Teil 5: Schlussbemerkung

A. Datenschutz vor neuen Herausforderungen

Das digitale Zeitalter hat dem Menschen viele Möglichkeiten eröffnet. Was in der Vergangenheit kaum vorstellbar war, ist heute der Regelfall: elektronische Daten, die täglich und überall erstellt werden, finden mannigfaltige Verwendung und Verarbeitung. Die unter modernsten Datenverarbeitungsbedingungen erlangten Informationen sind zumeist bedeutsamer als die originären Daten an sich. Die schnelle Verarbeitungsgeschwindigkeit und die Speicher- und Verknüpfungsmöglichkeiten im Umgang mit elektronischen Daten machen das menschliche Leben einerseits bequem und praktisch; andererseits können sie das freiheitliche Leben der Menschen jedoch auch gefährden. Aufgrund der Aussagekraft dieser Daten können umfassende Bewegungs- und Persönlichkeitsprofile erstellt werden. Durch die Kombination mit anderen Daten nähern wir uns dem gläsernen Bürger. Der Betroffene kann die Richtigkeit und die Verwendung seiner Daten nicht ausreichend kontrollieren. In bisher unbekannter Weise haben sich die Möglichkeiten einer Einsicht- und Einflussnahme erweitert, die auf das Verhalten des Einzelnen durch psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.[681] Im Rahmen dieser Herausforderungen steht die Freiheit des Einzelnen auf dem Spiel.

Die Krise der Freiheit wird durch soziale Kontrollmechanismen, die auf gesteigerten gesellschaftlichen Sicherheitsbedürfnissen aufgrund permanenter Verunsicherung,[682] Management von Risikoquellen, die sich nicht auf bestimmte Situationen oder bestimmte Personen beziehen, und Techniken des Ausschlusses gefährlicher Personen[683] basieren, immer weiter verschärft. Die Strafrechtspflege steht mit der Einführung neuer technikgestützter Ermittlungsmaßnahmen, die personenbezogene Daten im Strafverfahren verwenden, ebenfalls vor selbigen Problemstellungen. Die Form der Informationsbeschaffung zur Strafverfolgung und zur poli-

681 BVerfGE 65, 1 (42).

682 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., S. 38 ff.

683 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., S. 87 f.

zeirechtlichen Gefahrenabwehr wurde angesichts neuer technischer Möglichkeiten und sicherheitspolitischer Bedürfnisse beständig ausgebaut. Im Namen der Sicherheitsgewährleistung durch effektive strafrechtliche Ermittlungen entstanden einhergehend mit dem Verlust von Freiheit neue Herausforderungen.

Die Freiheit des Einzelnen bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße dem Schutz durch wirksame Vorkehrungen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten des Einzelnen. In diesem Zusammenhang ist die Gewährleistung von Datenschutz von großem Interesse und Aufgabe der modernen Gesellschaft. Zur Bewältigung dieser Datenschutzaufgaben wurden und werden sowohl auf nationaler als auch auf internationaler Ebene zahlreiche Anstrengungen unternommen. Der Schutz personenbezogener Daten als Teil der Privatsphäre unter den modernen Datenverarbeitungsbedingungen kann aus der Verfassung, den einfachen Gesetzen als der Konkretisierung der Verfassung oder den gerichtlichen Entscheidungen anhand allgemeiner Prinzipien und Werte abgeleitet werden.[684] Mit der vorliegenden Arbeit wurde insbesondere aufgezeigt, wie der Datenschutz in Deutschland und den USA implementiert wird. Besondere Anknüpfungspunkte lassen sich hier im Verfassungsrecht und in bestimmten Bereichen des Strafregisters, der Rasterfahndung und der Vorratsdatenspeicherung finden. Ferner wurde in der vorliegenden Arbeit beleuchtet, ob der jeweilige Datenschutz als hinreichend bewertet werden kann, um die Freiheit des Einzelnen effektiv gegen eine potenziell unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten unter der heutigen automatisierten Datenverarbeitung zu schützen.

B. Bilanz der Vergleichsergebnisse

Der Schutz personenbezogener Daten setzt grundsätzlich die Befugnis des Einzelnen voraus, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Konkret bedeutet dies, dass der Einzelne selbst darüber entscheiden kann, ob, wann, wie und in welchem Maße seine Daten veröffentlicht und verwendet werden. Dieses Recht des Einzelnen hat die deutsche Rechtsprechung aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet

684 *Genz*, Datenschutz in Europa und den USA, S. 7.

und konkretisiert. Der Schutz der Daten gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten wurde vom Bundesverfassungsgericht als eine Voraussetzung der freien Persönlichkeitsentfaltung anerkannt.[685] Zum Schutz dieses Rechts stellte das Bundesverfassungsgericht auch konkrete Anforderungen auf: Gesetzesvorbehalt, Normenklarheitsgebot, Verhältnismäßigkeits- sowie Zweckbindungsgrundsatz, verbunden mit der Forderung nach organisatorischen und verfahrensrechtlichen Vorkehrungen. Demgegenüber wurde in den USA der Begriff der *privacy* noch nicht abschließend definiert, und das Recht auf Datenschutz wurde bisher von der Rechtsprechung nur vermutet. Eine feste verfassungsrechtliche Verankerung ist nicht erkennbar. Das entscheidende Kriterium für den Schutz der Privatheit hat sich gemäß der Rechtsprechung vom physischen Betreten eines Raums zur begründeten Erwartung auf *privacy* gewandelt und somit erweitert. Außerdem wird angesichts der fortgeschrittenen technischen Möglichkeiten die Gewöhnlichkeit der eingesetzten Technik im Hinblick auf die subjektive Katz-Prüfung zusätzlich berücksichtigt.

So wird in Deutschland versucht, durch mehrere miteinander verbundene Grundrechte die verschiedenen Aspekte der Privatsphäre und sogar die personenbezogenen Daten als Teil der Privatsphäre zu schützen. Des Weiteren ist der effektive Schutz der Privatsphäre sowie von personenbezogenen Daten gegen neuartige technikgestützte Beeinträchtigungen dadurch möglich, dass der Schutzbereich des allgemeinen Persönlichkeitsrechts möglichst weit interpretiert wird.[686] Zum Schutz personenbezogener Daten tragen mithin die konkreten Anforderungen bei, die auf der Grundlage des Rechts auf informationelle Selbstbestimmung von der Rechtsprechung entwickelt wurden. Darauf basierend werden die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch das BDSG kontrolliert, das wiederum den Umgang mit personenbezogenen Daten grundsätzlich verbietet und nur ausnahmsweise zulässt. Der EuGH befand, dass das Gefühl, überwacht zu werden, das durch das Sammeln umfangreicher Metadaten erzeugt wird, der Privatsphäre abträglich ist und schlug daher vor, dass der Einzelne dann geschützt werden solle, wenn er mit Hilfe neuer technologischer Mittel mit anderen interagiert. Darüber hinaus forderte der EuGH für Eingriffe in die Privatsphäre ein hö-

685 BVerfGE 65, 1 (43).

686 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 76.

heres Maß an gerichtlicher Kontrolle im Hinblick auf Erforderlichkeit und Verhältnismäßigkeit, auch wenn diese Eingriffe aus Gründen der nationalen Sicherheit vorgenommen werden.[687] Deutschland schließt sich beim Schutz der Privatsphäre und der Daten dem EuGH an. Der US-amerikanische Supreme Court hatte kürzlich Interesse an ähnlichen Rechtssachen.[688] Mehrere ständig gültige US-Verfassungsgrundsätze wie etwa die *Third-Party-Doctrine* schränken jedoch den Schutz der Privatsphäre und personenbezogener Daten in der digitalen Welt ein.[689] Indem die US-Verfassung für einen engen inneren und speziellen Bereich den Schutz des Privatlebens i. w. S. zumindest vor hoheitlichen Eingriffen garantiert, so wurde zwar der Rahmen festgelegt, der bestimmte Sphären von Privatheit garantiert, jedoch nur geringe Möglichkeiten bietet, einen alle Bereiche des Privatlebens umfassenden Schutz herbeizuführen.[690] Da hier nur einige bestimmte Bereiche nach dem Grundsatz der „grundsätzlichen Zulassung mit einigen Verbotsausnahmen" rechtlich kontrolliert werden und es kein einheitliches Datenschutzgesetz gibt, scheint der Datenschutz in seiner konkreten Ausgestaltung in den USA noch einen langen Weg vor sich zu haben. Dieser Unterschied hinsichtlich der Grundsätze des Datenschutzes hat zu einer Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA, nämlich zu den Grundsätzen des „Safe Harbor", geführt.[691]

---

687 EuGH, Urteil vom 8. April 2014 in den Rechtssachen C-293/12, C-594/12.

688 In der Rechtssache USA gegen Jones stellte der Gerichtshof einstimmig fest, dass die GPS-Überwachung eines Fahrzeugs, das sowohl geografisch als auch zeitlich den Geltungsbereich eines *warrant* überschreitet, eine Durchsuchung gemäß der vierten Änderung darstellt (United States v. Jones, 132 S. Ct. 945 (949)), und mehrere Richter stellten separat das Erfordernis der Geheimhaltung als Vorbedingung für *privacy* in Frage (United States v. Jones, 132 S. Ct. 945 (957)). In der *Kyllo*-Entscheidung erkannte die Richterin Scalia an, dass die Doktrin des vierten Verfassungszusatzes angepasst werden müsse, um die traditionellen Erwartungen an privacy vor der fortgeschrittenen Technologie zu bewahren (Kyllo v. United States, 533 U. S. 27 (33, 34)).

689 *Fabbrini*, Human Rights in the Digital Age: The Europe Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014, S. 91.

690 *Genz*, Datenschutz in Europa und den USA, S. 48.

691 Safe Harbor, Kommissionsentscheidung 2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA.

Die Unterschiede im Hinblick auf die verfassungsrechtlichen Grundlagen und die Grundsätze des Datenschutzes in beiden Ländern wirken sich auch auf konkrete einfachgesetzliche Maßnahmen aus. Zunehmend spielen personenbezogene Daten in Strafverfahren eine verfahrensrechtlich bedeutsame Rolle. Je größer die Wertigkeit personenbezogener Daten in Strafverfahren ist, desto wichtiger ist auch deren Schutz. Die Verarbeitung personenbezogener Daten ohne angemessene Schutzmaßnahmen gegen die unbefugte oder übermäßige Erhebung, Speicherung, Verwendung und Weitergabe sollte nicht gerechtfertigt sein. Im Bereich des Strafregisters, dem klassischen Bereich des Schutzes personenbezogener Daten, erkennt Deutschland das öffentliche Interesse an Strafregistern an, berücksichtigt jedoch auch das Interesse der Verurteilten an ihrer Wiedereingliederung in die Gesellschaft und konkretisiert daher die Notwendigkeit des Datenschutzes hinsichtlich der Strafregistrierungen. Im Rahmen der Abwägung beider Interessen wurden Schutzvorkehrungen getroffen, um einen unbefugten oder übermäßigen Zugriff auf die fraglichen Daten zu verhindern. In den USA hingegen scheinen im Bereich des Strafregisters die Verwaltungsinteressen, die sich aus der effektiven Übermittlung nützlicher Daten an die erforderlichen Stellen ergeben, vorrangig zu sein. Der Privatsphären- und Datenschutz scheint hier Berücksichtigung zu finden. Die Bewertung ergibt sich aus der Tatsache, dass in Deutschland die mitteilungspflichtigen Stellen, die ins BZR einzutragenden Inhalte, die Mitteilungs-, Anfrage- sowie Auskunftsmethode und die Datenverwendung und -weitergabe gesetzlich vorgesehen und daher eingeschränkt werden, während in den USA ausschließlich der Austausch zwischen den Einzelstaaten bundesgesetzlich vorgesehen ist und die Erhebung, Speicherung, Verwendung sowie Weitergabe der Strafregistrierungen den Einzelstaaten überlassen bleibt. Hier gibt es zwar die Einschränkung der Verwendungsberechtigten und des Verwendungszweckes, jedoch erschöpft sich ihre Anwendung in den Strafverfahrensdaten ohne Verurteilung. Das Problem verschärft sich insbesondere dann, wenn nicht nur Strafregistrierungen, sondern auch bloße Verhaftungsdaten gespeichert werden. Es scheint hier ein Mangel an angemessenen Schutzvorkehrungen zu bestehen, um den Einzelnen vor der unbefugten oder übermäßigen Erhebung, Speicherung, Verwendung und Weitergabe zu schützen.

Die entsprechende Vergleichseinschätzung gilt auch bei der Rasterfahndung, bei der bestimmte Personengruppen aus öffentlichen oder privaten Datenbanken herausgefiltert werden, damit Hinweise oder Spuren bekannter oder unbekannter Täter gefunden werden können. Im Rahmen des automatischen maschinellen Datenabgleichs werden zwar in beiden

Ländern die Erfassung vergleichbarer Daten nicht ausdrücklich gesetzlich vorgeschrieben, die Datenverwendung wird jedoch an bestimmte Voraussetzungen geknüpft. Die Voraussetzungen werden in der US-amerikanischen Praxis durch „routine use" mehrfach umgangen, sodass der Schutz der Betroffenen eingeschränkt wird, während die Betroffenen beim deutschen Datenabgleich zutreffend durch die Einschränkung auf Katalogtaten und den Richtervorbehalt geschützt werden. Darüber hinaus wird in Deutschland die Datenverwendung für einen anderen als den ursprünglichen Zweck durch die Aufbewahrungs- und Löschungsvorschrift verhindert. Vergleichbare Schutzregelungen sind in den USA nicht angelegt. In Anbetracht dieser Regelungslage lässt sich feststellen, dass in den USA im Vergleich zu Deutschland auch im Rahmen der Rasterfahndung ein geringerer Schutz personenbezogener Daten gewährt wird. Jedoch ist anzumerken, dass der deutsche Richtervorbehalt problematisch ist, um den Einzelnen zu schützen. Insbesondere deshalb, weil die Bedeutung des Richtervorbehalts durch die Möglichkeit der staatsanwaltschaftlichen Eilanordnung bei Gefahr im Verzug abgeschwächt wird. Ebenso scheint das Bedürfnis nach der Eilanordnung bei der Rasterfahndung nicht nachvollziehbar. Das Problem wird insofern verschärft, als das deutsche Recht für die Erkenntnisse, die unter der staatsanwaltschaftlichen Eilanordnung ohne eine nachträgliche gerichtliche Bestätigung gewonnen werden, keine Löschung und auch kein Verwendungsverbot vorsieht.

Abschließend wendet Deutschland bei der Vorratsdatenspeicherung, deren Gültigkeit bisher offenbleibt, das Doppeltürmodell an. Die Anbieter der Telekommunikationsdienste sind dazu verpflichtet, bestimmte Daten anlasslos zu speichern, während versucht wird, der unbefugten oder übermäßigen Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten dadurch zu begegnen, dass die Strafprozessordnung den Zugriff auf diese Daten an enge Voraussetzungen knüpft. Dies ist in Anerkennung der Notwendigkeit der Vorratsdatenspeicherung unter den modernen Datenverarbeitungsbedingungen das Ergebnis des Ausgleichs des Interesses an der effektiven Strafverfolgung einerseits und des Interesses des Einzelnen am Datenschutz andererseits. Die Vorratsdatenspeicherung wird trotz mehrerer Gesetzgebungsversuche in den USA bisher nicht angewendet. Bei dem US-amerikanischen sog. „Quick-Freeze-Verfahren" bezieht sich die Datenspeicherung – anders als bei der Vorratsdatenspeicherung, bei der Telekommunikationsunternehmen die im Gesetz vorgesehenen Daten für einen bestimmten Zeitraum speichern müssen – unter dem ECPA nur auf bestimmte Daten, die von einer Behörde verlangt werden. Das ECPA stellt je nach Art der von den Strafverfolgungsbehörden

angeforderten Daten unterschiedlich strenge Anforderungen. Es ist überraschend, dass die USA, die kein Datenschutzgesetz statuieren, dennoch konkrete Anforderungen an das Quick-Freeze-Verfahren stellen. Angesichts des Umstands, dass in den USA der Umgang mit personenbezogenen Daten im privaten Bereich nicht gesetzlich beschränkt ist, ist es jedoch schwer festzustellen, ob dieses System in den USA dem Schutz personenbezogener Daten zuträglicher ist als die deutsche Vorratsdatenspeicherung.[692]

C. Rechtspolitische Empfehlungen

Ein Interessenausgleich ist eine herausfordernde Aufgabe für den Gesetzgeber, der den verfassungsrechtlichen Konflikt zwischen Freiheit und Sicherheit beilegen muss, indem er das Sicherheitsinstrument auf das notwendige Maß beschränkt und dessen Missbrauchspotenziale soweit wie möglich vermeidet oder vermindert. Angesichts neuer Bedrohungen muss sich die Rechtslehre diesbezüglich weiterentwickeln. Die Möglichkeiten der modernen Datenverarbeitungstechnologie sind enorm. Im digitalen Zeitalter sollten rechtliche Sicherungsmaßnahmen für den Privatsphären- und Datenschutz weiter gestärkt und ausgebaut werden. Denn unter den modernen Datenverarbeitungsbedingungen haben personenbezogene Daten sehr große Aussagekraft. Diesen Daten sind nicht nur vielfältige Auswertungsmöglichkeiten, sondern auch erhebliche Missbrauchspotenziale inhärent, die die Freiheit des Einzelnen gefährden können. Die computergestützte Verarbeitung von Daten führt aufgrund der Verarbeitungsgeschwindigkeit und der Verknüpfungs- und Speichermöglichkeiten zur Gefahr der Entstehung eines umfassenden Überwachungsstaates, die ungleich größer ist als die der manuellen Datenverarbeitung. In der Regulierung der einzelnen Maßnahmen ist somit ein Ausgleich der Interessen von Sicherheit und Freiheit anzustreben und zu erreichen. Unabdingbar ist daher die Auswertung personenbezogener Daten mit angemessenen Schutzvorkehrungen, die den Einzelnen gegen die unbefugte oder übermäßige Erhebung, Speicherung, Verwendung und Weitergabe ihn betreffender Daten hinrei-

692 Dazu kritisch siehe *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, S. 7: *Ringland* vertritt die Auffassung, dass durch das US-amerikanische Datenspeicherungsmodell im Vergleich zu der deutschen Vorratsdatenspeicherung eine bessere Abwägung zwischen der Unterstützung der Strafverfolgung und der Minimierung der Kosten für Unternehmen und Verbraucher erreicht wird.

chend schützt. Hierfür ist es erforderlich, dass dem Betroffenen bewusst ist, welche seiner personenbezogenen Daten wo, in welchem Umfang und wie genutzt werden. Im Folgenden werden die Empfehlungen an den Gesetzgeber für einen Interessenausgleich bei der Regulierung konkreter Sicherheitsmaßnahmen zusammengefasst:

1. Die Erhebung und Speicherung personenbezogener Daten müssen präzisen vorgesehenen Befugnissen und Voraussetzungen unterliegen. Die im Rahmen aller Ermittlungsmaßnahmen zu verwendenden Daten sind gesetzlich einzuschränken.
2. Bezogen auf Sensitivität und Vulnerabilität sind verschiedene Datenkategorien zu unterscheiden, die wiederum differenzierten Speicherfristen, Verwendungsbefugnissen und Schutzvorkehrungen unterliegen.
3. Die Datenverwendung ist an einen bestimmten Verwendungszweck zu binden, um dem Risiko der unbegrenzten Verwendung auch für andere Zwecke als den ursprünglichen zu begegnen.
4. Der Umgang mit personenbezogenen Daten ist den Betroffenen durch eine Benachrichtigung mitzuteilen, sodass dieser eine Kontrollmöglichkeit erhält. Die Benachrichtigung der Betroffenen garantiert Rechtsschutz. Der effektive Schutz des Rechts auf informationelle Selbstbestimmung setzt voraus, dass die Bürger grundsätzlich Kenntnis davon haben müssen, über welche sie betreffenden Daten staatliche Stellen verfügen.
5. Die Zulässigkeit konkreter Maßnahmen ist von Gerichten zu überprüfen. In diesem Zusammenhang ist die Möglichkeit der staatsanwaltschaftlichen Eilanordnung bei der Rasterfahndung zu streichen.