Einleitung

A. Freiheit und Sicherheit im digitalen Zeitalter

I. Daten als Machtquelle

Im digitalen Zeitalter sind Informationen[1] Macht. Die Erhebung, Speicherung und Nutzung von Daten ist zu einer wichtigen Ressource für den gesamten sozialen und wirtschaftlichen Austausch geworden. Die Macht der Information offenbart sich vor allem dann, wenn im Zuge moderner Datenverarbeitungsprozesse, bei denen in Echtzeit Daten in riesigen Mengen erzeugt werden, ein im Grunde unbedeutendes Datenelement durch die der Informationstechnologie inhärenten Verarbeitungs- und Verknüpfungsmöglichkeiten einen neuen Stellenwert erhält. Die mit dem Aufkommen des digitalen Zeitalters einhergehenden Veränderungen in unserem Leben brachten unter anderem die Entwicklung und die rasche Verbreitung des Personal Computers (PC) mit sich. Durch die Entwicklung von Datenbanken und der jeweils zugehörigen Office-Software-Typen wurden Arbeitsprozesse in erheblichem Maße beschleunigt und erleichtert. Anders als bei der Verwendung von Papier, das einem physischen Verfallsprozess unterliegt, können Daten beliebig lange gespeichert und abgerufen werden. Einmal gespeichertes Wissen geht nicht mehr verloren und ist jederzeit zugänglich. Die Entwicklung des World Wide Web hat die rapide Steigerung der Erzeugung, der Verteilung und des Verbrauchs von Daten verursacht. Die hochgradig entwickelte Informationstechnologie hat folglich das Leben des Einzelnen auf signifikante Weise verändert. Des Weiteren ist das technische Verständnis im Umgang mit dem Computer für die

1 Laut *Luciano Floridi* werden vier Arten von miteinander kompatiblen Phänomenen als Information bezeichnet: 1) Informationen über etwas (z. B. einen Zugfahrplan); 2) Informationen als etwas (z. B. DNA oder Fingerabdrücke); 3) Informationen für etwas (z. B. Algorithmen oder Anweisungen); 4) Informationen in etwas (z. B. ein Muster oder eine Beschränkung). Nach *Floridi* wird das Wort „Informationen" meist metaphorisch oder abstrakt verwendet, was dazu führt, dass dessen Bedeutung unklar ist. Hier bezieht sich das Wort „Information" jedoch auf Erkenntnisse, die durch die Kombination und die Analyse verschiedener Daten erhalten wurden. Es wird also verwendet, um Informationen von Daten als solchen zu unterscheiden.

Bürger zu einem entscheidenden Faktor geworden, um als Mitglied auf dem neu strukturierten Arbeitsmarkt bestehen zu können.[2]

Die Entwicklung der elektronischen Kommunikationstechnologie, die Universalisierung des Internets und die Verbreitung des PC haben es Einzelpersonen ermöglicht, zeit- und ortsunabhängig Zugang zu Daten zu haben, verschiedene Daten zu sammeln sowie neue Daten zu schaffen und zu verarbeiten. Unter dem Schlagwort *Informationsgesellschaft* leben die Bürger im 21. Jahrhundert, fernab des industriell geprägten Lebens vorangehender Generationen, in einer neu geschaffenen, digitalen Welt des zeit- und ortsunabhängigen Zugangs zu Informationen, der Kommunikation via E-Mail sowie der Möglichkeit des elektronischen Geschäftsverkehrs.[3] Man kann mit einer kleinen und leichten Kreditkarte, einem Computer oder einem Smartphone wirtschaftliche Transaktionen durchführen, verschiedene Daten sammeln oder neue Daten erzeugen und verarbeiten. Durch Kreditkartentransaktionen anstelle von Barzahlungen wird die Transaktionshistorie schnell an Kreditkartenunternehmen, Produkthersteller sowie Informationsunternehmen übertragen. Diese Unternehmen sammeln und verarbeiten die übermittelten Daten, um sie zum Zwecke der Gestaltung ihrer Werbung oder ihrer Produkte anzuwenden. Die Besuche der Webseiten über das Internet hinterlassen Cookies auf dem Computer des Benutzers. Diese Cookies werden von Unternehmen ebenfalls zur Sammlung von Daten für die Analyse des Verbraucherverhaltens genutzt. So können personenbezogene Daten, die über das Internet übertragen werden, auf verschiedene Weise verwendet werden. Auch durch die Verwendung zunächst unbedeutend scheinender Datenelemente können aufgrund des Umstands, dass große Mengen an Daten elektronisch gesammelt, verarbeitet und genutzt werden, durch die Kombination mit unzähligen weiteren Daten neue Informationen generiert werden. Veränderungen in der sozialen Struktur führen zu Veränderungen in der Lebensweise und Denkweise der Menschen. In einer solchen Gesellschaft kann niemand leugnen, dass die Fähigkeit, Daten zu sammeln, zu verarbeiten und zu nutzen, eine wesentliche Rolle spielt. Heutzutage ist das

2 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 26 m. w. N.

3 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 17 m. w. N.

menschliche Leben ohne die Informationstechnologie nicht mehr vorstellbar.

II. Daten als neue Bedrohungsquelle der Freiheit

Es ist offensichtlich, dass die Verbreitung des Internets, die automatisierte Datenverarbeitung, die verbesserten Zugangsmöglichkeiten zu Daten und das World Wide Web das Alltagsleben der Menschen bequemer gestalten. Neben diesen Vorteilen entstehen jedoch auch viele Nachteile oder zumindest Umstände, bezüglich derer man Bedenken anmelden kann. Diese Bedenken betreffen vor allem die mögliche Beeinträchtigung der Grundrechte der Bürger und die potenzielle Entwicklung von einem Verfassungs- zu einem Überwachungsstaat. Die elektronische Verarbeitung personenbezogener Daten macht es Einzelpersonen schwer oder unmöglich, ihre Daten zu kontrollieren. Unter den Bedingungen der modernen Datenverarbeitung stellen die Bürger ihre personenbezogenen Daten oft zur Verfügung, ohne zu wissen, wo und wie ihre Daten verwendet und wohin sie übermittelt werden. Die Erweiterung der Speicherung sowie die uneingeschränkte Verarbeitung personenbezogener Daten ermöglichen es Unternehmen, Medien und sogar dem Staat, tiefere Einblicke in das Privatleben von Einzelpersonen zu gewinnen, wodurch die Freiheitsrechte dieser Einzelpersonen potenziell gefährdet sind. Die Bürger müssten in so einem Fall die sogenannte *Zero Privacy Society*[4] fürchten, in der ihre personenbezogenen Daten nicht vor potenziellem Missbrauch durch Befugte oder Unbefugte sicher sind. Niemand könnte sich hier vor einem möglichen Missbrauch personenbezogener Daten, sei es durch den Staat, durch Privatpersonen und insbesondere durch Unternehmen, absichern. Werden Daten durch Computer und Netzwerke über das Internet verarbeitet und kontrolliert, kann die unbefugte Datenspeicherung sowie der unbefugte Zugriff auf oder die unbefugte Verwendung von gespeicherten Daten schwerwiegende Konsequenzen haben. Personenbezogene Daten, die durch Computer und das Internet erhalten werden, werden im privaten Sektor hauptsächlich

4 *Scott McNealy*, CEO von Sun Microsystems, sagte einmal: „Wir haben bereits ‚zero privacy'. Finden Sie sich damit ab." (*Solove/Rotenberg/Schwartz*, Information Privacy Law, S. 635); „It is already far too late to prevent the invasion of cameras and databases. The djinn cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases" (*Brin*, The Transparent Society, S. 8–23).

zu dem Zweck gesammelt und verarbeitet, die Verbrauchsmuster von Käufern zu analysieren und die Arbeitshaltung am Arbeitsplatz zu verwalten. Beispielsweise bietet die *Ubiquitous-Technologie*[5] einen Mechanismus zur Weitergabe und Überwachung personenbezogener Daten, der weiter geht als je zuvor, da beim Herstellen einer Verbindung zu einem Endgerät über ein bestimmtes Netzwerk sowohl der aktuelle Standort des Benutzers als auch weitere nachverfolgbare Verhaltensmuster in Echtzeit angezeigt werden können.

III. Datennutzung im Strafverfahren

Auf staatlicher Ebene werden zum Schutz der öffentlichen Sicherheit internationale Antiterrornetzwerke aufgebaut. Hierbei werden beträchtliche Mengen personenbezogener Daten von Bürgern gesammelt und gespeichert. Diese Tendenz ist auch im Strafverfahren zu beobachten. Der Um-

5 Einhergehend mit dem Eintreten in die *Ubiquitous Society* werden vier Internet-Szenarien für die Zukunft vorgeschlagen: 1) eine Welt, in der die menschlichen Bedürfnisse in hohem Maße berücksichtigt werden; 2) eine Welt, in der die grundlegenden Leistungen für alle angeboten werden; 3) eine Welt, in der jeder Inhalt, jedes Gerät oder jedes Format jederzeit abrufbar sind und 4) eine Welt, in der Viren, Spam, Junkmails oder Hacking nicht existieren können (Digital Dystopia). (Smart Internet Technology CRC, „Smart Internet 2010“, 09.2005). Durch die Kombination von Informationstechnologien wird eine *Ubiquitous-Gesellschaft* geschaffen, die die Bedürfnisse von Einzelpersonen, Ländern oder Gesellschaften jederzeit und überall in Echtzeit befriedigen kann. Der Ausdruck *Ubiquitous-Technologie* bezieht sich dabei auf eine Technologie, die die Fernsteuerung von alltäglichen Bedarfsgegenständen, Haushaltsgeräten und automatisierten Wohnräumen über eine Vielzahl von alltäglichen Bedarfsgegenständen ermöglicht, die hochmoderne Mikro-Halbleiter enthalten und die jederzeit und überall den Zugriff auf ein großes Netzwerk ermöglichen. Dies erzeugt ein Umfeld, das verschiedene Informationskommunikationsdienste nutzen kann, indem es unabhängig von Zeit und Ort auf das Informationskommunikationsnetzwerk zugreift. Es handelt sich um eine Voraussetzung für die allgegenwärtige Netzwerktechnologie, die Computer- sowie Informations- und Kommunikationstechnologien in verschiedene Geräte und Objekte integriert, sodass die Benutzer jederzeit und überall miteinander kommunizieren können. Es geht also um eine Gesellschaft, deren Gebrauchsgegenstände „intelligent“ (smart) und miteinander vernetzt sind, um die Kommunikation zwischen Menschen und Menschen, zwischen Gegenständen und Menschen und sogar zwischen Gegenständen und Gegenständen zu ermöglichen. Des Weiteren wird die Wettbewerbsfähigkeit des Staates durch die Verbesserung der individuellen Lebensqualität, die Steigerung der Unternehmensproduktivität und die Innovation öffentlicher Dienstleistungen gestärkt.

gang mit personenbezogenen Daten, insbesondere mit denen, die elektronisch gespeichert sind, hat im Strafprozessrecht in den letzten Jahren eine immer größere Bedeutung erlangt. Im Zuge des technischen Fortschritts haben sich die strafprozessualen Ermittlungen geändert. Das Aufkommen von Computern, die große Mengen an Informationen speichern können, hat die Polizei dazu veranlasst, diese zu Zwecken von Rasterfahndungen zu nutzen.[6] Nach den Terroranschlägen vom 11. September 2001 führte die Angst vor neuen Terroranschlägen weltweit zu einer Diskussion um den Einsatz umfassender und effektiver Antiterrormaßnahmen.[7] Diese Angst führte zu einem erhöhten Bedürfnis nach Sicherheit und Prävention, das ihrerseits zur Schaffung neuer Straftatbestände und Ermittlungsmaßnahmen führte, auch auf Kosten der Freiheit. Auf dieser Grundlage entstanden in der jüngeren Vergangenheit und entstehen weiterhin in der Strafprozessordnung neuartige Ermittlungsmethoden, die elektronische personenbezogene Daten verwenden. Aufgrund der Verbreitung sozialer Netzwerke steht dabei ein bedeutender Datenschatz zur Verfügung, der auf vielfältige Art und Weise genutzt werden kann. Die Möglichkeiten zur Verbrechensaufklärung sind beispielsweise durch die Verfügbarkeit von Verkehrsdaten besser geworden. In dieser Hinsicht bietet die technische Entwicklung große Vorteile für strafprozessuale Ermittlungen.

Wo jedoch die Veröffentlichung von Informationen und der unkomplizierte Zugang zu personenbezogenen Daten allgegenwärtig ist, besteht die Gefahr, dass der Schutz der Persönlichkeit des Einzelnen und – in Verbindung damit – sein Recht auf Wahrung einer geschützten Privatsphäre zugunsten übergeordneter Interessen der Gemeinschaft in den Hintergrund treten. Für die Effektivität der Ermittlung (Sicherheitsgarantie) ist die möglichst umfangreiche Speicherung und Auswertung möglichst vieler Daten offensichtlich nützlich. Dabei werden die Sicherheitsinteressen des Staates nicht selten stärker gewichtet als die von diesen staatlichen Eingriffsbefugnissen betroffenen Freiheitsrechte der Bürger.[8] Dies kann

6 Ende der siebziger, Anfang der achtziger Jahre sorgten Veröffentlichungen in der Presse über durchgeführte Datenabgleiche für gesteigerte Aufmerksamkeit. So wurde bekannt, dass die Ermittlungsbehörden sich mehrfach und mit unterschiedlichem Erfolg der Rasterfahndung bedient hatten.

7 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 18.

8 *Bundesbeauftragter für den Datenschutz,* 19. Tätigkeitsbericht – 2001–2002, BT-Drs. 15/888, S. 24 f.; *Weichert,* Grundrechte in der Informationsgesellschaft, DuD 2000, 104, 106; *Germann,* Gefahrenabwehr und Strafverfolgung im Internet, S. 35.

jedoch zu einer grenzüberschreitenden Überwachung durch den Staat führen. Denn es besteht die Möglichkeit, dass einzelne Datenbankkonstruktionen oder Personalisierungsarbeiten, die mit personenbezogenen Daten in öffentlichen und nichtöffentlichen Sektoren durchgeführt werden, durch die öffentliche Sicherheitsgarantie sowie die Aufrechterhaltung der Ordnung und des Gemeinwohls oder durch optimale Nutzung von personell und materiell begrenzten Ressourcen gerechtfertigt werden. Die Gefahren hierbei liegen unter anderem in einer maßlosen Datenerhebung, -speicherung und -weitergabe sowie in unbefugtem Zugriff auf die Daten.[9] Ein solches Datenverarbeitungsverhalten könnte zur Verwirklichung von Foucaults Panopticon[10] führen, in dem die Bürger sowohl vom *Big Brother* (dem Staat) als auch vom *Big Browser* (dem Privaten) flächendeckend überwacht werden. Die elektronische Verarbeitung personenbezogener Daten macht es dem Einzelnen schwer oder sogar unmöglich, die Erhebung, Speicherung und Verwendung seiner Daten zu überblicken und zu kontrollieren. Die Art und Weise der Datenverarbeitung seitens des Staates kann den Lebensstil und das Kommunikationsverhalten der Bürger, folglich auch das Gemeinwohl entscheidend beeinträchtigen.[11] Gemäß dem Konzept des Panopticons unterlägen die persönlichen Entfaltungsmöglichkeiten der Bürger den Beschränkungen durch die Überwachung und Registrierung durch den Staat. Dies würde dazu führen, dass die Bürger sich der Überwachung in einem bestimmten Maße bewusst werden, sich darauf einstellen und sich den an sie gerichteten Erwartungen anpassen.[12] Werden diese bedeutenden Probleme vom Gesetzgeber nicht

9 Vgl. *Bull*, Datenschutz oder die Angst vor dem Computer, S. 242: Die Datenschützer sahen in den Ermittlungsmethoden – insbesondere z. B. in der Rasterfahndung – die Gefahr, „dass jeder in Verdacht geraten könne, auch der Fromme und Frömmste, auch der Unauffälligste."

10 Foucaults Panopticon beschreibt einen Ort, an dem jede Person vollständig beobachtet werden kann. Es beschränkt sich also nicht auf das ‚Panradicon'. Ein Panopticon ist schließlich ein Ort, an dem jede Bewegung eines anderen, unabhängig von seiner Form, sei es kreisförmig oder quadratisch, überwacht werden kann.

11 BVerfGE 65, 1 (43).

12 *Schmidt*, Die bedrohte Entscheidungsfreiheit, JZ 1974, 241, 245; Foucaults Kernprinzip beim Panopticon besteht darin, dass das Überwachungsobjekt das „Auge" der Überwachung verinnerlicht. Die Person, die in einem Panopticon überwacht wird, weiß nicht, wann der Blick der Überwachung in einem bestimmten Raum oder Bereich auf sie fallen wird. Die Überwachten verinnerlichen daher die Existenz eines solchen Blickes, sodass das Verlangen nach Aufbruch und Rebellion, das von innen heraus entstehen kann, unterdrückt wird, was dazu führt, dass

hinreichend berücksichtigt, können solche neuen Ermittlungsmethoden zu einer grenzüberschreitenden Überwachung durch den Staat führen und damit die Freiheitsrechte der Bürger gefährden. Innerhalb der Gesellschaft wächst die Besorgnis, dass sich der Verfassungsstaat als Reaktion auf die terroristische Bedrohung in einen Überwachungs- oder Präventionsstaat verwandelt.[13]

IV. Notwendiger Datenschutz

Die oben beschriebenen neuen Ermittlungsmittel generieren in der Konsequenz also auch Gefahren für den Datenschutz und die Privatsphäre. Die Standardisierung der Datenerhebung, die elektronische Datenspeicherung und deren weltweite Nutzung, der Trend zu immer detaillierteren Datensammlungen für unterschiedliche Zwecke, die zunehmende Vernetzung der Systeme und das wachsende Verlangen nach eigenmächtigem Zugriff auf die in anderen Datenbanken gespeicherten Informationen[14] gefährden den Schutz personenbezogener Daten und der Privatsphäre. Die Möglichkeiten und Gefahren der automatisierten Datenverarbeitung haben daher die Notwendigkeit des Datenschutzes deutlich hervortreten lassen. Je größer die Bedeutung der Datennutzung in einer Informationsgesellschaft wird, desto stärker bekundet die Gesellschaft ihr Interesse an Datenschutz. Es handelt sich hierbei also um ein Spannungsverhältnis zwischen der Aufgabe des Staates, für die Sicherheit seiner Bürger zu sorgen, und dem Recht auf informationelle Selbstbestimmung des Einzelnen. Der Staat ist dazu verpflichtet, die Sicherheit zu gewährleisten und zugleich die Grundrechte der Bürger zu achten. Jeder Eingriff in die Grundrechte muss in einem ausgewogenen Verhältnis zu dem gewählten Mittel und dem beabsichtigten Zweck stehen.[15] Daraus ergibt sich, dass der Staat die Sicherheit seiner Bürger durch möglichst geringe Eingriffe in die Freiheitsrechte zu gewährleisten hat. Dazu ist ein Ausgleich zwischen dem Datenschutz

---

die Regeln aus Angst vor Überwachung immer und überall eingehalten werden, selbst dann, wenn das Individuum de facto gar nicht überwacht wird.

13 *Hirsch*, Gesellschaftliche Folgen staatlicher Überwachung, DUD 2008, 87, 89; *Albrecht, P.-A.*, Vom Präventionsstaat zur Sicherheitsgesellschaft, Wege kontinuierlicher Erosion des Rechts, in: *Herzog/Hassemer* (Hrsg.), Festschrift für Winfried Hassemer; dazu kritisch *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, S. 18.

14 *Tolzmann*, Bundeszentralregistergesetz, S. 1.

15 BVerfGE 35, 410.

einerseits und der Datennutzung zum Zweck der Verbrechensprävention oder -aufklärung andererseits erforderlich.

Als Reaktion auf eine sich zunehmend zu einer Leistungsverwaltung entwickelnden öffentlichen Verwaltung, die sich immer komplexeren Aufgabenstellungen und damit korrespondierend ständig steigenden Informationserwartungen ausgesetzt sah, erfolgte die fortschreitende Automatisierung der Datenverarbeitung. Die mit dieser Automatisierung einhergehenden Gefahren für die Persönlichkeitsrechte des Einzelnen bestehen zum einen in möglichen Fehlinformationen durch Falschverarbeitung und zum anderen im Kontextverlust durch Abtrennung abstrakter Daten von dem konkreten Lebenszusammenhang, innerhalb dessen sie erhoben worden sind, sowie in dem Informationsvorsprung, den die öffentliche Verwaltung zunehmend erhält. Diese Gefahren mussten zu sozialen und politischen Konsequenzen in Form von gesetzlichen Regelungen zum Schutz der Bürgerinnen und Bürger führen.[16] Auch das Bundesverfassungsgericht hat die der EDV immanenten Gefahren wahrgenommen und die Notwendigkeit des Schutzes davor betont.[17] Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung und Verwendung sowie gegen die Weitergabe seiner personenbezogenen Daten voraus. Dieser Missbrauch kann entweder innerhalb des Gesetzesrahmens erfolgen, etwa durch die Ausnutzung von Lücken in bestimmten Vorschriften, oder aber im Rahmen eines Vertrags mit Dateninhabern, die sich das Fehlen solcher Gesetze zunutze machen. Von Seiten der Gesetz-

16 *Tolzmann*, Bundeszentralregistergesetz, S. 25 ff.

17 BVerfGE 65, 1 (42 f.): „Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweisen oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen."

gebung wurde bereits mit zahlreichen Novellierungen bestehender sowie durch die Verabschiedung neuer Gesetze auf die zunehmende elektronische Verarbeitung von Daten reagiert.

Um die Bürger vor einer übermäßigen oder unbefugten Erhebung, Speicherung, Verwendung und Weitergabe ihrer Daten zu schützen – obwohl all dies zur Effizienz von Ermittlungen beitragen mag –, sollten verfahrensrechtliche und organisatorische Sicherheitsvorkehrungen getroffen werden. Ohne diesen Schutz kann eine Person sich nicht frei entfalten. Im Zusammenhang mit diesem Ausgleich zwischen dem Datenschutz und der Datenverwendung gibt es in Deutschland bereits einige Entscheidungen des Bundesverfassungsgerichts – z. B. das Vorratsdatenspeicherungsurteil[18] oder das Volkszählungsurteil[19] – sowie einige gesetzliche Regelungen.[20,21] Einige Autoren haben sich bereits mit dem Interessenausgleich zwischen Freiheit und Sicherheit in Bezug auf das Thema Datenschutz befasst.[22] Es mangelt gleichwohl an einer rechtsvergleichenden Untersuchung oder einer Gesamttheorie sowie an grundsätzlichen Lösungsprinzipien, die in sämtlichen Stadien des Strafverfahrens Anwendung finden können. Wesentlich für jeglichen Diskurs über den Datenschutz im Strafverfahren ist die Klärung der folgenden Fragen und Faktoren: Mit welchen verfahrensrechtlichen und organisatorischen Sicherheitsvorkehrungen sind strafprozessuale Maßnahmen versehen, die personenbezogene Daten für Zwecke des Strafverfahrens nutzen? Sind die Vorkehrungen im Hinblick auf die Eingriffsintensität einer Maßnahme hinreichend, um die Freiheitsrechte der Bürger zu schützen? Darüber hinaus gibt es weitere Aspekte, die zum effektiven Schutz personenbezogener Daten unter den Bedingungen der modernen Datenverarbeitung zu beachten sind. Als Voraussetzung gilt,

18 BVerfGE 125, 260.

19 BVerfGE 65, 1: Das Volkszählungsurteil ist eine Grundsatzentscheidung des Bundes-verfassungsgerichts vom 15. Dezember 1983, mit der das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde etabliert wurde. Das Urteil gilt als ein Meilenstein des Datenschutzes.

20 Zum Beispiel im BDSG, TKG oder in der StPO usw.

21 In diesem Zusammenhang gibt es in den USA den Privacy Act (1974), den Electronic Communications Privacy Act (1986) und den Communications Assistance for Law Enforcement Act (1994) usw.

22 Vgl. *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit; *Wiedner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht; *Wiedemann*, Regieren mit Datenschutz und Überwachung.

dass es für die Betroffenen nachvollziehbar sein muss, welche ihrer Daten von wem, in welchem Verwendungszusammenhang weiterverarbeitet werden dürfen. Hierfür ist auch erforderlich, dass die Zwecke der Datenverarbeitung bereichsspezifisch und präzise festgelegt werden, d. h. die für einen bestimmten Zweck erhobenen Daten dürfen nicht ohne Weiteres für andere Zwecke an andere Stellen weitergegeben werden.

B. Forschungsziel, Forschungsmethode und Gang der Untersuchung

I. Forschungsziel

Das Forschungsziel besteht darin, einen grundsätzlichen Lösungsansatz für den Schutz und die Auswertung personenbezogener Daten im Strafverfahren zu finden. Das dient nicht nur der Analyse der vorhandenen Rechtslage des Strafrechts, sondern soll auch zur Erarbeitung verschiedener Reformvorschläge führen. Es soll dargelegt werden, ob und inwieweit persönliche Daten im Strafverfahren genutzt werden und wie sie in Zukunft im Strafverfahren geschützt werden sollten. Gegenstand der vorliegenden Untersuchung sind dabei Ermittlungsmaßnahmen im Rahmen des neuen Strafprozessrechts sowie außerhalb des Strafprozessrechts, aber es sollen auch diverse klassische Fragestellungen miteinbezogen werden.

Im Vordergrund dieser Untersuchung steht die Frage, ob und wie unter den Bedingungen der modernen Datenverarbeitung Freiheits- und Sicherheitsinteressen miteinander in Einklang gebracht werden können. Ein wesentlicher Bestandteil der Arbeit ist dabei die Untersuchung der Fragen, wie der Schutz der Privatsphäre bzw. personenbezogener Daten als ein Freiheitsgrundrecht der Bürger im Grundgesetz festgelegt ist, wie personenbezogene Daten im Strafverfahren genutzt werden, ob und inwieweit die neuen sicherheitspolitischen Instrumente, die personenbezogene Daten verwenden, mit Maßnahmen bewehrt sind, sodass die Bürger vor der unbefugten oder übermäßigen Erhebung, Speicherung und Nutzung ihrer personenbezogenen Daten geschützt werden, und ob die getroffenen Maßnahmen hinreichend sind, um die Freiheitsrechte des Einzelnen unter den Bedingungen der automatisierten Datenverarbeitung zu schützen. Denn nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 über die Vorratsdatenspeicherung wurde die Frage, ob und wie durch das Grundgesetz ein Ausgleich zwischen Freiheit und Sicherheit erzielt

wird, der den Herausforderungen des 21. Jahrhunderts gerecht wird, neu aufgeworfen.[23]

II. Forschungsmethode

1. Gründe für die Länderauswahl

Die Untersuchungsgegenstände hinsichtlich der Forschungsfragen der vorliegenden Arbeit bilden das deutsche und das amerikanische Recht. Diese Rechtsordnungen wurden nicht nur deswegen ausgewählt, weil sie wichtige Referenzrechtsordnungen darstellen, sondern auch insbesondere im Hinblick auf ihre grundlegenden Unterschiede, die interessante rechtsvergleichende Ergebnisse versprechen. Die vorliegende rechtsvergleichende Untersuchung zielt daher insbesondere darauf ab, Hinweise auf vorbildhafte Ausgleichsregelungen zu finden. Die Auswahl soll durch die folgenden Erwägungen näher begründet werden:

Die deutsche und die US-amerikanische Rechtsordnung beruhen grundsätzlich auf unterschiedlichen rechtssystematischen Grundlagen, nämlich auf dem kontinentaleuropäischen Recht auf der einen und dem *Common Law* auf der anderen Seite. Die beiden Rechtsordnungen unterscheiden sich ferner auch in ihrer rechtspolitischen Orientierung: die sogenannte *right-dominated-policy* steht im Gegensatz zu der sogenannten *market-dominated-policy*. Es scheint interessant zu beobachten, wie die beiden Rechtsordnungen auf dieser unterschiedlichen Grundlage die Aufgabe des Datenschutzes unter den Bedingungen der modernen Datenverarbeitung wahrnehmen. Bislang wurden in der europäischen Union einige Richtlinien und Verordnungen zum Datenschutz erlassen. Aus der Feststellung seitens der EU, dass die USA im Vergleich zu den EU-Mitgliedstaaten hinsichtlich des Datenschutzes kein angemessenes Schutzniveau bieten, ergab sich die Unterzeichnung der Safe-Harbor-Vereinbarung zwischen dem US-Handelsministerium und der Europäischen Kommission. Außerdem wurde mit dem NSA-Skandal die Diskussion um das Verhältnis zwischen Freiheit und Sicherheit im digitalen Zeitalter neu entfacht. Überraschenderweise zeigte der NSA-Skandal auf, dass die USA über ein umfangreicheres Überwachungsprogramm als Deutschland verfügen oder verfügt haben. In Deutschland gibt es zwar schon rechtsvergleichende Untersu-

23 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 2.

chungen bezüglich anderer Mitgliedstaaten der EU,[24] jedoch fehlt es an rechtsvergleichenden Untersuchungen bezüglich der US-amerikanischen Rechtsordnung.

Die methodische Herausforderung bei diesem Ansatz besteht darin, dass aufgrund der ausgeprägten föderalistischen Struktur der USA das bundesstaatliche und das einzelstaatliche Recht nebeneinander stehen. In vielen Bereichen fehlt es daher häufig an einer umfassenden Kodifizierung auf bundesstaatlicher Ebene. Um den Vergleich des US-amerikanischen Rechts mit dem deutschen Recht sinnvoll durchzuführen, wird daher in der vorliegenden Arbeit in bestimmten Bereichen zunächst auf eine umfassende Kodifizierung auf bundesstaatlicher Ebene eingegangen. Sollten bundesstaatliche Kodifizierungen fehlen, so soll exemplarisch auf die einzelstaatlichen Regelungen zurückgegriffen werden.

2. Rechtsvergleichende Untersuchung im Rahmen des Verfassungsrechts und des einfachen Rechts

Um das Ziel der vorliegenden Arbeit zu erreichen, das darin besteht, durch eine rechtsvergleichende Untersuchung einen grundsätzlichen Lösungsansatz zu finden, ist es sinnvoll, die Rechtslagen in beiden Ländern mit den unterschiedlichen Rechtssystemen sowohl im Verfassungsrecht als auch im einfachen Recht zu untersuchen und den Datenschutz sowie die Datennutzung in beiden Rechtsordnungen miteinander zu vergleichen.

3. Untersuchung in ausgewählten Einzelbereichen: Vorratsdatenspeicherung, Rasterfahndung und Strafregister

Nach der Einführung in die Datenverwendung im Strafverfahren wird die Untersuchung in den Einzelbereichen vertieft. Zunächst wird der Themenkomplex um das Strafregister analysiert, bevor die Rasterfahndung als ein neuartiges Ermittlungsmittel in der StPO untersucht werden soll. Schließlich wird die Vorratsdatenspeicherung als ein aktueller Bereich in Bezug auf den Datenschutz und gleichzeitig als eine Maßnahme außer-

24 Zum Beispiel im Bereich der Vorratsdatenspeicherung: *Chmielewski*, Die Vorratsdatenspeicherungsrichtlinie und ihre Umsetzung in Deutschland und in Polen; *Roßnagel/Moser-Knierim/Schweda*, Interessenausgleich im Rahmen der Vorratsdatenspeicherung.

halb der StPO, also als eine Maßnahme des überstrafprozessrechtlichen Präventionsrechts beleuchtet. Obwohl die Problemstellungen hinsichtlich des Strafregisters zunächst nur in geringem Maße mit den beiden anderen Themen zusammenzuhängen scheinen, ermöglicht eine dahingehende Untersuchung einen Überblick über einen klassischen Bereich, in dem personenbezogene Daten verwendet werden, wodurch es möglich wird, ein breites Spektrum von Problemen bezüglich des Datenschutzes im Strafverfahren zu behandeln.

4. Funktionale Rechtsvergleichung bei einzelnen Maßnahmen

Methodisch soll die Untersuchung mittels einer funktionalen Rechtsvergleichung vorgenommen werden. Unvergleichbares kann nicht sinnvoll miteinander verglichen werden, und vergleichbar ist im Recht nur, was dieselbe Aufgabe, dieselbe Funktion erfüllt.[25] Daher wird ein aussagekräftiger Vergleich in Bezug auf die Verwendung und den Schutz personenbezogener Daten in den untersuchten Rechtsordnungen nur auf dem Wege eines Vergleichs derjenigen Regelungen erreicht, die in den ausgewählten Bereichen funktional dieselbe Aufgabe übernehmen. Die Gesamtlösung der untersuchten Problemstellung erfordert daher auf allen Ebenen die Erkennung sämtlicher funktionaler Äquivalente nach einer umfassenden Betrachtung der zu untersuchenden Rechtsordnungen.[26]

III. Gang der Untersuchung

Die vorliegende Arbeit lässt sich in fünf Teile gliedern:

Im ersten Teil mit dem Titel „Kollision zwischen Freiheit und Sicherheit“ werden die neuen Herausforderungen beleuchtet, die sich angesichts des Versuchs stellen, im digitalen Zeitalter sowohl Freiheit als auch Sicherheit zu gewährleisten. Hierbei wird erklärt, wie und warum sich die soziale Kontrolle in der modernen Gesellschaft verändert hat und welche neuen technikgestützten Instrumente in Strafangelegenheiten unter diesen

25 *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, 3. neubearb. Aufl., 1996, S. 33.

26 *Sieber*, Strafrechtsvergleichung im Wandel: Aufgaben, Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft, in: Sieber/Albrecht (Hrsg.), Strafrecht und Kriminologie unter einem Dach, Berlin 2006, S. 112 f.

Bedingungen eingesetzt werden. Durch die Vorführung neuer technikgestützter Instrumente lässt sich nachvollziehen, in welchem Maße sich die strafrechtlichen Ermittlungsmaßnahmen im digitalen Zeitalter geändert haben. Anknüpfend an die Thematisierung der internationalen Besorgnis und der Bemühungen um den Datenschutz folgt die Untersuchung des Verhältnisses zwischen Freiheit und Sicherheit angesichts neuer Herausforderungen.

Teil zwei und Teil drei präsentieren einen Landesbericht jeweils für Deutschland und die USA bezüglich des verfassungsrechtlichen Datenschutzes und des Datenschutzes bei konkreten strafrechtlichen Maßnahmen des Strafregisters, der Rasterfahndung und der Vorratsdatenspeicherung. Es bedarf einer verfassungsrechtlichen und einfachgesetzlichen Analyse des Datenschutzes sowie der Datennutzung. Konkret wird untersucht, wie personenbezogene Daten verfassungsrechtlich geschützt werden, welche Rolle diese Daten in den ausgewählten Bereichen spielen und welche Maßnahmen bei der Nutzung dieser Daten zum Schutz des Einzelnen vor möglichen Gefahren ergriffen werden.

Im vierten Teil wird auf Grundlage der oben genannten Landesberichte der Datenschutz im Verfassungsrecht sowie hinsichtlich der konkreten Maßnahmen in beiden Ländern rechtsvergleichend untersucht. Durch diesen Rechtsvergleich sollen die Notwendigkeiten und die Mängel des Datenschutzes klar definiert werden.

Im Anschluss an die Zusammenfassung der Untersuchungen wird auf die Fragen eingegangen, wie im digitalen Zeitalter die Privatsphäre bzw. die personenbezogenen Daten als Freiheitsgrundrechte des Einzelnen verfassungsrechtlich geschützt werden sollen und welche Anforderungen auch bei Einführung neuer technikgestützter Ermittlungsmaßnahmen in einer freien Gesellschaftsordnung nicht aufgegeben werden dürfen.