

531 Executive Order No. 12,333, 3 C. F. R. 1981, available at http://www.archives.gov/federal-register/codification/executive-order/12333.html. Department of Defense Personnel Security Program Regulation, 3 C. F. R. 1981, 32 C. F. R. § 154 (2012). "The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General." a. a. O. Siehe 1.8. "Agencies with the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General." a. a. O., siehe 2.3.

532 *Ahuja*, FAQ: What you need to know about NSA surveillance and Edward Snowden, WASHINGTON POST v. 5.8.2013, abrufbar unter: https://www.propublica.org/article/nsa-data-collection-faq.

533 NAT'L COMM'N TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT 75 (July 22, 2004) [hereinafter 9/11 COMMISSION REPORT], available at http://www.9-llcommission.gov/report/9llReport.pdf; *Baker*, In the Common Defense, 2014.

534 *Baker*, In the Common Defense, 2014, S. 79–80.

535 50 U. S. C. § 1804 (a) (4) (A) (2014).

536 Title-III ist eine Abhörmaßnahme des Bundes und ein Verweis auf den Teil des Omnibus Crime Control and Safe Streets Act von 1968 Pub. L. No. 90–351, 82 Stat. 197 (codified as amended in scattered sections of 42 U. S. C.), der die Strafverfolgungsbehörden dazu ermächtigte, die Erlaubnis zum Abhören von kabelgebundenen und mündlichen Kommunikationen ohne das Wissen oder die Zustimmung der Teilnehmer zu beantragen. 18 U. S. C. § 2518 (2000 &

Unter den FISA-Anforderungen können Ausländer auch ohne eine gerichtliche Anordnung überwacht werden, soweit es *keine substanzielle Wahrscheinlichkeit* dafür gibt, dass die Überwachung den Inhalt einer Kommunikation offenlegt, an der US-Bürger teilnehmen.[537] Der Großteil der von der NSA durchgeführten Überwachung fällt unter die Kategorie „Ausländer zu Ausländer" und wird daher von der FISA nicht erfasst, da die Überwachung in Übersee und in der Regel gegen Ausländer erfolgt.

Früher gab es bei der Übermittlung der von der NSA gespeicherten Daten eine Mauer zwischen der Strafverfolgungsbehörde und dem Geheimdienst, die verhinderte, dass eine Strafverfolgungsbehörde die FISA-Daten verwendet, um die Notwendigkeit einer rechtmäßigen Titel-III-Anordnung zu negieren und die Anforderung absichtlich zu umgehen, einen *probable cause* für eine Entscheidung darüber zu entwickeln, ob eine Zielperson eine Straftat schon begangen hat oder begehen wird. Hier wurde ein Verfahren über die Übermittlung und die Weitergabe der von der NSA gespeicherten Daten eingerichtet. Die Mauer konnte nur mit der Zustimmung des Generalstaatsanwalts und des FISC überwunden werden. So gab es keinen Grund zur Sorge, dass die Geheimdienstdaten in einem Strafverfahren gegen einen Angeklagten verwendet würden.

Nach den Anschlägen vom 11. September 2001 wurde die Befugnis der NSA, nationale Kommunikationen zu überwachen, zuerst durch das *President's Surveillance Program* (PSP) und später durch gesetzliche Grundlagen – den PATRIOT Act[538] – erweitert. Mit dem PATRIOT Act von 2001 wurden die Exekutivbefugnisse auch in der Telekommunikationsüberwachung

---

Supp. 2014) legt die verfahrensrechtlichen Anforderungen an die Überwachung fest. Das Gesetz regelt im Wesentlichen Folgendes: (1) Es verbietet der Regierung, eine unbefugte und nicht einvernehmliche Überwachung der Kommunikation per Telefon, Internet, E-Mail usw. zu implementieren; (2) es legt das Verfahren fest, wie die Regierung eine gerichtliche Anordnung zur Durchführung einer Abhörmaßnahme anfordern kann; und (3) es regelt die Offenbarung von abgefangenen Kommunikationen. Um eine gerichtliche Anordnung für das Abhören kabelgebundener oder elektronischer Kommunikationen zu erhalten, muss ein föderales Verbrechen begangen werden und die Identität der Zielpersonen, ihr kriminelles Verhalten und die Art und Weise, in der das Zielgerät zur Förderung der Strafverfolgung verwendet wird, müssen angegeben werden. Es wird manchmal gesagt, dass die Titel-III-Anordnungen schwieriger zu erhalten sind als die FISA-Anordnung.

537 50 U. S. C. § 1802 (B).

538 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (der USA PATRIOT Act) Act of 2001, sec. 208 (1), Pub. L. No. 107-56, 115 Stat. 272 [im Folgenden: der PATRIOT Act] (codified in scattered titles of U.S.C.), at sec. 203. Den PATRIOT Act verabschie-

umfangreich erweitert, damit die Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen. Die Erweiterung des Zugriffs der Strafverfolgungsbehörden zu den elektronischen Daten erfolgte mit der Reduktion der Data Privacy der Bürger. Der PATRIOT Act erlaubte zum einen, dass Telekommunikationsunternehmen unter bestimmten Bedingungen die Kommunikations- und Standortdaten an die Strafverfolgungsbehörden freiwillig übergeben, und erweiterte zum anderen die Arten von Daten, die den Strafverfolgungsbehörden mit *subpoenas* verfügbar sind.

Die Gesetze durchbrachen unter dem Abschnitt 203 mit dem Titel *Authority to share criminal investigative information* vor allem die Mauer, die den Datenaustausch zwischen Nachrichtendienst- und Strafverfolgungsbehörden blockiert hatte. Der Abschnitt 215 des PATRIOT Act ermächtigte die Regierung außerdem dazu, eine geheime gerichtliche Anordnung zu beantragen, mit der Dritte wie Telefongesellschaften dazu aufgefordert werden können, Daten oder andere „tangible things" zu übergeben, wenn sie für eine Untersuchung relevant sind, die der Sammlung ausländischer nachrichtendienstlicher Daten, die nicht US-Bürger betreffen, oder dem Schutz vor internationalem Terrorismus oder Geheimdienstaktivitäten dient. Aber die Regierung glaubte immer noch, dass sie aufgrund der Third-Party-Doktrin[539] nicht einmal gerichtliche Anordnungen benötigt, wenn sie beschließt, diese Daten mit *subpoenas* zu sammeln. Auf dieser Grundlage hat die NSA von Telekommunikationsanbietern Listen mit allen von ihren Kunden geführten und erhaltenen Anrufen angefordert und erhalten, einschließlich der üblicherweise aufgezeichneten Metadaten wie Uhrzeit, Dauer des Anrufs und Telefonnummern am Endgerät (aber nicht

---

dete der Kongress am 25. Oktober 2001 als Reaktion auf die Anschläge vom 11. September 2001.

539 Die *Fourth Amendment* verbietet nicht den Erhalt von Daten, die Dritten gegenüber offengelegt und von diesen an Regierungsbehörden übermittelt wurden, auch wenn die Informationen in der Annahme offenbart werden, dass sie nur für einen begrenzten Zweck verwendet werden und das Vertrauen in Dritte nicht verraten wird (United States v. Miller, 425 U. S. 435 (1976), S. 443). Im Anschluss an Miller entschied der Gerichtshof in der Entscheidung Smith v. Maryland, dass ein Anrufer keine begründete Erwartung auf *privacy* hat, wenn er seine Daten freiwillig an Telefongesellschaften weitergibt. Das beruht auf der Erwägung, dass der Anrufer bei der freiwilligen Weitergabe seiner Daten an Dritte das Risiko eingeht, dass die Telefongesellschaft seine Daten der Polizei offenbart. Aus diesem Grund verlangt der vierte Zusatzartikel nicht, dass die Regierung eine gerichtliche Anordnung einholt, bevor sie Anrufmetadaten erhält (Smith v. Maryland, 442 U. S. 735 (747)).

des Inhaltes).[540] So stellte sich heraus, dass eine Kopie jeder elektronischen Kommunikation, die über die Glasfaserkabel übermittelt wurde, die über die *Folsom St.* in das AT&Ts Intranet gelangten, durch die im geheimen Raum installierte Ausrüstung zur NSA geschickt wurde.[541] Um diese Daten zu sammeln, musste die Regierung eine Anordnung des Abschnitts 215 vom FISC erhalten. Sie konnte vor dem FISC beantragen, diese Daten von anderen Unternehmen zu erfragen, solange die Daten für eine terroristische Untersuchung relevant waren. Die nach dem Abschnitt 215 erlangten Daten, die sich auf US-Bürger bezogen, konnten nur an das FBI oder andere Nachrichtendienste weitergegeben werden, und die Hinweise aus den Metadaten beschränkten sich auf Antiterrorismusuntersuchungen.[542] Mit dem Abschnitt 215 war auch die parlamentarische Kontrolle für das FISA-Programm eingerichtet, indem das DOJ (U.S. Department of Justice) dazu aufgefordert wurde, eine Prüfung des Programms und der Wirksamkeit des Abschnitts 215 durchzuführen.

Unter den eigenen Befugnissen (*inherent powers*) des Präsidenten und der Verwaltung verfügte die NSA über die Ermächtigung, US-Amerikaner innerhalb des Landes ohne eine gerichtliche Anordnung zu überwachen, solange sich eine Partei außerhalb der USA befand und der Analytiker vermutete, eine Partei sei ein Terrorist oder ein Mitarbeiter oder Mitglied einer mit dem Terrorismus verbundenen Organisation, insbesondere Al-Qaida.[543] Durch die Enthüllungen des ehemaligen NSA-Mitarbeiters *Snowden* wurde offengelegt, dass die US-amerikanischen Nachrichtendienste im Laufe von sieben Jahren täglich Massentelefonmetadaten für jeden Anruf gesammelt hatten, die Kunden multinationaler Telekommunikationsunternehmen tätigten.[544] Vor Snowdens Enthüllungen entschied der FISC, dass die Massentelefoniemetadatensammlung gemäß dem Abschnitt 215 gerechtfertigt sei. Wegen dieses Umstands hatte das Parlament die neuen

---

540 *Kadidal*, NSA Surveillance: The Implications For Civil Liberties, S. 444.

541 Hepting v. AT&T, No. 06-17131 (9th Cir. 2007).

542 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 437 f.

543 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 440 f.

544 *Greenwald*, NO PLACE TO HIDE: Edward Snowden, the NSA, and the U. S. Surveillance State, 2015.

Rechtsgrundlagen[545] geschaffen, auf denen die NSA auch ohne eine gerichtliche Anordnung zur Überwachung ermächtigt wurde. Abschnitt 702 ermächtigte die Regierung dazu, die Kommunikation außerhalb des traditionellen FISA- oder Titel-III-Anordnungsprozesses zu überwachen, und legte das Verfahren fest, an dem die Überwachung auf die Kommunikation anderer Personen als der US-Bürger, die sich außerhalb der USA befinden, ausgerichtet wird.[546] Im Rahmen des Abschnitts 702 wurden *minimization procedures*[547] geschaffen, damit die *privacy* der versehentlich überwachten US-Bürger geschützt werden kann.

Durch den Foreign Intelligence Surveillance Act von 1978 und den FISA Amendments Act von 2008 wurde ein Verfahren implementiert, das die Massenüberwachung in gewissem Maß begrenzt: gerichtliche Kontrolle, parlamentarische Kontrolle und *minimization procedures*. Die Metadatensammlung der NSA stieß aus verschiedenen Gründen auf Kritik. Zu diesen Gründen gehörte, dass sich das FISC bei seiner Entscheidung auf die von der Regierung vorgelegten Informationen stützte, dass die Mauer zwischen Nachrichtendienst- und Strafverfolgungsbehörden nach den Anschlägen am 11. September 2001 zusammenbrach, dass die Befugnisse der NSA durch den Abschnitt 702 erweitert wurden und dass die Third-Party-Doktrin, deren Zulänglichkeit in der modernen digitalen Gesellschaft zweifelhaft ist, aufrechterhalten wurde.[548] Aber in der *States v. Jones*-Entscheidung stellte das Gericht fest, dass der Massendatensammlung

---

545 Der Protect America Act aus dem Jahr 2007, Pub. L. No, 110–55, 121 Stat. 552 (codified at 50 U. S. C. §§ 1805a to 1805c (2003 & Supp. 2014) als ein Übergangsgesetz und als Rechtsnachfolger des FISA Amendments Act of 2008, H. R. 6304, 110th Cong. (2007–2008) – ist ansonsten als Abschnitt 702 oder FAA bekannt.

546 50 U. S. C. § 1881 (a) (2003 & Supp. 2014).

547 Sie legen die Voraussetzungen fest, unter denen der Inhalt und die Identität der US-Bürger, die versehentlich überwacht wurden, gelöscht werden müssen. Dazu ausführlich *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 442 f.

548 Der Kern dieser Doktrin, deren Ursprung in dem Fall Smith v. Maryland zu finden ist, besteht darin, „dass einer Person eine subjektive Erwartung der Privatsphäre in Bezug auf Daten fehlt, die mit einem Dritten geteilt werden." Die Doktrin beseitigt die Möglichkeit eines Verstoßes gegen den vierten Verfassungszusatz, weil keine begründete Erwartung der *privacy* in den Metadaten bestand, da die Kunden ihre Daten mit einem Drittanbieter austauschten. Diesbezüglich erhöhte sich die Forderung nach einer nochmaligen Überlegung der Third-Party-Doktrin (siehe *Barnett*, Why the NSA Data Seizures are unconstitutional, Harvard Journal of Law & Public Policy, Vol. 38 No. 1, 2014, S. 10 ff.).

besondere Bedeutung zukommen kann, obwohl die gesammelten Daten freiwillig an Dritte weitergegeben wurden.[549] Das Gericht entschied, dass eine begründete Erwartung in puncto *privacy* in bestimmten Datenmengen anerkannt wird, selbst wenn solche Erwartungen in ihren Bestandteilen nicht angenommen werden können.[550]

bb) Der Freedom Act nach den Snowden-Enthüllungen

Die Metadatensammlung der NSA hat durch die Verabschiedung des Freedom Act eine neue Phase erreicht. Nach Snowdens Enthüllungen wurden die Recht- und Verfassungsmäßigkeit des Metadatensammlungsprogramms der NSA für Massentelefonie in zwei bedeutsamen Fällen[551] bestritten, die in Erwägungen über eine einstweilige Anordnung zu völlig unterschiedlichen Ergebnissen führten. Das Parlament hat daher im Jahr 2015 ein neues Gesetz[552] erlassen, um dabei zu helfen, Rechtsstreitigkeiten beizulegen und das Metadatensammlungsprogramm der NSA für Massentelefonie unter strengere Voraussetzungen zu stellen. Das Gesetz zielt vor allem auf die Beendigung der Massenverbindungsdatensammlung durch die NSA.

Das Gesetz brachte zwei bedeutende Änderungen mit sich: Die erste Änderung betrifft die Einführung eines neuen, eng eingeschränkten Mechanismus für die gezielte Sammlung von Telefonmetadaten für mögliche Verbindungen zwischen ausländischen Mächten oder Vertretern ausländischer Mächte und anderen Personen vor, die im Rahmen einer be-

549 United States v. Jones, 132 S. Ct. 945 (2012).

550 *Gray/Citron*, A Shattered Looking Glas: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, North Carolina Journal of Law and Technology, Vol. 14, No. 2, 2013, 381, 381-382.

551 ACLU v. Clapper, 959 F. Supp. 2d 724 (S. D. N. Y. 2013) (Die Beschwerde wurde teilweise mit der Begründung abgelehnt, dass die Kunden im Rahmen des Präzedenzfalles des vierten Verfassungszusatzes keine berechtigten Erwartungen auf *privacy* in telefonischen Metadaten haben, die ein Dritter besitzt) und 785 F. 3d. 787 (2nd Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D. D. C. 2013) (Es wurde festgestellt, dass das Gericht zwar für die Überprüfung des Antrags auf den Administrative Procedure Act (APA) nicht zuständig war, aber konstitutionelle Herausforderungen für das Verhalten der NSA behandeln konnte. Hier wurde einem Antrag auf einstweilige Anordnung stattgegeben.)

552 USA FREEDOM Act (the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), H. R. 3361, 113th Cong. (2013–2014).

fugten Ermittlung zum Schutz vor internationalem Terrorismus verfolgt werden. Es wird hier vorausgesetzt, dass die Regierung eine FISC-Anordnung für Metadatensätze einholen muss, die direkt von Unternehmen aufbewahrt werden, erst nachdem eine bestimmte Person, ein Konto, eine Adresse oder ein anderer spezifischer Identifikator als Gegenstand einer spezifischen Untersuchung bestimmt wurde.[553] Wird die gerichtliche Anordnung erteilt, muss der Telekommunikationsanbieter oder ein anderer Unternehmensanbieter die Metadatensätze gemäß einer spezifischen Untersuchung erstellen.[554] Die Verbindungsdaten wurden also vorher von der NSA massenhaft gespeichert. Aber diese werden gemäß diesem Gesetz von den Telekommunikationsanbietern gespeichert und nur noch auf Anfrage bereitgestellt. Die zweite Änderung bezieht sich auf die Forderung nach mehr Transparenz und öffentlicher Berichterstattung über die nationalen Sicherheitsprogramme. In diesem Zusammenhang wurden einige Verfahren eingerichtet: zusätzliche Benachrichtigung an das Parlament, jährliche öffentliche Transparenzberichte sowie Benachrichtigungsmöglichkeit im Privatsektor, die vor Einführung des USA Freedom Act (USAF) wegen der geheimen Natur der FISA-Anordnung ausgeschlossen wurde. Aber das USAF gibt Unternehmen die Möglichkeit, ihre Kunden sowohl in den USA als auch im Ausland über das Volumen und die Arten der nationalen Sicherheitsanfragen zu informieren, die sie erhalten. Das USAF verlangt also von den Geheimdiensten mehr Transparenz bezüglich der von ihnen gesammelten Daten. Die Telekommunikationsanbieter unterliegen nicht mehr der Anordnung, die sie daran hindert, ihre Kunden darüber zu informieren, dass ihre privaten Daten an die Regierung übermittelt werden. Durch die Einführung des USAF wurden die folgenden Maßnahmen mög-

553 USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101 (a) (3), 129 Stat. 268, 26970 (codified at 50 U.S.C. § 1861 (b) (2) (C) (2016)) ("[An] application for the production on a daily basis of call detail records […] conducted to protect against international terrorism. "a statement of facts showing that […] (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required […] are relevant to such investigation; and (ii) there are facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power.").

554 USA FREEDOM Act of 2015, § 101 (b), 129 Stat. at 270; *Steinhauer/Weisman*, U. S. Surveillance in Place Since 9/11 is Sharply Limited, The New York Times v. 2.6.2015, abrufbar unter: https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html: "The storage of those records now shifts to the phone companies, and the government must petition a special federal court [FISC] for permission to search them."

lich, die zu mehr Transparenz führen: Freigabe von FISC-Stellungnahmen mit wesentlichen rechtlichen Auslegungen, ein institutionalisierter Prozess für die Teilnahme von *Amicus Curiae* und der Ersatz des weitgehend einseitigen FISC-Prozesses – also einer fehlenden Berufungsmöglichkeit – durch das Berufungsgericht, das *Foreign Intelligence Surveillance Court of Review* (FISCR).

Der Freedom Act ist mit Blick auf die individuelle Freiheit und die Privatsphäre gegenüber dem PATRIOT Act zwar als eine Verbesserung anzusehen, reicht jedoch noch nicht weit genug. Denn das Gesetz schränkt nur die Massenmetadatensammlung der NSA bezüglich des Abschnitts 215 PATRIOT Act, aber nicht die Massenmetadatensammlung selbst ein. Damit ist nicht die Beauftragung der anderen Behörden mit der Massenmetadatensammlung verboten. Außerdem ist die Regulierung der Massenmetadatensammlung bezüglich E-Mails, Internetsuche und Web-Browser-Verläufen ausgeschlossen.[555] Die Datenspeicherung in einer Datenbank durch die Regierung mit einzelnen *subpoenas* wird ebenfalls noch vertreten. Durch die Verpflichtung zur Datenspeicherung beim Telekommunikationsunternehmen würden diesem Kosten auferlegt, Innovationen behindert und der Zugang zu ICT eingeschränkt.[556] Es wird die Meinung vertreten, dass Drittanbieter diese Daten höchstwahrscheinlich nicht über einen längeren Zeitraum aufbewahren werden, und auch wenn sie dazu aufgefordert werden, würden sie eine beträchtliche Gebühr von der Regierung verlangen oder die Kosten an die Verbraucher weitergeben. Die Daten würden dann in die Hände einer dritten Partei gelangen, wobei die Kontrolle der Datenbank durch staatliche Einrichtungen wie dem Kongress nur in einem geringen oder unwesentlichen Maße möglich wäre.[557] Angesichts des Gefährdungspotenzials der Privatsphäre des Einzelnen durch die Regierung und der außergewöhnlicher Aussagekraft der Metadaten ist diese Ansicht nicht vertretbar.

555 *Hu*, Bulk Biometric Metadata Collection, North Carolina Law Review, Vol. 96, 2018, S. 1469.

556 *Center for Democracy and Technology*, Introduction to Data Retention Mandates, 2012, S. 5.

557 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 454.

2. Aktuelle Rechtslage

Um das Freiheits- und Persönlichkeitsinteresse des Einzelnen zu schützen, garantiert der vierte Verfassungszusatz das Recht, frei von einer unbegründeten Durchsuchung und Beschlagnahme zu sein. Eine begründete Durchsuchung und Beschlagnahme setzt eine gerichtliche Anordnung voraus, die auf der Wahrscheinlichkeit einer Straftat basiert (*warrant on probable cause*). Diese Anordnung ist nach der Katz-Entscheidung beim Vorliegen der begründeten Erwartung auf *privacy* notwendig. Die Telekommunikationsdaten werden auch im Kontext des vierten Verfassungszusatzes geschützt. Danach dürfen sie nur mit einem gerichtlichen Befehl durchsucht und in Beschlag genommen werden. Dies beruht auf der Entscheidung *Katz v. United States* von 1967, nach der der vierte Verfassungszusatz nicht nur die Beschlagnahme von materiellen Gegenständen regelt, sondern sich auch auf die Aufzeichnung mündlicher Aussagen erstreckt.[558] Nachdem sich herausgestellt hatte, dass die Telekommunikationsdaten der Bürger ohne diese fundamentale Voraussetzung einer gerichtlichen Anordnung durch die Nachrichtendienste erhoben und gespeichert wurden, standen die USA unter Schock. Die Snowden-Enthüllungen führten zu Einschränkungen in diesem Bereich.

Den Betroffenen ist die Überwachung in der Regel nicht bewusst. Die Aussagekraft dieser Daten ist weitreichend, weil sich bei umfassender und automatisierter Auswertung aus diesen Daten inhaltliche Rückschlüsse ziehen lassen, die bis in die Intimsphäre hineinreichen. Bei der weiteren Nutzung der Telekommunikationsdaten und bei zunehmender Dichte könnten eine Speicherung und eine Nutzung der Telekommunikationen die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jedes Bürgers ermöglichen. Die Telekommunikationsüberwachung greift in dieser Hinsicht intensiver in Grundrechte ein als normale Durchsuchungen. Dies gilt nicht nur im Bereich des Nachrichtendienstes, sondern auch im Bereich der Strafverfolgung. In Anbetracht dieser Gefahr der Telekommunikationsüberwachung hat das US-Parlament zum Ziel des Privatsphärenschutzes der Bürger im Jahr 1968 den Federal Wiretap Act von 1968 (*Title III of Omnibus Crime Control and Safe Streets Act*)[559] erlassen, dem gemäß die absichtliche Überwachung kabelgebundener Kommunikationen verboten ist, außer wenn eine gesetzliche Ausnahme angewandt wird. Da der Act nur die kabelgebundene Kommunikation zum Gegen-

558 Katz v. United States, 389 U. S. 347 (347).
559 Pub. L. 90-351, June 19, 1968, 82 Stat. 42 U. S. C. § 3711.

stand hatte, bedurfte es einer Gesetzesanwendung auch auf die drahtlosen Kommunikation. Der Electronic Communications Privacy Act (ECPA) von 1986[560] hat damit den Title III (den Federal Wiretap Act) geändert und zwei weitere Gesetze als Reaktion auf Entwicklungen in der Computertechnologie und in den Kommunikationsnetzwerken eingeführt: 1. den Wiretap Act (18 U. S. C. §§ 2510–2522); 2. den Stored Communications Act (SCA) (18 U. S. C. §§ 2701–2711); und 3. den Pen Register Act (18 U. S. C. §§ 3121–3127). Danach wurde der USA PATRIOT Act[561] verabschiedet, mit dem geringfügige Änderungen am bestehenden Datenerhaltungsmodell vorgenommen wurden. Mit dem PATRIOT Act wurden Teile des ECPA geändert, wodurch der Zugang der Strafverfolgungsbehörden zu elektronischen Daten verbessert und der Datenschutz der Verbraucher verringert wurde. Der PATRIOT Act erlaubt es Internet Service Providern, Verkehrs- und Standortdaten unter bestimmten Umständen freiwillig an die Strafverfolgungsbehörden weiterzugeben. Das Gesetz erweitert auch die Daten, die die Strafverfolgungsbehörden von einem Diensteanbieter nur mit einer *subpoena* anfordern können – und zwar ohne Benachrichtigung des Betroffenen.[562]

Es wurde bereits erwähnt, dass das US-Gesetzbuch keine Bestimmung zur Vorratsdatenspeicherung enthält, das der in Deutschland gültigen entspricht und die die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber dazu verpflichtet, bestimmte Daten in einem bestimmten Zeitraum auf Vorrat zu speichern.[563] Aufgrund der Erfahrungen der Bürger mit der Datenspeicherungspraxis der Regierung wurde die Einführung der Vorratsdatenspeicherung in den USA trotz mehrerer Gesetzgebungsversuche verhindert. Denn die Regierung hat das Vertrauen der Bürger in ihre Führungspraxis von Telekommunikationsdaten verloren. Während die EU-Staaten auf die Terroranschläge

560 Pub. L. 99-508, October 21, 1986, 100 Stat. 1848. Der Electronic Communications Privacy Act und der Stored Wire Electronic Communications Act werden allgemein als der ECPA von 1986 bezeichnet.

561 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

562 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009; *Young*, Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation, International Journal of Communications Law & Policy, No. 9, 2004.

563 *Crump*, Data Retention: Privacy, Anonymity, and Accountability Online, Stanford Law Review, Vol. 56, 2003, 191.

mit der Vorratsdatenspeicherung reagiert haben, wird in den USA das sog. *Quick-Freeze-Verfahren* oder *Data-Freeze-Verfahren* (das anlassbezogene *Data-Preservation-Modell*) praktiziert,[564] das auch in Europa zuweilen als Alternative zur Vorratsdatenspeicherung vorgeschlagen[565] oder als ein zusätzliches Ermittlungsmittel praktiziert wird. Darunter versteht man ein Verfahren, in dem die Daten einer verdächtigen Person ab dem Zeitpunkt einer polizeilichen Anordnung gegen ein Telekommunikationsunternehmen (oder einen Internet Service Provider) gespeichert und damit „eingefroren" werden.[566] Nach dem US-Internet-Service-Provider-Verein sei das Data-Preservation-Modell „der bevorzugte Mechanismus, um die Gefahr des Löschens von Datensätzen und Kommunikationen zu minimieren, die während einer Ermittlung eines Verbrechens notwendig sein können"[567]. Bei diesem Verfahren geht es um eine allgemeine Kommunikationsdatenanfrage, mit der auf die zu und ab dem Zeitpunkt einer Anordnung noch vorhandenen und entstehenden Telekommunikationsverbindungen zugegriffen wird. Insoweit erfasst ein solches Verfahren allerdings gerade solche Daten nicht, auf die die Vorratsspeicherung abzielt, nämlich diejenigen, die zu Betriebszwecken eines Unternehmens nicht gespeichert werden, und diejenigen, die vor der in der Vorratsdatenspeicherungsregelung vorgesehenen Frist von Telekommunikationsunternehmen gelöscht werden.[568] Außerdem werden Bestands- und Verkehrsdaten in den USA

564 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009.

565 *Der Deutsche Bundestag*, Plenarprotokoll 16/19, Stenographischer Bericht, 19. Sitzung in der 16. Wahlperiode, Berlin, 16. Feburar2006, S. 1419, abrufbar unter: http://dip.bundestag.de/btp/16/16019.pdf; *Dix*, Freiheit braucht Sicherheit – Sicherheit braucht Freiheit, Benjamin Franklin und die Freiheit zur unbeobachteten Kommunikation, in: *Bundeskriminalamt* (Hrsg.), Informations- und Kommunikationskriminalität, Vorträge anlässlich der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003, Kriminalistik 2004, S. 82.

566 *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministeriums der Justiz, S. 182.

567 *Petersen*, Toward a U. S. Data-Retention Standard for ISPs, EDUCAUSE Review, Vol. 41, No. 6, 2006, 78-79: "The preferred mechanism to minimize the risk of deletion of records and communications that may be necessary during an investigation of a crime."

568 *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei

nicht voneinander unterschieden. Während die Datenspeicherung im Rahmen des Nachrichtendienstes bei den staatlichen Stellen selbst geschieht, werden die Kommunikationsdaten nach dem ECPA von Telekommunikationsanbietern gespeichert.

Im Hinblick auf das Quick-Freeze-Verfahren kommt dem Communications Assistance for Law Enforcement Act von 1994 (CALEA)[569] eine wichtige Bedeutung zu. Das Quick-Freeze-Verfahren gewinnt tatsächliche Vollzugskraft durch das CALEA, das die Zusammenarbeit von Dienstleistungsanbietern erzwingt. Das Gesetz schreibt vor, dass Telekommunikationsunternehmen ihre Netze so auslegen müssen, dass sie auf das befugte behördliche Überwachungsersuchen antworten können. Alle Telekommunikationsunternehmen müssen demnach dazu in der Lage sein, elektronische Kommunikationen zu isolieren und zu überwachen und die Daten an die Strafverfolgungsbehörden zu übermitteln. Der Zweck des Gesetzes ist es, die Fähigkeit der Strafverfolgungsbehörden zu verbessern, elektronische Überwachung durchzuführen. Dies geschieht durch die Forderung, dass die Telekommunikationsunternehmen ihre Ausrüstung, Einrichtungen und Dienstleistungen so verändern und gestalten müssen, dass sichergestellt ist, dass diese eingebaute Überwachungsmöglichkeiten haben, sodass Bundesbehörden jede Telekommunikation abhören können.[570] Das CALEA ist also das Gesetz, das die im ECPA geregelte Telekommunikationsüberwachung und das Erlangen von Kommunikationsdaten durch staatliche Behörden ermöglicht. Darin wird die Pflicht eines Telekommunikationsanbieters[571] vorgeschrieben, das Abhören durchzusetzen und der Strafverfolgungsbehörde dessen Ergebnisse zu übermitteln, wenn eine Strafverfolgungsbehörde mit einer gerichtlichen Anordnung oder einer anderen gesetzmäßigen Erlaubnis ein Abhören beantragt. Dabei werden die

---

Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministeriums der Justiz, S. 182 f.

569 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U. S. C. §§ 1001 – 1010.

570 47 U. S. C. § 1002 (a) (4) (A).

571 Das CALEA gilt nicht für Informationsdienste, ein bedeutsamer und über viele Jahre angewandter Begriff im Telekommunikationsrecht. Es gilt für Telekommunikationsunternehmen. Informationsdienstanbieter fallen nicht unter das CALEA, was bedeutet, dass sie ihre Netzwerke nicht so gestalten müssen, dass sie für Strafverfolgungsbehörden zugänglich sind (vgl. *Solove/Schwartz*, PRIVACY LAW: FUNDAMENTALS, 2011, S. 42); American Council on Education v. FCC, 451 F.3d 266 (D. C. Cir. 2006): Das Gericht bestätigte die FCC-Klassifizierung des Breitband-Internetzugangs und des Voice-over-Internet-Protokolls (VoIP) als Telekommunikationsanbieter gemäß dem CALEA.

Bestands- und Verbindungsdaten in dem Umfang bereitgestellt, in dem der Diensteanbieter sie vernünftigerweise erwerben kann.[572] Nach § 1002 CALEA stellt ein Telekommunikationsanbieter sicher, dass er die zur Überwachung erforderlichen Geräte, Einrichtungen oder Dienstleistungen bereitstellt und bei berechtigtem Verlangen einer staatlichen Behörde eine Überwachung unternimmt sowie ihr Ergebnis an die Stelle übermittelt. Außerdem ist er dazu verpflichtet, bei berechtigtem Verlangen einer staatlichen Behörde die Kommunikationsdaten zu übermitteln, die ihm vernünftigerweise zur Verfügung stehen.

In diesem Zusammenhang geht es im Wiretap Act (18 U. S. C. §§ 2510–2522) um die Überwachung laufender Kommunikationen, also um die Regelungen über das Abhören stimmlicher, digitaler und elektronischer Telekommunikationen, an das nach der Berger-Entscheidung höhere Anforderungen als an die übliche Anordnung gestellt werden. Im SCA (18 U. S. C. §§ 2701–2712) handelt es sich um die Erhebung gespeicherter Kommunikationsdaten nach bereits beendeter Kommunikation, also um den Zugang zu Daten im elektronischen Speicher oder um Daten von ISPs und im Pen Register Act (18 U. S. C. §§ 3121–3127) um die Zulassungsbedingungen eines Gerätes (*Pen Register Device* und *Trap and Trace Device*), das dazu dient, künftige Kommunikationsdaten fortdauernd auszuspähen.[573] Diese verschiedenen Maßnahmen sind mit unterschiedlichen Voraussetzungen verbunden. Unter ihnen ist jedoch ausschließlich der Erhalt von Bestands- und Verbindungsdaten schon beendeter Kommunikationen mit der deutschen Vorratsdatenspeicherung vergleichbar. Da die vorliegende Arbeit auf die Untersuchung der Datenverwendung zum Ziel der Straftatenermittlung in den USA im Vergleich zur deutschen Vorratsdatenspeicherung abzielt, aber nicht auf die Überwachung laufender Kommunikationen, konzentriert sich diese Arbeit hier vornehmlich auf die Behandlung bereits gespeicherter oder künftig zu speichernder Kommunikationsdaten im Sinne des SCA und des Pen Register Act. Die Erhebung künftiger Kommunikationsdaten mit Hilfe eines Gerätes nach dem Pen Register Act unterscheidet sich zwar von der deutschen Vorratsdatenspeicherung dahingehend, dass die staatliche Behörde zukünftige Kommunikationsdaten ab dem Zeitpunkt des Gerätanschlusses erhält. Der Vergleich dieser Maßnahme mit der Vorratsdatenspeicherung ist jedoch insofern

572 47 U. S. C. § 1002.

573 Für eine anschauliche Darstellung der unter dem ECPA zu erhaltenden Daten siehe unten Tabelle 3.

sinnvoll, als die Kommunikationsdaten für einen bestimmten Zeitraum nach dem Anschluss des Geräts gespeichert werden.

Im Folgenden soll untersucht werden, wie, wann und unter welchen Voraussetzungen welche Daten zum Ziel der Straftatenermittlung unter dem US-amerikanischen Ansatz nach dem ECPA gespeichert und verwendet werden dürfen.

Tabelle 3: Die Klassifikation der unter dem ECPA zu erhaltenden Daten

<table>
<tr><td rowspan="5">ECPA</td><td>Wiretap Act</td><td>Kommunikations-überwachung</td><td></td></tr>
<tr><td rowspan="3">SCA</td><td rowspan="3">Die Erhebung gespeicherter Kommunikationsdaten nach der Beendigung der Kommunikation</td><td>Kommunikations-inhalte im elektronischen Speicher</td></tr>
<tr><td>Kommunikations-inhalte im Remote Computing Service</td></tr>
<tr><td>Bestands- und Verbindungsdaten bezüglich des elektronischen Kommunikations-dienstes oder des Remote Computing Service</td></tr>
<tr><td>Pen Register Act</td><td>Der Erhalt von Bestands- und Verbindungsdaten bezüglich künftiger Kommunikationen</td><td></td></tr>
</table>

a) Zu speichernde Daten

Anstatt die zu speichernden Telekommunikationsdaten konkret und eingeschränkt zu regeln, bleibt die Speicherpraxis von Bestands- und Verkehrsdaten der Entscheidung der Telekommunikationsanbieter überlas-

sen.[574] Denn es existieren in den USA für den Privatsektor so gut wie keine Datenschutzregelungen. Während bei der ehemaligen Speicherpraxis der Daten durch die NSA die staatliche Behörde die Daten, die von den Telekommunikationsanbietern täglich übertragen werden, von sich aus speichert, werden die Daten hier von den Telekommunikationsanbietern auf Antrag der staatlichen Behörde für einen bestimmten Zeitraum gespeichert. Anstatt zu speichernde Telekommunikationsdaten zu regulieren, bestimmt das ECPA Datenarten, die Telekommunikationsanbieter auf Antrag einer staatlichen Stelle an sie übermitteln sollen. 18 U. S. C. § 2703 (c) sieht vor, dass ein Anbieter eines elektronischen Kommunikationsdienstes oder eines *remote computing service* einen Datensatz oder andere Informationen über seine Kunden (außer den Kommunikationsinhalten) auf Antrag einer befugten Behörde offenlegen soll – Namen, Adressen, Listen von Fernsprechanschlüssen, Daten über die Anzahl und die Dauer der Anrufe in einem bestimmten Zeitraum, die Dienstdauer (einschließlich des Anfangsdatums) und die Art der benutzten Dienste und Zahlungsmittel (einschließlich Kreditkarten- oder Bankkontonummer). Hierbei hängen die Daten, die die staatlichen Behörden erhalten, von der Datenspeicherungspraxis des betreffenden Unternehmens ab. Dies liegt daran, dass nur die Daten, die das Unternehmen bereits vor dem Antrag der Behörde aufbewahrt hat, durch die Maßnahme abgerufen werden können. Da die USA jedoch kaum oder gar nicht über Regelungen zum Datenschutz im privaten Sektor verfügen, wird die Vorschrift letztendlich die Arten von Daten einschränken, die die Behörde erhalten darf. Anstatt die Art der Daten festzulegen, die vorab gespeichert werden müssen, ist das Unternehmen nach dem CALEA nur dazu verpflichtet, die Kommunikationsdaten an die berechtigte Stelle zu übermitteln, die ihm vernünftigerweise zur Verfügung stehen, damit der Verlust erforderlicher Daten bei der Datenanfrage verhindert wird.

Darüber hinaus können auch die zukünftigen Verbindungsdaten mit einem *Pen Register Device* oder einem *Trap and Trace Device* erhoben werden. Das *Pen Register Device* registriert oder dekodiert die Wähl-, Routing-, Adressierungs- und Signalisierungsinformationen, die durch ein Instrument oder eine Einrichtung übertragen werden, von der die kabelgebundenen oder elektronischen Kommunikationen übertragen werden (§ 3127 (3) ECPA). Das *Trap and Trace Device* erfasst eingehende elektronische oder andere Impulse, die die Ursprungsnummer oder andere Wähl-, Rou-

574 *Büllingen*, Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, 349, 351 f.

ting-, Adressierungs- und Signalisierungsinformationen identifizieren, die die Quelle einer kabelgebundenen oder elektronischen Kommunikation mit angemessener Wahrscheinlichkeit identifizieren. Ein *Trap and Trace Device* zeigt also, welche Rufnummern ein bestimmtes Telefon gewählt hat, d. h. alle eingehenden Telefonnummern, während ein Pen-Register eher zeigt, welche Rufnummern ein Telefon angerufen hat, also alle Telefonnummern von ausgehenden Anrufen. Die durch diese Geräte gewonnenen Daten gehören zu den Verkehrsdaten, die eine staatliche Behörde zur Strafverfolgung verwenden kann.

b) Zugriff auf Daten

Auf die Daten, die die Telekommunikationsanbieter auf Antrag einer staatlichen Behörde gespeichert haben, darf je nach Datenarten unterschiedlich zugegriffen werden. Das ECPA schließt also den Zugriff entsprechend den Typen von staatlichen Behörden angefragter Daten an unterschiedliche Anforderungen an. Der Unterschied bezüglich der Anforderungen beruht auf dem verschiedenen Schutzniveau der *privacy*. Das ECPA stellt damit für die Überwachung laufender Kommunikationen die höchsten Anforderungen, für den Zugriff auf schon gespeicherte Kommunikationsinhalte die üblichen Anforderungen, für den Zugriff auf vergangene Bestands- und Verkehrsdaten die erleichterten Anforderungen und für den Zugriff auf künftige Bestands- und Verkehrsdaten durch die Installation des *Pen Register* oder der *Trap and Trace Devices* die am meisten erleichterte Anforderung. Die Voraussetzungen unter dem ECPA finden aber dann keine Anwendung, wenn die Betroffenen zustimmen. Um zu erklären, wie auf die Daten zugegriffen werden kann, die mit den durch die deutsche Vorratsdatenspeicherung erhobenen Daten vergleichbar sind, sollen hier ausschließlich die Zugriffsvoraussetzungen der beim ISP schon in Bewahrung stehenden vergangenen Verkehrsdaten erörtert werden.

Um die vergangenen Verkehrsdaten zu erheben, muss eine staatliche Behörde zuerst den Telekommunikationsdienstanbietern die Speicherung dieser Daten gebieten. Der Anbieter ergreift auf Ersuchen dieser Stelle alle erforderlichen Maßnahmen, um die Daten und die anderen in seinem Besitz befindlichen Beweismittel bis zur Erteilung einer gerichtlichen Anordnung oder zu anderen Verfahren aufzubewahren. Die Daten sind neunzig Tage lang aufzubewahren, wobei diese Frist auf erneuten Antrag der staatlichen Stelle um weitere neunzig Tage verlängert werden kann. Die auf diese Weise gespeicherten Daten dürfen durch diese Stelle nur

unter bestimmten Voraussetzungen erhoben werden. Eine staatliche Behörde kann von einem Telekommunikationsdienstanbieter die Übermittlung dieser Daten (außer dem Kommunikationsinhalt) nur dann verlangen, wenn die Behörde von einem zuständigen Gericht einen *warrant* erwirbt, wenn die Behörde eine gerichtliche Anordnung für eine solche Offenlegung erhält, indem sie spezifische und klare Tatsachen darstellt, aus denen ersichtlich ist, dass Grund zu der Annahme besteht, dass die angeforderten Daten für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind, wenn die Behörde die Zustimmung des Betroffenen zu einer solchen Offenlegung erhält, wenn die Behörde einen formellen schriftlichen Antrag einreicht, der von einer Strafverfolgungsuntersuchung in Bezug auf Telemarketing-Betrug betroffen ist oder wenn die Behörde die bestimmten Daten mit einer *subpoena* sucht: den Namen, die Adresse, die Telefonverbindungsdaten oder die Daten über Verbindungszeiten und -dauer, die Dienstdauer (einschließlich Startdatum) und die Art der in Anspruch genommenen Dienste, die Telefon- oder Instrumentennummer oder die Nummer oder die Identität anderer Teilnehmer (einschließlich einer vorübergehend zugewiesenen Netzwerkadresse) und die Zahlungsmittel und -quelle für diese Dienstleistung (einschließlich Kreditkarten- oder Bankkontonummer).

Dementsprechend können vergangene Verkehrsdaten im Fall der Nutzung mobiler Telefondienste unter der erleichterten Voraussetzung gemäß 18 U. S. C. § 2703 (c) erhoben werden. Dabei kann sich aus den Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss während der Verbindung genutzt wurden, die überschlägige geografische Lage des genutzten mobilen Telefons ergeben. Unter Berücksichtigung der Größe der Personen werden deren Standortdaten an öffentlichen Orten grundsätzlich nicht durch die begründete Erwartung auf *privacy* geschützt, solange sie sich nicht absichtlich mit bedecktem Gesicht bewegen. Im Karo-Fall entschied der Supreme Court, dass ein *warrant* erforderlich ist, damit ein GPS-Tracker an eine Person oder an ihre Besitztümer angeschlossen werden kann, da dadurch der Standort im Innenraum bekannt gemacht wird, der mit bloßem Auge nicht sichtbar ist.[575] Aus der gleichen Logik ergibt sich, dass für die Anschließung des GPS-Trackers an

575 United States v. Karo, 468 U. S. 705 (1984). In diesem Zusammenhang entschied der Supreme Court, dass für die Positionierung in Innenräumen durch eine Wärmebildkamera ein *warrant* eingeholt werden muss (Kyllo v. United States, 533 U. S. 27).

ein Auto kein *warrant* erforderlich ist.[576] Diese Entscheidungen wurden ursprünglich so interpretiert, dass nur für die Positionierung in Innenräumen ein *warrant* erforderlich ist. Praktisch wird jedoch anerkannt, dass die Nutzung aller Positionstracker warrant-pflichtig ist, sodass die Bundespolizei zur Installation eines Positionstrackers regelmäßig einen *warrant* beantragt.[577] Hierbei kann die Frage gestellt werden, ob die Standortdaten eines mobilen Telefons durch die Bezeichnungen der Funkzellen mit einem Standorttracker vergleichbar sind, der an eine Person oder an ihre Besitztümer so angeschlossen wird, dass der Standort im Innenraum bekannt gemacht wird, der mit bloßem Auge nicht sichtbar ist. Wenn die Frage bejaht wird, muss die weitere Frage gestellt werden, ob die Erhebung der vergangenen Verkehrsdaten im Fall der Nutzung mobiler Telefondienste unter der erleichterten Voraussetzung gemäß dem ECPA in einem angemessenen Verhältnis zur Eingriffsintensität steht. Diesen Fragen kommt eine Bedeutung zu, weil die Voraussetzungen davon abhängen, wie das Wesen der Standortdaten des mobilen Telefons durch die Bezeichnungen der Funkzellen zu begreifen ist. Wenn die Standortdaten des mobilen Telefons durch die Bezeichnungen der Funkzellen zu den vergangenen oder zukünftigen Verkehrsdaten gehören, wäre es möglich, sie unter den erleichterten Voraussetzungen – gemäß dem SCA oder den am meisten erleichterten Voraussetzungen gemäß dem Pen Register Act – zu erheben, während sie, wenn sie als ein Standorttracker anzusehen sind, unter den normalen Voraussetzungen erhoben werden müssten. Da das ECPA über keine Einschränkung auf die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss *bei Beginn der Verbindung* genutzt wurden, verfügt und sich die Telekommunikationstechnik immer noch entwickelt, kann man nicht gänzlich die Möglichkeit ausschließen, dass die Standortdaten des mobilen Telefons durch die Bezeichnungen der Funkzellen mit einem Standorttracker vergleichbar sind. Einige Gerichte entschieden, dass die Bezeichnungen der Funkzellen während der Verbindung sowie bei Beginn oder Ende der Verbindung unter den Vorausset-

576 U. S. v. Moran, 349 F. Supp.2d 425 (N. D. N. Y. Jan 05, 2005).

577 U. S. v. In re Application for Tracking Devices on a White Ford Truck, 155 F. R. D. 401, 403 (D. Mass. 1994).

zungen des SCA oder des Pen Register Act erhoben werden dürfen.[578] Andere Gerichte kamen jedoch zu einem umgekehrten Ergebnis.[579]

Der Pen Register Act sieht vor, dass die Installation oder die Verwendung des *Pen Register* oder eines *Trap and Trace Device* grundsätzlich einer richterlichen Anordnung auf Antrag der Staatsanwaltschaft bedarf (18 U. S. C. §§ 3122 und 3123).[580] Für diese Anordnung genügt eine Bescheinigung, die besagt, dass die Daten, die möglicherweise durch eine Installation oder Verwendung eines solchen Geräts erhalten werden, für eine laufende strafrechtliche Untersuchung relevant sind (§ 3122 (b) (2)). Bei einem dringenden Fall kann die gerichtliche Anordnung nachträglich – innerhalb von 48 Stunden nach der Installation des Geräts – eingeholt werden.[581] Dabei soll die Maßnahme dann beendet werden, wenn die gesuchten Informationen gewonnen wurden, wenn der Antrag auf eine

578 In re Application of U. S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, S. D. N. Y. 2006, 460 F. Supp. 2d 448.

579 In re U. S. for an Order Authorizing the Release of Prospective Cell Site Information, D. D. C. 2006, 407 F. Supp. 2d 134.

580 In der *Smith v. Maryland*-Entscheidung stellte das Gericht unter Anwendung der third party doctrine fest, dass Strafverfolgungsbehörden keine gerichtliche Anordnung aufgrund eines *probable cause* im Kontext des vierten Verfassungszusatzes benötigen, um ein sogenanntes „Pen-Register" auf einem Telefonkonto zu installieren, das die angerufenen Nummern und die Dauer der Anrufe aufzeichnet und meldet, nicht jedoch den Inhalt der Gespräche (442 U. S. 735, 741 ff.).

581 § 3125 – Emergency pen register and trap and trace device installation
(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—
(1) an emergency situation exists that involves—
(A) *immediate danger of death or serious bodily injury to any person*;
(B) *conspiratorial activities characteristic of organized crime*;
(C) *an immediate threat to a national security interest*; or
(D) *an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year*;
that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and
(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

gerichtliche Anordnung abgewiesen wurde oder wenn seit dem Beginn der Maßnahmen 48 Stunden abgelaufen sind. Zum Einsatz dieser Maßnahme sind also weder eine Anlasstat noch ein Straftatbezug erforderlich. Nur mit Relevanz für eine laufende strafrechtliche Untersuchung – auch mit Wesentlichkeit bei schon gespeicherten Kommunikationsdaten außer Inhalten – dürfen also die schon gespeicherten oder die künftigen Kommunikationsdaten außer Inhalten angefordert und übermittelt werden. Die staatlichen Behörden weisen den jeweiligen Telekommunikationsanbieter an, noch vorhandene und anfallende Daten „einzufrieren" und zu speichern. Auf Ersuchen einer Behörde ergreift der Telekommunikationsanbieter alle erforderlichen Maßnahmen, um die in seinem Besitz befindlichen Daten und sonstige Beweismittel aufzubewahren, bis eine gerichtliche Anordnung erteilt wird oder ein anderes Verfahren vorliegt. Die Behörde kann dann mit einer gesetzmäßigen Befugnis (einer gerichtlichen Anordnung, der Zustimmung oder einer *subpoena*) auf die Daten zugreifen.

Zusammenfassend schließt sich die – sowohl durch das sog. Quick-Freeze-Verfahren als auch durch den Einsatz eines Gerätes geschehene – Erhebung von Kommunikationsdaten außer Inhalten, die mit der deutschen Vorratsdatenspeicherung vergleichbar sind, weder an den Verbrechenskatalog als eine Anlasstat noch an die Zweckbindung an. Da das ECPA die speziellen Zwecke, für die die Daten erhoben werden dürfen, nicht erwähnt, ist die Verwendung der erhobenen Daten und damit auch ihre Weitergabe nicht eingeschränkt. Obwohl kein bestimmter Verdacht auf eine Anlasstat erforderlich ist, darf auf die Daten nur mit einer erleichter-

---

may have installed and use a pen register or trap and trace device if, *within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title*.
(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.
(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.
(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

ten Anordnung zugegriffen werden.[582] Angesichts der Aussagekraft dieser Kommunikationsdaten bleibt die Zugriffsvoraussetzung auf einem erheblich niedrigen Niveau: 1. der Darstellung spezifischer und klarer Tatsachen, aus denen ersichtlich ist, dass ein Grund zu der Annahme besteht, dass der Kommunikationsinhalt oder die angeforderten Telekommunikationsdaten für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind; 2. einer Bescheinigung, die besagt, dass die Daten, die möglicherweise durch eine Installation oder Verwendung eines solchen Geräts erhalten werden, für eine laufende strafrechtliche Untersuchung relevant sind; oder 3. sogar einer exekutiven *subpoena*. Die einzelnen Übermittlungsverfahren der Daten zur Datensicherheit wie etwa Verschlüsselung sind nicht geregelt. Es ist nur geregelt, dass Telekommunikationsunternehmen alle erforderlichen Schritte unternehmen müssen, um Aufzeichnungen und andere Beweise in ihrem Besitz bis zur Erteilung einer gerichtlichen Anordnung oder zu anderen Verfahren zu erhalten, wenn sie von staatlichen Behörden angefragt werden. Nach dem CALEA ist ein Telekommunikationsbetreiber also nur dazu verpflichtet, einer staatlichen Behörde durch technische und organisatorische Maßnahmen zu ermöglichen, eine Kommunikation zu überwachen oder die Kommunikationsdaten zu erheben und zu verwenden. Er ist aber gesetzlich nicht dazu verpflichtet, seine Datenübermittlung an eine staatliche Behörde gegen unbefugte Kenntnisnahme und Verwendung zu schützen. Zur Transparenz der Datenverwendung berichtet der Generalstaatsanwalt dem Kongress jährlich über die Anzahl der Anordnungen des *Pen Register* und des *Trap and Trace Device*, die von Strafverfolgungsbehörden des Justizministeriums beantragt werden. Der Bericht enthält die Daten über die Dauer des durch eine gerichtliche Anordnung ermächtigten Abhörens sowie die Anzahl und Dauer einer etwaigen Verlängerung der Anordnung, die in der Anordnung angegebene Straftat, die Anzahl der betroffenen Untersuchungen, die Anzahl und das Wesen der betroffenen Anlagen und die Identität des Antragstellers oder der Strafverfolgungsbehörde, die die Anordnung stellt, und die Person, die die Anordnung erteilt.[583]

582 Für die unterschiedlichen Voraussetzungen je nach Typen der angefragten Daten siehe Tabelle 4.

583 18 U. S. C. § 3126.

Tabelle 4: Voraussetzungen nach Typen der angefragten Daten

Datenarten		Voraussetzungen	
Überwachung laufender Kommunikationen		Super warrant	*Warrant* (*probable cause*) Subsidiarität (Die Überwachung ist auf andere Weise gescheitert, wahrscheinlich erfolglos oder zu gefährlich.) Minimization process und bestimmte Verbrechen (predict offenses)
Für 180 Tage oder kürzer gespeicherte Kommunikationen		Üblicher Warrant	*Warrant* (*probable cause*)
Länger als 180 Tage gespeicherte Kommunikationen	Ohne Vorankündigung	Üblicher Warrant	*Warrant* (*probable cause*)
	Mit Vorankündigung	Erleichterte Voraussetzungen	*subpoena* oder gerichtliche Anordnung (Proof of specific and articulable facts showing relevance)
Bestands- und Verkehrsdaten vergangener Kommunikationen (ISP-Records)		Erleichterte Voraussetzungen	*Warrant* (*probable cause*); gerichtliche Anordnung; (proof of specific and articulable facts showing relevance);

		Zustimmung des Betroffenen; förmlicher schriftlicher Antrag oder *subpoena*
Bestands- und Verbindungsdaten bezüglich künftiger Kommunikationen	Am meisten erleichterte Voraussetzungen	gerichtliche Anordnung (certification of relevance)

Das Datenanfrageverfahren ist bei den Geheimdiensten im Rahmen der Terrorabwehr ein anderes.[584] Das FBI darf einen Telekommunikationsanbieter um die Bestandsdaten, die Rechnungsdaten oder die elektronischen Handelsdaten seiner Kunden ersuchen, wenn das FBI dem Anbieter schriftlich bestätigt, dass die ersuchten Daten für eine berechtigte Untersuchung zum Schutz gegen internationalen Terrorismus oder illegale Geheimdienstaktivitäten relevant sind und wenn eine solche Untersuchung einer Person aus den Vereinigten Staaten nicht allein auf der Grundlage von Aktivitäten erfolgt, die durch den ersten Verfassungszusatz geschützt sind. Der Telekommunikationsanbieter muss der Anfrage dann auch ohne eine gerichtliche Anordnung nachkommen.[585] Die Anfrage des FBI kann auf Antrag des Ersuchten von einem Gericht überprüft werden. Das Gericht kann das Ersuchen ändern oder aufheben, wenn die Auskunft auf Anfrage unbegründet, unterdrückerisch oder rechtswidrig ist.[586] Die Datenerhebung anlässlich der Terrorabwehr unterliegt weniger Einschränkungen als die zur Strafverfolgung.

584 Da sich sowohl die Datenspeicherungspraxis der amerikanischen Geheimdienste als auch die deutsche Vorratsdatenspeicherung aus dem Anlass der Terrorabwehr entwickelt haben und in Bereichen der Geheimdienste und der Strafverfolgung bewegen, ist zudem die Datenspeicherungspraxis im Rahmen der Geheimdienste erwähnenswert.

585 18 U. S. C. § 2709.

586 18 U. S. C. § 3511 (a).

c) Löschungspflicht

Anstatt der Bestimmung der pflichtgemäßen Löschung der durch den Diensteanbieter gespeicherten Daten – was bei fast keinem Datenschutzgesetz im Privatsektor eine konsequente Folge sein kann – wird die maximale Frist der Datenspeicherung, die die berechtigten Stellen vom Diensteanbieter fordern dürfen, gesetzlich eingeschränkt. Die Kommunikationsdatenanfrage ist im 18. U. S. C. § 2703 (f) geregelt. Danach kann jede staatliche Behörde die Telekommunikationsunternehmen oder die Internet Service Provider anweisen, noch vorhandene und künftig anfallende Kommunikationsdaten für einen Zeitraum von bis zu neunzig Tagen zu speichern. Die Speicherdauer kann nur einmalig um weitere neunzig Tage verlängert werden. Da es fast keine datenschutzrechtlichen Regelungen für die private Datenspeicherungspraxis und auch keine Regelung für die Löschungspflicht gibt, lassen sich die Speicherung und die Löschung der Daten kaum kontrollieren. Die Speicherdauer von neunzig Tagen – gegebenenfalls um weitere neunzig Tage – stellt ausschließlich die Speicherung der angeforderten Daten in diesem Zeitraum sicher, aber nicht ihre Löschung. Die Speicherungspraxis ist nicht an eine gesetzliche Löschungspflicht gebunden, sondern unterliegt der Marktautonomie. In Anbetracht des geltenden Gesetzes bewahren die meisten Internetdienstanbieter in den USA Daten mindestens dreißig bis neunzig Tage lang auf.[587] Die Internetdienstanbieter vernichten häufig die Daten, die für geschäftliche Zwecke wie Netzwerküberwachung, Betrugsprävention oder Abrechnungsstreitigkeiten nicht mehr erforderlich sind.[588] Nach US-amerikanischem Recht sind die Internetdienstanbieter jedoch nicht dazu verpflichtet, diese Daten innerhalb eines bestimmten Zeitraums zu vernichten. Die Löschungsvorschriften zahlreicher Einzelstaaten fordern ausschließlich, dass ein Unternehmen die personenbezogenen Daten dann sicher und effektiv vernichten muss, wenn es die Daten nicht mehr aufbewahren *will*. Darüber hinaus gibt es keine Löschungs- oder Übermittlungsverbotsvorschriften für bereits an die Ermittlungsbehörden übermittelte Daten.

587 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009; *McCullagh*, Gonzales Pressures ISPs on Data Retention, ZDNET News v. 27. Mai 2006, abrufbar unter: https://www.zdnet.com/article/gonzales-pressures-isps-on-data-retention/.

588 *Swartz/Johnson*, U. S. asks Internet Firms to Save Data, NEWSWATCH v. 1. Juni 2006, abrufbar unter: https://newswatch.write2kill.in/news/2006/06/01/us-asks-internet-firms-to-save-data.

Der Privacy Act beschränkt die Übermittlung der Daten nur durch die Bestimmung, dass keine Behörde ihre Daten ohne schriftliche Aufforderung oder Einverständniserklärung der Betroffenen an eine andere Person oder Behörde weitergeben darf.[589] Hier bestehen jedoch keine spezifischen Erklärungen über den Begriff der anderen Behörden und keine Einschränkungen bezüglich der Datenverwendung zu anderen Zwecken innerhalb derselben Behörden. Für die hier genannten anderen Behörden gibt es keinen spezifischen Geltungsbereich und keine Beschränkungen für die Verwendung der Daten zu anderen Zwecken.

Auch für den Einsatz eines Geräts zum Erhalt der künftigen Verkehrsdaten ist die Verwendungsdauer gesetzlich bestimmt. Das *Pen Register Device* oder das *Trap and Trace Device* darf für einen Zeitraum von höchstens sechzig Tagen eingesetzt werden, und seine Einsatzdauer kann nur einmalig um weitere sechzig Tage verlängert werden.[590] Die Verlängerung kann nur mit einer gerichtlichen Anordnung auf Antrag der Staatsanwaltschaft gewährt werden. Für den Verlängerungsantrag genügt – genau wie für den Antrag auf eine erstmalige Anordnung – eine Bescheinigung, die besagt, dass die Daten, die möglicherweise durch eine Installation oder Verwendung eines solchen Geräts erhalten werden, für eine laufende strafrechtliche Untersuchung relevant sind. Nach Ablauf des ermächtigten Zeitraums wird das eingesetzte Gerät deinstalliert.

Ein Problem liegt aber bei den Daten, die entweder mit der Befugnis gemäß § 2703 ff. oder mit dem Einsatz eines Geräts nach § 3121 ff. schon von einem Telekommunikationsunternehmen an die Strafverfolgungsbehörden übermittelt wurden. Die Verarbeitung und die Löschung der schon übermittelten und damit der Kontrolle der Strafverfolgungsbehörden unterliegenden Daten sind gesetzlich nicht geregelt. Das ECPA beinhaltet also keine Regelung darüber, bis wann und wie die von einem Telekommunikationsunternehmen erhaltenen und damit bei einer anfragenden Stelle liegenden Daten nach der Verwendung gelöscht werden sollen.

d) Mitteilungspflicht

Die Benachrichtigungspflicht gilt nur für die Erhebung von Kommunikationsinhalten mit einer *subpoena* oder einer erleichterten Anordnung. Das

589 5 U. S. C. § 552a (b).
590 18 U. S. C. § 3123 (c) (1) und (2).

heißt, selbst wenn die Kommunikationsinhalte erlangt werden, besteht keine Mitteilungspflicht, soweit dies mit einer normalen Anordnung, also einem *warrant*, erfolgt. Die Mitteilungspflicht kann für einen Zeitraum von höchstens neunzig Tagen zurückgestellt werden, wenn das Gericht feststellt, dass ein Grund zur Annahme besteht, dass die Benachrichtigung über das Vorliegen einer gerichtlichen Anordnung nachteilig sein kann: wenn die Gefährdung des Lebens oder der körperlichen Sicherheit einer Person, die Flucht vor der Strafverfolgung, die Vernichtung oder die Manipulation von Beweisen oder die Einschüchterung potenzieller Zeugen droht oder wenn andernfalls ernsthaft eine Untersuchung gefährdet wird oder sich eine Verhandlung unnötig verzögert.[591]

Die Benachrichtigung ist aber nicht erforderlich für die Erhebung von Verkehrsdaten. Bei der Erhebung von Kommunikationsdaten nach § 2703 (c) oder nach § 3121 ff. entsteht keine Mitteilungspflicht. Bei der Datenerhebung nach § 2709 kann das FBI sogar das Offenlegungsverbot der Anfrage durch den Anbieter anfordern, wenn es versichert, dass das Fehlen eines Offenlegungsverbots zu einer Gefahr für die nationale Sicherheit der Vereinigten Staaten, zu einer Störung der strafverfolgenden oder geheimdienstlichen Ermittlungen, zu einer Störung der diplomatischen Beziehungen oder zu einer Gefahr für das Leben oder die körperliche Sicherheit einer Person führen kann.[592]

Der Rechtsschutz setzt die Kenntnisnahme des von einer staatlichen Maßnahme Betroffenen voraus. Die staatliche Behörde besitzt und verwendet hier jedoch die Kommunikationsdaten des Betroffenen, ohne dass er von dieser Maßnahme weiß. Doch unter dem Umstand, dass der Betroffene nicht davon weiß, kann der Schutz gegen eine unbefugte oder unbeschränkte Erhebung, Speicherung, Verwendung und Weitergabe von Kommunikationsdaten unmöglich gewährleistet werden.

591 18 U. S. C. § 2703 (b) (1) (B) und § 2705 (a) (1) und (2).
592 18 U. S. C. § 2709.