Teil 1: Kollision zwischen Freiheit und Sicherheit

Die Gewährleistung von Freiheit und Sicherheit stellen zwei der wichtigsten Aufgaben des Staates dar. Neue Bedrohungslagen, damit verbundene neue gesellschaftliche Anforderungen und die stetig fortschreitende Digitalisierung sind hierbei große Herausforderungen. Durch eine Ausweitung der gesamtgesellschaftlichen Überwachung als Reaktion auf terroristische Bedrohungen ist die Gewährleistung der Sicherheit ins Zentrum der Debatte gerückt, wobei sich in Teilen der Gesellschaft die Befürchtung ausgebreitet hat, dass sich der Verfassungsstaat in einen Überwachungs- oder Präventionsstaat verwandelt.[27] Die Erfassung und Auswertung großer Mengen personenbezogener Daten soll zwar ermöglichen, zukünftigen Verbrechen vorzubeugen oder strafbare Handlungen effektiv zu verfolgen, jedoch kann das staatliche Handeln auch zu maßlosen Eingriffen in die Privatsphäre des Einzelnen führen. Das Spannungsverhältnis von Freiheit und Sicherheit hat sich durch die digitale Datenverarbeitung, Technisierung, Globalisierung und die neuen Gefährdungslagen verschärft. Dabei wird in der aktuellen Diskussion sogar vielfach die Frage gestellt, ob es nicht mittlerweile „Sicherheit statt Freiheit" heißt.[28] Erforderlich ist hierbei die Herstellung eines möglichst optimalen Ausgleichs zwischen dem Bedürfnis nach kollektiver Sicherheit und der Wahrung individueller Freiheit. In diesem Zusammenhang entfachte im 21. Jahrhundert eine kontrovers geführte Diskussion um das Verhältnis zwischen Freiheit und Sicherheit.

Die veränderten gesellschaftlichen Bedingungen stellen die frühere Sozialkontrolle in Frage: Wie können unter den Bedingungen digitaler Datenverarbeitung und unter dem Druck terroristischer Bedrohungslagen Freiheit und Sicherheit gewährleistet werden?

---

27 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 2; *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; *Huster/Rudolph*, Vom Rechtsstaat zum Präventionsstaat; *Trojanow/Zeh*, Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte.

28 *Hornig*, Sicherheit statt Freiheit, 2010.

Zur Klärung dieser Frage soll erfasst werden, wie sich die gesellschaftlichen Bedingungen in der modernen Gesellschaft verändert haben und in welche Richtung sich die gegenwärtige Sozialkontrolle aus der strafrechtlichen Perspektive betrachtet entwickelt (I). Danach werden die neuen, aufgrund der veränderten Sozialkontrolle eingeführten technikgestützten Maßnahmen zur Sicherheitsgewährleistung vorgestellt (II). Anhand dessen lässt sich feststellen, wie ein Staat in einer modernen Gesellschaft die Sicherheit gewährleistet. Anschließend wird der Frage nachgegangen, welche Bedeutung dem Datenschutz im digitalen Zeitalter zukommt und welche Anstrengungen international hinsichtlich der Sicherstellung dieses Schutzes unternommen werden (III). Dies ist deshalb wichtig, weil die internationalen Bemühungen um die Sicherstellung des Datenschutzes als Voraussetzung für die Freiheitsgewährleistung des Einzelnen in der digitalen Zeit einen ganz entscheidenden Einfluss auf die Entwicklung und Ausgestaltung der jeweiligen nationalen Regelungen haben. Abschließend wird das gesellschaftliche Phänomen unter dem Aspekt der Kollision zwischen Freiheit und Sicherheit erklärt (IV). Dadurch soll wiederum die Notwendigkeit betont werden, diese beiden legitimen Interessen miteinander in Einklang zu bringen.

A. Neue Sozialkontrolle in der modernen Gesellschaft

Die Gegenstände und Ziele von sozialer Kontrolle sowie ihre Mechanismen und Techniken hängen von den soziokulturellen, wirtschaftlichen und politischen Strukturen und Bedingungen innerhalb einer Gesellschaft ab.[29] Was also jeweils als Bedrohung der sozialen Ordnung aufgefasst und in welcher Weise darauf reagiert werden soll, variiert mit den jeweiligen Entwicklungen der Gesellschaft.[30]

I. Sozialkontrolle im Wohlfahrtsstaat

Im 19. und 20. Jahrhundert war zumindest in Europa unter der wohlfahrtsstaatlichen Politik die Sozialkontrolle durch Disziplinierung,

29 Siehe *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 17 m. w. N.

30 *Groenemeyer*, Wege der Sicherheitsgesellschaft, Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten, S. 8.

Behandlung und Rehabilitation (Resozialisierung) von Tätern vorherrschend. Aus dieser Perspektive werden die Gründe für von sozialen Normen abweichende Verhaltensweisen in mangelnden Integrationsfähigkeiten oder -möglichkeiten der Individuen gesehen, die wiederum durch persönliche und sozialstrukturelle Defizite verursacht werden.[31] Bei diesem Modell wurde der Schwerpunkt auf die positive Spezialprävention und die negative Generalprävention gelegt. Die Resozialisierung des Täters als das alleinige Ziel des Freiheitsentzugs steht im Vordergrund, der Gesellschaftsschutz hingegen wird nur als (untergeordnete) Aufgabe des Strafvollzugs angesehen (§ 2 Strafvollzugsgesetz). Das Bundesverfassungsgericht hat das Resozialisierungsgebot sogar aus der Verfassung abgeleitet: „Von der Gemeinschaft aus betrachtet verlangt das Sozialstaatsprinzip staatliche Vor- und Fürsorge für Gruppen der Gesellschaft, die aufgrund persönlicher Schwäche oder Schuld, Unfähigkeit oder gesellschaftlicher Benachteiligung in ihrer persönlichen und sozialen Entfaltung behindert sind; dazu gehören auch die Gefangenen und Entlassenen."[32]

II. Wandel der gesellschaftlichen Strukturen

Die wohlfahrtsstaatliche Politik muss seit geraumer Zeit auf Veränderungen der gesellschaftlichen Strukturen reagieren. Infolgedessen sind neue Anforderungen an soziale Kontrolle sowie neue Möglichkeiten derselben entstanden. Die soziale Kontrolle konnte sich nur wenig auf eine wohlfahrtsstaatliche Integration mittels Disziplinierung, Behandlung und Resozialisierung verlassen.

1. Veränderte gesellschaftliche Bedingungen

Der wohlfahrtsstaatliche Integrationsansatz wurde vor allem durch eine veränderte Vorstellung von der Delinquenz zurückgedrängt: Bereits in der kriminalpolitischen Debatte der 1970er Jahre hatte sich die Anerkennung der Ubiquität von Delinquenz durchgesetzt. Damit einhergehend erhöhte sich der empirische Zweifel daran, ob die mit dem Strafrecht verfolgten Ziele – General- und Spezialprävention – tatsächlich erreicht werden kön-

31 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 26 f.
32 BVerfGE 35, 202 (236).

nen.[33] Daraus ergab sich ein Orientierungswandel des Strafrechts dahingehend, den Strafzweck auf die Sicherung des Täters zu richten (negative Spezialprävention) und auf eine positive Generalprävention abzustellen.

Außerdem schwinden durch die fortschreitende Globalisierung zunehmend territoriale Grenzen. Hierdurch wird nicht nur der Verkehr von Waren, Dienstleistungen, Personen, Technik und sogar kulturellen Werten internationalisiert, sondern auch die Kriminalität. Parallel dazu internationalisieren sich auch die Sicherheitspolitik und die Strukturen sozialer Kontrolle. Sicherheit kann nicht mehr durch Maßnahmen auf ausschließlich nationaler Ebene gewährleistet werden. Denn es bedarf einer internationalen Zusammenarbeit, um die grenzüberschreitende Kriminalität zu bekämpfen.

2. Neue Anforderungen

Einhergehend damit, dass eine permanente Verunsicherung die Gesellschaft beherrscht,[34] ist seit den 1990er Jahren Sicherheit international zu einem Leitmotiv kriminalpolitischer Reformen geworden. Anlass zu dieser Bewegung gaben beispielsweise der Fall Dutroux (1995)[35] und der Fall Nathalie (1996)[36]. Infolge dieser beiden Fälle wurde das Verlangen nach Sicherheit in Verbindung mit einer Diskussion um Sicherheitslücken und einer kollektiven Identifizierung mit Kriminalitätsopfern immer stärker.[37]

Die Forderung nach Sicherheit wurde durch eine Reihe von Terroranschlägen auf der ganzen Welt verstärkt. Die Angst vor erneuten Terroran-

---

33 Zusammenfassend *Albrecht, P.-A.*, Kriminologie, S. 51 ff.; *Stolle*, Das Strafrecht, seine Zwecke und seine Alternativen, in: Studentische Zeitschrift für Rechtswissenschaft, S. 27 ff.

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

35 *Albrecht*, *H.-J.*, Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: *Koch*, Wegsperren? – Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter im internationalen Vergleich, 431 (431).

36 *Der Spiegel*, Verbrechen: Schrei der Hilflosigkeit, Der Spiegel 40/1996 v. 30.9.1996, abrufbar unter: https://www.spiegel.de/spiegel/print/d-9095363.html.

37 *Albrecht*, *H.-J.*, Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: *Koch*, Wegsperren? – Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter im internationalen Vergleich, 431 (483).

schlägen rückt die Gewährleistung von Sicherheit als eine der zentralen staatlichen Aufgaben in den Vordergrund und scheint den Einzelnen dazu zu veranlassen, willentlich seine Freiheit für die Sicherheit aufzugeben. Dies zeigt sich auch ganz klar in der Befürchtung des ehemaligen Verfassungsrichters *Grimm*: „Im Kampf gegen den Terrorismus läuft der Staat Gefahr, die Freiheit der Sicherheit zu opfern."[38]

Es könnte zwar einige Gründe für die von permanenter Verunsicherung und permanentem Sicherheitsbedürfnis beherrschte Gesellschaft geben, eine wichtige Rolle spielt aber die Entwicklung der Massenmedien. Ungeachtet dessen, dass die Zahl der Kriminalitätsfälle tatsächlich nicht steigt, reagiert die Gesellschaft in Bezug auf die Gefahren von Kriminalität mit einer Verunsicherung, die angesichts der Fakten allein unerklärlich bleiben muss. Sie hat daher im Rahmen der Sicherheitsherstellung immer höhere Erwartungen an den Staat und das Strafrecht.

3. Neue technische Möglichkeiten

Neue technische Entwicklungen eröffnen viele Möglichkeiten im menschlichen Leben. Es erweist sich jedoch, dass die stetigen Fortschritte auf dem Gebiet der Wissenschaft und der Technik selbst Mittel zur Erzeugung von Großrisiken werden können. Damit wird die Sicherheit bürgerlicher Lebensbedingungen durch neue Gefahrengruppen bedroht, die durch die Entwicklung der modernen Technik hervorgerufen werden. Während die neue Technologie einerseits den Menschen mehr Wohlstand ermöglicht, kann sie andererseits aber auch zur Folge haben, dass sich die Menschen neuen Arten von Gefahren ausgesetzt sehen und solche Entwicklungen als Möglichkeiten zur Bedrohung der Sicherheit des Lebens eingesetzt werden. Angst und Furcht vor diesen neuen Gefahren- und Risikogruppen führen zu einem gesteigerten Sicherheits- und Präventionsbedürfnis, was die Schaffung neuer Strafvorschriften begünstigt.[39] Diese gesellschaftliche Veränderung drängt den Gesetzgeber dazu, Sicherheit und Prävention gegenüber Freiheit kriminalpolitisch höher zu gewichten (Tendenz des Prä-

38 *Grimm*, Aus der Balance, Die Zeit v. 28.11.2007, abrufbar unter: https://www.zeit.de/2007/49/Schaeuble-Antwort.

39 *Sieber*, Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten.", NStZ 2009, 353.

ventionsstrafrechts). Dabei werden die staatlichen Eingriffe zeitlich immer mehr vorverlagert, damit die Aufgaben des Staates effektiv erfüllt werden können. So entstehen beispielsweise die Kriminalisierung im Vorfeld einer Rechtsgutsverletzung sowie die Erweiterung der – abstrakten oder konkreten – Gefährdungsdelikte.[40]

Auch bei der Absicherung vor Risiken sind die technischen Fortschritte hilfreich. Die Kombination der neuen technischen Möglichkeiten mit dem steigenden Sicherheitsbedürfnis innerhalb der Gesellschaft löst im Zusammenhang mit einem neuen Mechanismus neue Methoden sozialer Kontrolle aus: eine Ausweitung und Intensivierung der Überwachung sowie die Ausforschung sozialer Lebensumstände durch staatliche und private Akteure.[41] Auf diese Weise ermöglicht die moderne automatisierte Datenverarbeitung die Verwaltung und den Umgang mit zuvor nicht handhabbaren Datenmengen. Der Risikokontrolle und der Gefahrenabwehr kommt dabei eine erhebliche Bedeutung zu. Die auf diesen Trend ausgerichtete Sicherheitsgesetzgebung wird zu einer „Querschnittsmaterie“[42], die die Freiräume der modernen Zivilgesellschaft – und damit deren Substanz – als potenzielle Gefahr versteht und somit unter Generalverdacht stellt. Dadurch bedingt nimmt auch die Einbeziehung der Zivilgesellschaft in die Kontrolle und Repression von Kriminalität zu.[43,44]

III. Sozialkontrolle der Gegenwart

Durch die oben aufgeführten Änderungen wandelt sich auch die soziale Kontrolle der Gegenwart. Die Kontrolltechnik macht nicht nur das

---

40 Gefährdungstatbestände sind zwar nicht allein der modernen Strafrechtsentwicklung geschuldet, aber im modernen Strafrecht scheint ihre Verbreitungsgeschwindigkeit mit veränderten Anwendungsbereichen sowie Legitimationsbegründungen zuzunehmen.

41 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 25

42 *Albrecht*, *H.-J.*, Der erweiterte Sicherheitsbegriff und seine Folgen, RAV Infobrief # 91, S. 6.

43 *Albrecht*, *H.-J.*, Der erweiterte Sicherheitsbegriff und seine Folgen, RAV Infobrief # 91, S. 16: Diese Einbeziehung verwirklicht sich besonders auf dem Gebiet der Telekommunikation.

44 *Singelnstein* befürchtet, dass man eher in eine permanente Unsicherheit gerät, wenn immer häufiger über Risikokontrolle und Gefahrenabwehr diskutiert wird (*Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 35).

Individuum, sondern auch die Gefahr und weiter das Risiko zu ihrem Gegenstand. Parallel zu den Forderungen nach Sicherheit, die in einer von Risiken und Verunsicherung beherrschten Gesellschaft in ihrer Häufigkeit und Intensität zunehmen, ändert sich auch die soziale Kontrolle. Sie setzt sich im Zusammenhang mit Gefährdungslagen zunehmend unabhängig von konkreten Anlässen oder bestimmten Personen durch.[45] Diese Gefährdungslage ist eine abstrakte Gefahr oder sogar ein Gefahrenpotenzial.

Im Anschluss an die Anwendung des Begriffs „Risikogesellschaft" von Beck werden mehrere Begriffe für diese Entwicklung sozialer Kontrolle dargelegt.[46] Nach *Legnaro*, der die gesellschaftlichen Änderungen im Jahre 1997 mit dem Begriff „Sicherheitsgesellschaft" bezeichnet hat, besitzt die Sicherheitsgesellschaft folgende Merkmale:

> „[…] dass nicht nur staatliche, sondern allmählich und in stetig zunehmendem Ausmaß auch private Akteure an der Produktion von Sicherheit teilnehmen, dass die Überwachung nicht nur dem Staatsschutz im engeren Sinne gilt, sondern Aktivitätskontrollen von allen Bürgern – tendenziell durch alle Bürger – mit dem Ziel Risikominimierung für alle angestrebt werden und dass schließlich die Produktion von Sicherheit nicht nur eine staatliche Aufgabe ist, sondern eine permanente gesellschaftliche Anstrengung, ein Regime des täglichen sozialen Lebens."[47]

Im Zusammenhang damit zeichnet sich die gegenwärtige Gesellschaft zumeist durch folgende Besonderheiten aus:[48] die Allgegenwärtigkeit der Bedrohungen von Sicherheit, die Politisierung und Entprofessionalisierung der Sicherheitspolitik, die Privatisierung und Technisierung sozialer Kontrolle, den grundlegenden Wandel der Logik politischer und staatlicher Sicherheitsproduktion weg von der Resozialisierung und Reintegration von Tätern[49] hin zu der Idee des Gesellschaftsschutzes, der Entwicklung

---

45 *Legnaro*, Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze, in: Leviathan, S. 274: *die Personalisierung des Verdachts*.

46 Beispielsweise Risikogesellschaft, Sicherheitsgesellschaft, Sicherheitsstaat, Präventions-staat, Überwachungsstaat o. Ä.

47 *Legnaro*, Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze, in: Leviathan, S. 271 f.

48 Vgl. *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert.

49 Die Anwendung von Gewalt und Zwang gegen abweichendes Verhalten war für die Disziplinargesellschaft des 19. und 20. Jahrhunderts kennzeichnend. Der Begriff der Disziplinargesellschaft geht auf Foucault zurück. Die Disziplinargesellschaft war durch ein allgemein gültiges Normen- und Wertegefüge gekennzeich-

einer Kontrollkultur und der gleichzeitigen Moralisierung und Entmoralisierung abweichenden Verhaltens sowie schließlich durch ein permanentes Verunsicherungsgefühl, das allein mit dem Aspekt abweichenden oder kriminellen Verhaltens nicht erklärt werden kann.[50]

Der Wandel sozialer Kontrolle hat vor allem auf das Strafrecht einen erheblichen Einfluss. Dieser Wandel lässt sich zunächst hinsichtlich der menschlichen Erkenntnisse feststellen. Die alte kriminalpolitische Logik, dass von sozialen Normen abweichende Verhaltensweisen vor allem in bestimmten marginalen Klassen vorkommen und dass darauf mit der Politik der Resozialisierung reagiert werden sollte, wurde durch die neue Erkenntnis abgelöst, dass Verbrechen nicht nur durch Personen aus diesen Kreisen, sondern durch solche aus allen Schichten der Gesellschaft begangen werden (Ubiquität von Delinquenz).[51]

Ein empirischer Erfolgsnachweis über die Erreichung der angestrebten Ziele ist jedoch nicht möglich. Es fehlen vor allem sichere empirische Belege dafür, dass das Strafrecht negative Generalprävention und positive Spezialprävention erreichen kann.[52] Vielmehr zeigt beispielsweise eine Untersuchung von Martinson und seiner Feststellung *nothing works*,[53] dass die Resozialisierungsstrategie zu keinem Erfolg führt. Ferner ergaben empirische Untersuchungen, dass die Rückfallquoten umso höher ausfallen, je schwerer und höher die verhängte Strafe ist[54] und dass eine formelle Sanktionierung bei Jugendlichen sich eher kontraproduktiv auswirkt.[55]

Diese Erkenntnisse stellen das Strafrecht in seiner bisherigen Form in Frage. Die Form der Informationsbeschaffung zur Strafverfolgung und zur polizeirechtlichen Gefahrenabwehr wurde angesichts neuer technischer

---

net, bei dessen Verletzung das Individuum diszipliniert und an der präskriptiven Norm ausgerichtet wurde (vgl. *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 62 und 119).

50 *Groenemeyer*, Wege der Sicherheitsgesellschaft, Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten, S. 15 ff.

51 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 20.

52 *Albrecht*, *H.-J.*, Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: *Koch*, Wegsperren? – Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter im internationalen Vergleich, 431, S. 448 m. w. N.

53 *Martinson*, What Works? – Questions and Answers About Prison Reform. The Public Interest Issue 35, 1974, 22–54.

54 *Jehle/Heinz/Sutterer*, Legalbewährung nach strafrechtlichen Sanktionen. Eine kommen-tierte Rückfallstatistik, 51 ff.

55 *Albrecht*, *P.-A.*, Jugendstrafrecht, 50 ff.

Möglichkeiten und sicherheitspolitischer Bedürfnisse beständig ausgebaut. Die soziale Kontrolle, die sich lange Zeit überwiegend auf die Täter und ihre Veränderung durch Abschreckung, soziale Dienste und Sozialpolitik bezog, wird in vielen Bereichen durch Orientierung an der Kontrolle von Situationen ersetzt, die, wenn möglich, mit Hilfe automatisierter Techniken durchgeführt werden soll. Hier steht vor allem die möglichst frühzeitige Identifizierung von Risiken im Vordergrund. Um die Sicherheit der Gesellschaft zu gewährleisten, zeichnet sich im Rahmen des materiellen Rechts vor allem die Tendenz zu einer Vorverlagerung des strafrechtlichen Schutzes durch abstrakte Gefährdungsdelikte und durch überindividuelle Rechtsgüter ab. In der gegenwärtigen Gesellschaft werden daher häufig präventive Maßnahmen ergriffen. Bezüglich solcher präventiven Maßnahmen stellt *Singelnstein* fest, der Hauptzweck solcher Techniken bestehe „in dem räumlichen Fernhalten der ‚Gefährlichen' und in der sozialen Ausgrenzung der ‚Überflüssigen'."[56] Zu diesen Zwecken nutzt das Strafrecht darüber hinaus auch die neuen technischen Möglichkeiten, die zur Optimierung der Strafverfolgung eingesetzt werden.

Unter dieser veränderten Sozialkontrolle werden im Rahmen der Strafverfolgung neue technikgestützte Maßnahmen eingesetzt, um eine Optimierung der Ermittlung zu erreichen und strafverfahrensrechtliche Maßnahmen effektiv durchzusetzen. Dies hat der technische Fortschritt ermöglicht. Mit Hilfe der modernen automatisierten Datenverarbeitung versucht das Strafrecht, schon im Vorfeld mit Risiken umzugehen, beispielsweise, indem ohne Anfangsverdacht flächendeckend ermittelt wird oder indem Maßregeln nicht durch Verurteilung, sondern durch die Feststellung eines Risikos ergriffen werden. Hierbei spielen personenbezogene Daten eine maßgebliche Rolle. Die veränderte strafrechtliche Orientierung, die neuen Forderungen der Gesellschaft nach Sicherheit und die neue Technik, die in der Lage ist, mit beträchtlichen Datenmengen umzugehen, führen jedoch auch zu neuen Herausforderungen – vor allem zur Aufgabe von Freiheit.

B. Neue technikgestützte Maßnahmen zur Sozialkontrolle

Die Feststellung und die Durchsetzung eines im Einzelfall bestehenden staatlichen Strafanspruchs zur Sicherung der gesellschaftlichen Ordnung

56 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 87.

setzen die Wahrheitsfindung und die Erforschung des Sachverhalts voraus, welcher der Straftat zugrunde liegt. Dies kann oftmals auch durch die Ermittlung im privaten Umfeld der verdächtigen Person und durch die Suche nach entsprechenden personenbezogenen Informationen geschehen. Dafür stehen den Strafverfolgungsbehörden zahlreiche spezielle Ermittlungsbefugnisse zur Verfügung, mittels derer auch in die Privatsphäre der Menschen eingegriffen werden kann. Denn deren Privatsphäre wird zwar grundrechtlich garantiert, unter bestimmten Einschränkungen darf jedoch in sie eingegriffen werden. Mit diesen Befugnissen kann auf den privaten Lebensbereich eines Menschen, insbesondere auf seine personenbezogenen Daten, zugegriffen werden. Im Zusammenhang mit der Sicherheitspolitik und der fortgeschrittenen Technik sind diese Befugnisse zu einer erheblichen Kraft geworden. Der technische Fortschritt ermöglicht es nun, zuvor nicht handhabbare Datenmengen miteinander zu vergleichen und zu analysieren sowie auch den privaten Raum oder das nichtöffentlich gesprochene Wort zur Kenntnis zu nehmen, wenn die Strafverfolgungsbehörden darauf bestehen.

Um zu klären, in welcher Weise die fortgeschrittene Technik in der Praxis genutzt und damit die Optimierung der Strafverfolgung erhöht wird – d. h. inwieweit die Gesellschaft heutzutage die Eingriffe dieser Maßnahmen in die Privatsphäre eines Menschen duldet –, sollen anschließend die neuen technikgestützten Maßnahmen übersichtlich vorgestellt werden.

I. Der Lauschangriff

Um insbesondere im Hinblick auf die Organisierte Kriminalität ein Eindringen in die Kernbereiche von Organisationen und somit eine Offenlegung der Strukturen zu ermöglichen, wird in der Praxis der sogenannte Große Lauschangriff eingesetzt. Darunter wird das heimliche Abhören und Aufzeichnen von den innerhalb der Wohnungen der überwachten Individuen stattfindenden Lebensvorgängen, insbesondere des dort nichtöffentlich gesprochenen Wortes, unter Zuhilfenahme technischer Mittel verstanden.[57] Dies kann sowohl in der Wohnung selbst geschehen, etwa durch einen dort versteckten Miniatursender („Wanze"), als auch

57 *Bludovsky*, Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100 c Abs. 1 Nr. 3 StPO, S. 21 f.; *Geis*, Großer Aufwand für großen Lauschangriff, JuS 1998, 1174, 1174; *Müller*, Der sogenannte „Große Lauschangriff", Eine Untersuchung zu den

von außerhalb, beispielsweise mit Hilfe von Richtmikrofonen.[58] Zu den herkömmlichen Ermittlungsmethoden, die ähnlichen Zwecken wie dem Lauschangriff dienen, zählt die Telefonüberwachung oder der Einsatz von verdeckt ermittelnden Personen. Der Einsatz des Großen Lauschangriffs beruht auf der Erwägung, dass die herkömmlichen Ermittlungsmethoden, verglichen mit dem heutigen Stand der Organisierten Kriminalität, als nicht hinreichend angesehen werden.

Abzugrenzen vom Großen Lauschangriff ist der Kleine Lauschangriff, sprich, die Überwachung des nichtöffentlich gesprochenen Wortes mit technischen Mitteln außerhalb von Wohnungen. Diese Ermittlungsmethode wird oft zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität eingesetzt. Denn die herkömmlichen Ermittlungs- und Aufklärungsmethoden wurden mit Blick auf die besonderen Strukturen der Organisierten Kriminalität und die fortschreitende Professionalisierung der Straftäter in diesem Bereich als nicht mehr ausreichend angesehen.[59] Zur Durchführung dieser Überwachung werden z. B. versteckte Mikrofone und Aufzeichnungsgeräte als technische Mittel genutzt.[60]

Mit diesen beiden Arten von Lauschangriffen wurden unter bestimmten Voraussetzungen Gespräche von Personen sowohl innerhalb als auch außerhalb der Wohnung zum Gegenstand der heimlichen Ermittlung gemacht. Als Folge kann in der heutigen Welt nicht mehr darauf vertraut werden, dass ein nichtöffentlich gesprochenes Wort niemals an die Öffentlichkeit gelangt.

Rechtsproblemen der Einführung der elektronischen Wohnraumüberwachung zur Beweismittelgewinnung, S. 5.

58 *Bludovsky*, Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100 c Abs. 1 Nr. 3 StPO, S. 23; *Glauben*, Kann der „Große Lauschangriff" zulässig sein? Ein Überblick über die verfassungsrechtlichen Aspekte, DRiZ 1993, 41.

59 *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, S. 187.

60 *Gercke*, HK-StPO, § 100f Rn. 4; *Schmitt*, Strafprozessordnung, § 100f Rn. 4.

II. Die Überwachung der Telekommunikation

Die Strafverfolgungsbehörden können die Telekommunikation[61] zu Zwecken der Sachverhaltserforschung oder der Ermittlung des Aufenthaltsortes des Beschuldigten überwachen und aufzeichnen. Mit dieser Befugnis können nicht nur die herkömmlichen Formen des Telefonierens und Fernschreibens, sondern auch die Datenübermittlung mittels neuerer Techniken wie Mobilfunk, Satellitenübertragung, Bildtelefon oder Text- und Bildübermittlungsdiensten sowie der Kommunikation in Computernetzen wie etwa per E-Mail-Verkehr oder Online-Kommunikation überwacht werden.[62] Die Telekommunikationsüberwachung wird in fast allen Staaten von den Regierungen erlaubt, auch wenn sie hinsichtlich solcher Faktoren wie z. B. den Bedingungen, unter denen dies geschehen darf, und ob nur die Verbindungsdaten oder auch die Inhalte überwacht werden dürfen, unterschiedlich geregelt ist.

Davon abzugrenzen ist die Vorratsdatenspeicherung, nämlich die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Speicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ohne dass ein einzelfallbezogener Anlass dazu besteht. Die im Zuge der Vorratsdatenspeicherung erfassten Daten können zu einem späteren Zeitpunkt zur Telekommunikationsüberwachung genutzt werden. Die Verpflichtung zur Speicherung von Verkehrsdaten soll verhindern, dass strafrechtliche Ermittlungen nicht weiterverfolgt werden können, weil die Telekommunikationsdienstanbieter die Verkehrsdaten entweder direkt nach Rechnungsstellung gelöscht oder sie mangels Berechtigung gar nicht erst erhoben haben.[63]

Der Zugriff der Strafverfolgungsbehörden darf sich damit auch auf die Datenübermittlung mittels Techniken erstrecken. Die Behörden dürfen z. B. Kenntnis darüber erlangen, wer, wann, mit wem, auf welche Weise und wie oft kommuniziert hat. Das Gefährdungspotenzial dieser Eingriffe

---

61 Nach § 3 Nr. 22 TKG i. V. m. § 3 Nr. 23 TKG ist „Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen, d. h. mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können."

62 *Schmitt*, Strafprozessordnung, § 100a Rn. 6 ff.; *Bruns*, KK-StPO, § 100a Rn. 16 ff.; *Hauck*, LR-StPO, § 100a Rn. 59.

63 BT-Drs. 16/5846, S. 31.

ist deshalb sehr hoch, weil die Aussagekraft der hier erhobenen Daten erheblich ist, da aus ihnen oder aus deren Kombination mit anderen Daten umfassende Bewegungs- und Persönlichkeitsprofile erstellt werden können.

III. Der IMSI-Catcher

Mit einem speziellen Messtechnikgerät, dem sogenannten IMSI-Catcher, lassen sich die digitale Kennung eines Mobilfunkgeräts, genauer gesagt die IMSI[64] und die IMEI[65], sowie dessen genauer Standort ermitteln.[66] IMSI-Catcher machen sich die Tatsache zunutze, dass Mobilfunktelefone in eingeschaltetem Zustand in regelmäßigen Abständen die IMSI und die IMEI an die nächste Basisstation der Funkzelle senden, in der sie sich aktuell befinden. Ein bekanntes Beispiel für einen solchen IMSI-Catcher ist der vom FBI genutzte „Stingray". Der Einsatz eines IMSI-Catchers kommt vor allem dann in Betracht, wenn bekannt ist, dass an einem bestimmten Ort Mobilfunktelekommunikation betrieben wird, jedoch keine näheren Erkenntnisse über die Identität der verdächtigen Person, das verwendete Mobiltelefon oder die Rufnummer vorliegen – etwa weil sich der zu Überwachende ein Mobiltelefon von einem Unbekannten geliehen, die Chipkarte ausgetauscht oder eine Karte unter falschen Personaldaten gekauft hat.[67]

IMSI-Catcher ermöglichen die Ermittlung der Geräte- und Kartennummer sowie des Standorts eines Mobiltelefons, aber auch das Mithören laufender Mobilfunkgespräche in Echtzeit, wenn auch mit Hilfe einer speziellen Software.

---

64 Die *International Mobile Subscriber Identity* (Kartennummer) ist eine weltweit gültige Kennung, die den Teilnehmer als Vertragspartner eines Netzbetreibers eindeutig identifiziert. Sie ist auf der Chipkarte gespeichert, die ein Mobilfunkteilnehmer bei Abschluss eines Vertrages erhält (hierzu *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, S. 188).

65 Die *International Mobile Station Equipment Identity* ist die weltweit nur einmal vergebene Geräte- oder Seriennummer eines Mobiltelefons. Sie ist fest mit dem jeweiligen Endgerät verbunden, sodass dieses anhand der IMSE eindeutig identifiziert werden kann (hierzu *Bär*, TK-Überwachung, S. 372).

66 *Schmitt*, Strafprozessordnung, § 100i Rn. 1.

67 *Fos*, Der IMSI-Catcher, DuD 2002, 212, 213; *Hilger*, Gesetzgebungsbericht – §§ 100g, 100h StPO, die Nachfolgeregelungen zu § 12 FAG, GA 2002, 228, 557; *Schmitt*, Strafprozessordnung, § 100i Rn. 1; *Ronellenfitsch*, Datennotwehr, DuD 2008, 110, 114.

IV. Die Rasterfahndung

Für Zwecke der Strafverfolgung werden bereits vorhandene, personenbezogene Datenbestände, die von öffentlichen und nichtöffentlichen Stellen ohne den Bezug zu Strafverfolgungsbehörden für von der Strafverfolgung unabhängige Zwecke erhoben wurden, computergestützt nach bestimmten tätertypischen Prüfungsmerkmalen (Rastern) überprüft und abgeglichen. Durch diesen Abgleich sollen Nichtverdächtige ausgeschlossen sowie Personen identifiziert werden, die weitere für die Ermittlungen bedeutsame Prüfungskriterien erfüllen. Mit Hilfe der Ermittlungsmethode der Rasterfahndung, bei der die Möglichkeit der automatisierten Datenverarbeitung für Zwecke der Strafverfolgung genutzt wird, sollen Hinweise und Spuren gefunden werden, die nach kriminalistischer Erfahrung zur Aufklärung einer Straftat beitragen können. Diesen Hinweisen und Spuren wird anschließend auf herkömmliche Weise weiter nachgegangen.[68]

Anders als beim üblichen polizeilichen Datenabgleich, bei dem der Polizei bereits zur Verfügung stehende Daten miteinander abgeglichen werden, werden bei der Rasterfahndung polizei-externe Daten, die aus anderen Gründen an anderen Stellen gespeichert sind, maschinell abgeglichen, um eine Straftat aufzuklären. Dies beruht darauf, dass der technische Fortschritt es ermöglicht, zuvor nicht handhabbare Datenmengen maschinell zu verarbeiten. Bei diesem Vorgehen werden zunächst alle auf diese Weise erfassten Personen, auf die bestimmte Merkmale zutreffen, verdächtigt.

V. Die DNA-Analyse

Die Speicherung von DNA-Identifizierungsmustern zwecks künftiger Strafverfolgung ist inzwischen eine weltweit verbreitete und häufig angewendete Ermittlungsmethode. Unter bestimmten Bedingungen dürfen die Strafverfolgungsbehörden dem Beschuldigten zur Identitätsfeststellung in einem anderen, zukünftigen Strafverfahren Körperzellen entnehmen und molekulargenetisch untersuchen. Die so erhobenen Daten dürfen in einer sogenannten DNA-Datenbank gespeichert werden. Zweck dieser Maßnahme ist es, durch eine schnellere Täteridentifizierung eine bessere Aufklärung von schweren Straftaten, insbesondere Sexualstraftaten, zu erreichen.[69]

---

68 BT-Drs. 12/989, S. 36.
69 Beispielsweise siehe BT-Drs. 13/10791, S. 4.

Ein großes Problem bei der DNA-Analyse liegt darin, dass bei ihr auf äußerst sensible personenbezogene Informationen zugegriffen wird, die eigentlich dem unantastbaren Bereich der menschlichen Persönlichkeit zuzuordnen sind, da die DNA Trägerin genetischer Informationen ist und damit sozusagen den Schlüssel zum Kern der Persönlichkeit eines Menschen darstellt. Dennoch wird weltweit zu Zwecken der Strafverfolgung häufig auf die DNA-Analyse zurückgegriffen, auch wenn ihre Verwendung von bestimmten Voraussetzungen abhängt.

VI. Die Online-Durchsuchung

Unter dem Begriff „Online-Durchsuchung" versteht man den verdeckten Zugriff staatlicher Behörden auf fremde informationstechnische Systeme über Kommunikationsnetze. Als Objekte dieser Art der Durchsuchung kommen alle von einem Mikroprozessor gesteuerten Geräte in Betracht, z. B. PCs und Mobiltelefone, aber auch elektronische Terminkalender. Die Online-Durchsuchung umfasst sowohl den einmaligen Zugriff auf den Datenbestand eines Systems als auch die sich über einen längeren Zeitraum erstreckende Online-Überwachung. Letztere ermöglicht es den Behörden, sich ein umfassendes Bild von der Nutzung des überwachten Systems zu machen. Die Online-Überwachung unterscheidet sich insofern von der Telekommunikationsüberwachung, als nicht allein der Datentransfer ausfindig gemacht wird, sondern die laufende Kommunikation der Zielpersonen direkt am Endgerät mittels Spionagesoftware überwacht wird, beispielsweise anhand eines sogenannten *Trojaner*-Programms. Trotz der heftigen Kritik an dieser Methode, die auf Eingriffe in die Grundrechte, die technischen Bedenken sowie das Missbrauchspotenzial abhebt, wird die Online-Durchsuchung in einigen Staaten[70] genutzt.

Im digitalen Zeitalter, in dem infolge der stetig steigenden Zahl von PC viele Daten mit Hilfe von Informationssystemen verarbeitet werden, könnte die Online-Durchsuchung zu ähnlichen Ergebnissen führen wie die Überwachung des Denkinhalts eines Menschen. Die Angst davor, dass die Gedanken eines Einzelnen überwacht werden könnten, kann einen enormen Einfluss auf seine Handlung nehmen. Darin liegt der bedenklichste Punkt der Online-Durchsuchung.

70 Zum Beispiel Deutschland, Österreich, Frankreich, die USA, China usw.

C. Der Schutz personenbezogener Daten

Der Einsatz technikgestützter Ermittlungsmittel zielt auf die effektive Gewährleistung der Sicherheit ab. Trotz des Erfolgs beim Einsatz solcher technikgestützter Ermittlungsmittel bei der effektiven Sicherheitsgewährleistung muss die Frage gestellt werden, ob beim Einsatz dieser Mittel ein angemessener Schutz personenbezogener Daten sichergestellt werden kann. Der Datenschutz steht im Hinblick auf die Freiheit des Einzelnen im Vordergrund. Er spielt insbesondere in der heutigen Zeit als eine Voraussetzung für die Freiheit eine wichtige Rolle.

Es ist hierbei erforderlich zu untersuchen, welche Bedeutung den personenbezogenen Daten im modernen Rechtsstaat zukommt. Anschließend soll analysiert werden, welche Bestrebungen von internationalen Organisationen unternommen werden, um personenbezogene Daten zu schützen. Die Untersuchung kann dazu dienen, die Bedeutung personenbezogener Daten zu verdeutlichen und zu betonen.

I. Die Bedeutung der Daten unter den Bedingungen der modernen automatisierten Datenverarbeitung

Die moderne automatisierte Datenverarbeitung eröffnet einerseits viele Möglichkeiten bei Ermittlungen und hilft dabei, Straftaten effektiv zu verfolgen. Sie schafft andererseits aber auch neue Herausforderungen beim Umgang mit personenbezogenen Daten. In der Informationsgesellschaft erlangen nicht nur der Austausch und die Auswertung, sondern auch der Schutz personenbezogener Daten immer mehr Bedeutung. Unter dem Begriff der *personenbezogenen Daten* sind gemäß § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“ zu verstehen. Der Begriff der persönlichen oder sachlichen Verhältnisse umfasst die körperlichen und geistigen Eigenschaften und Verhaltensweisen, die beruflichen, wirtschaftlichen, sozialen oder privaten Beziehungen sowie alle identifizierbaren Angaben wie etwa die Adresse, die Angaben als Kfz-Halter, das Bankguthaben, die Berufsbezeichnung, Krankheiten, Kreditdaten, Straftaten usw. Die Sensibilität oder Aussagekraft dieser Angaben ist für ihre Einordnung als personenbezogene Daten nicht relevant.[71] Gemäß der deutschen Rechtsprechung gibt es wegen der der Informationstechnologie

71 *Plath*, DSGVO/BDSG Kommentar, § 3 Rn. 8 m. w. N.

inhärenten Verarbeitungs- und Verknüpfungsmöglichkeiten unter den Bedingungen der automatischen Datenverarbeitung *sogar kein belangloses Datum* mehr.[72] Es besteht die Möglichkeit, aus den Daten umfassende Bewegungs- und Persönlichkeitsprofile zu erstellen. Auch wenn die jeweiligen Daten für sich allein genommen im Grunde unbedeutend und harmlos erscheinen mögen, besteht die Gefahr, dass aus deren Kombination mit anderen Daten ein Persönlichkeitsprofil eines Einzelnen hergestellt wird, was auf erhebliche Eingriffe in dessen Persönlichkeitsrecht hinauslaufen kann. Dies führt dazu, dass der Einzelne zunehmend *gläsern* wird.[73] Anders als bei anderen Grundrechten scheint sich eine Vielzahl von Menschen trotz des hohen Gefährdungspotenzials dieses Eingriffs der potenziellen Verletzung ihres Persönlichkeitsrechts im Alltag nicht bewusst zu sein. Eingriffe können infolgedessen immer häufiger und immer intensiver erfolgen.

Das Recht auf Schutz der Privatsphäre i. w. S.[74] ist ein national wie international anerkanntes Grundrecht und wird in fast allen Staaten der Welt geschützt, sei es verfassungsrechtlich oder einfachgesetzlich oder aber durch Gerichte gemäß allgemeiner Prinzipien und Werte.[75] Die personenbezogenen Daten spielen beim Schutz der Privatsphäre eine bedeutende Rolle. Auch der Datenschutz[76] gewinnt derzeit immer mehr an Bedeutung. Damit stellt sich die Frage, *wie und inwiefern personenbezogene Daten geschützt werden sollten*. Aus dieser Erkenntnis ergeben sich die nationalen sowie die internationalen Bemühungen um einen effektiven Datenschutz.

II. Internationaler Datenschutz

Jeder Staat bemüht sich darum, die individuelle Freiheit seiner Bürger zu schützen. Im digitalen Zeitalter wird versucht, personenbezogene Da-

72 BVerfGE 65, 1 (28).

73 *Comans*, Ein „modernes" europäisches Datenschutzrecht – Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, S. 66.

74 Siehe auch http://www.privacyinternational.org/survey/rankings2007/phrcomposort.pdf, http://www.privacyinternational.org/article.shtmal?cmd[347]=x-347-563326.

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

76 Der Begriff „Datenschutz" ist dabei missverständlich. Denn das Datenschutzrecht verfolgt nicht den Zweck, die auf einem „Träger" gespeicherten Daten, sondern den Einzelnen vor Verletzungen seiner Privatsphäre durch einen unzulässigen Umgang mit ihn betreffenden Daten zu schützen (vgl. § 1 Abs. 1 Nr. 1 BDSG; Art. 1 Abs. 1 Richtlinie 95/46/EG.).

ten als eine Voraussetzung für die individuelle Freiheit zu schützen. Die Staaten ergreifen dabei zwar auf nationaler Ebene Maßnahmen zum Datenschutz, stoßen dabei allerdings häufig an teilweise unüberwindbare Grenzen. Ist der Schutz personenbezogener Daten auf nationales Recht beschränkt, kann nur ein ungenügender oder sogar mangelnder Erfolg erzielt werden, da die Grenzüberschreitung des Datenverkehrs durch die zunehmende Globalisierung, die fortschreitende Technisierung, das Internet, die stetig steigende Anzahl und Nutzung von Personal Computern, die wachsende wirtschaftliche Bedeutung des internationalen Datentransfers sowie durch die sich neu ergebenden Vermarktungsmöglichkeiten immer einfacher erfolgt. Trotz dieses Umstands besteht noch immer kein allgemeiner und international gültiger Rechtsrahmen für den Datenschutz. Die Staaten trafen jedoch internationale Vereinbarungen, um die jeweiligen diversen nationalen Regelungen für den Datenschutz miteinander zu verbinden und bestehende Lücken zu schließen.[77] Diese internationalen Vereinbarungen beeinflussen wiederum die Entwicklung und die Ausgestaltung nationaler Regelungen. So wurden diese internationalen Vereinbarungen zur Grundlage der Datenschutzgesetze der einzelnen Länder.

1. Die Vereinten Nationen

Bereits die am 10. Oktober 1948 von der UN-Generalversammlung beschlossene Allgemeine Erklärung der Menschenrechte (AEMR)[78] misst der Privatsphäre der Menschen eine große Bedeutung zu. Im Art. 12 der Menschenrechtserklärung heißt es: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden."

Basierend auf dem nationalen Verständnis des Privatsphärenschutzes beinhaltet dies die notwendigen Bedingungen für die Anknüpfung an einen spezifischen internationalen Datenschutz. Die Vereinten Nationen begriffen, dass die Privatsphäre der Menschen durch die automatisierte Verarbeitung personenbezogener Daten gefährdet werden kann und daher

77 Beispielhaft dafür sind die „Safe Harbor Principles", die im Rahmen des Art. 25 der EU-Datenschutzrichtlinie am 21. Juli 2000 zwischen den USA und der Europäischen Union vereinbart wurden.

78 Resolution 217 (III) Universal Declaration of Human Rights in: United Nations, General Assembly, Official Records Third Session (part I) Resolutions (Doc. A/810).

deren Schutz notwendig ist. Aufgrund dieser Überlegung verabschiedete die UN-Generalversammlung am 14. Dezember 1990 die „Guidelines for the Regulation of Computerized Personnel Data Files" (A/RES/45/95), zu Deutsch die „Richtlinie zur Verarbeitung personenbezogener Daten in automatisierten Dateien". Sie fordert die Mitgliedstaaten zwar dazu auf, verbindliche nationale Rechtsvorschriften für die automatisierte Verarbeitung personenbezogener Daten zu schaffen, hat als Empfehlung jedoch keine bindende völkerrechtliche Wirkung. Dennoch sind die Ergebnisse der UN-Generalversammlungen beachtenswert, da Grundsätze wie *Rechtmäßigkeit der Datenverarbeitung, Richtigkeit der Daten, Zweckbestimmung und Einsichtnahme durch die Betroffenen* auf nationale datenschutzgesetzliche Regelungen eingewirkt haben.

2. OECD

Aufgrund des zunehmenden grenzüberschreitenden Datenverkehrs und der wachsenden wirtschaftlichen Bedeutung des internationalen Datentransfers verabschiedete die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) im Jahr 1980 die Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten,[79] um einen international einheitlichen Standard zu schaffen. Die Ziele dieser Richtlinien sind die Harmonisierung der Datenschutzbestimmungen der Mitgliedstaaten, die Förderung des freien Datenaustauschs sowie die Vermeidung ungerechtfertigter Handelshemmnisse.[80]

---

79 OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), Document C (80) 58 (Final), Bekanntgabe Banz, Amtl. Teil v. 14.11.1981, Nr. 215; siehe auch OECD, Recommendation on Cross-border Co-Operation in the Enforcement of Laws Protecting Privacy (2007).

80 Der Zweck der OECD-Richtlinie ist in der Präambel klar angegeben: „Im Zuge der Einführung der Informationstechnologien in verschiedene Bereiche der Wirtschaft und Gesellschaft und mit der zunehmenden Bedeutung und Leistungsstärke der elektronischen Datenverarbeitung beschloss die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) 1980, Richtlinien für eine internationale Politik über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten herauszugeben. Die rasch alle Bereiche durchdringende Entwicklung der Informations- und Kommunikationstechnologien, gekennzeichnet durch Erscheinungen wie das Internet, trug in jüngster Zeit zur beschleunigten Entstehung einer globalen Informationsgesellschaft bei. Die OECD hat sich daraufhin mit der Frage befasst, wie diese Richtlinien im 21.

Diesen Leitlinien kommt insofern eine besondere Bedeutung zu, als ihre Intention nicht nur in dem Bestreben besteht, die Privatsphäre des Individuums zu schützen. Stattdessen konzentrieren sich die Leitlinien erstmals auf den wirtschaftlichen Aspekt der Daten. Bei den Leitlinien handelt es sich aber nicht um bindendes Völkerrecht. Die Mitgliedstaaten sind nicht zur Umsetzung der Vorgaben in ein nationales Datenschutzrecht verpflichtet.

3. Europarat

Der Europarat wurde am 5. Mai 1949 von den Mitgliedern der Westeuropäischen Union (WEU) gegründet. Die Zielsetzung besteht vor allem darin, auf der Grundlage der Europäischen Menschenrechtskonvention (EMRK) einen effizienten Menschenrechtsschutz zu realisieren.[81] Bei der Entwicklung eines ungeschriebenen Grundrechtsstandards als eines Teils der allgemeinen Rechtsgrundsätze des Gemeinschaftsrechts wurde vom EuGH immer wieder auf die EMRK zurückgegriffen.[82] Sie gilt gemäß Art. 6 Abs. 3 EU zusammen mit dem Lissabon-Vertrag als ein allgemeiner Grundsatz des EU-Rechts.[83]

Nach Art. 8 Abs. 1 EMRK wird der Anspruch einer jeden Person auf Achtung ihres Privat- und Familienlebens sowie ihrer Wohnung und ihrer Korrespondenz gewährleistet. Auf der Grundlage dieser Vorschrift hat der Europarat im Jahre 1979 das international verbindliche Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, das kurz „Konvention 108" genannt wird, verabschiedet. Der Konvention 108 kommt insofern eine große Bedeutung zu, als sie die erste internationale Datenschutzregelung darstellt, die für die ver-

---

Jahrhundert bestmöglich umgesetzt werden können, um die Achtung der Privatsphäre und den Schutz personenbezogener Daten online zu gewährleisten."

81 Die Konvention zum Schutz der Menschenrechte und der Grundfreiheiten wurde am 4. November 1950 in Rom abgeschlossen und ist nach Ratifizierung von zehn Staaten am 3. September 1953 in Kraft getreten (vgl. BGBl. 1952 II, S. 686).

82 EuGH, Rs. 44/79, Slg. 1979, 3727 Rn. 17 ff.

83 Art. 6 Abs. 3 EU verweist ausdrücklich auf die EMRK: „Die Union achtet die Grundrechte, wie sie in der [...] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben."

pflichteten Staaten völkerrechtlich verbindlich ist.[84] Die der Konvention beitretenden Staaten sind dazu verpflichtet, die Regelungen in innerstaatliches Recht umzusetzen. Andererseits formuliert die europäische Datenschutzkonvention die Grundprinzipien des europäischen Datenschutzes: die rechtmäßige Erhebung und Verarbeitung personenbezogener Daten nach Treu und Glauben (Art. 5 lit. a); die Zweckbindung der Datenerhebung und -verarbeitung (Art. 5 lit. b); den Verhältnismäßigkeitsgrundsatz bei der Erhebung und der Verarbeitung (Art. 5 lit. c); das Prinzip der Datenqualität (Art. 5 lit. d); Sonderregelungen zum Umgang mit sensiblen Daten (Art. 6); den Grundsatz der Datensicherheit (Art. 7); die Rechte des Betroffenen wie etwa das Auskunftsrecht sowie die Rechte auf Berichtigung und Löschung (Art. 8) sowie die grenzüberschreitende Übermittlung personenbezogener Daten zwischen Vertragsstaaten (Art. 12).

4. Die Europäische Union

Auch die Europäische Union gewährleistet den Datenschutz sowohl durch datenschutzrechtliche Regelungen im Rahmen der europäischen Grundrechte[85] als auch durch allgemeine und bereichsspezifische Datenschutzvorschriften. Während Art. 7 der EU-Charta in Anlehnung an die europäische Menschenrechtskonvention den Schutz des Privatlebens regelt, garantiert Art. 8 der EU-Charta als lex specialis zu Art. 7 der EU-Charta den Schutz personenbezogener Daten. Zu diesem Zweck hat die Europäische Union Richtlinien erlassen,[86] in denen die Mindeststandards für den Da-

84 European Treaty Series No. 108; EU, DS, EuRAT Con.

85 Der Charta der Grundrechte kam ursprünglich keine verbindliche Rechtswirkung zu; sie wird jedoch durch den Verweis in Artikel 6 des durch den Lissabonner Vertrag geänderten EU-Vertrages für alle Staaten – ausgenommen das Vereinigte Königreich und Polen – für bindend erklärt.

86 Beispielsweise (1) die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG, ABl. EG 1995, L281, 31). Sie wurde am 25. Mai 2018 durch die am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlichte Datenschutz-Grundverordnung (DSGVO) abgelöst. Die DSGVO ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch sollen zum einen der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt sowie zum anderen der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden. (2) Die Richtlinie über die Verarbeitung personenbezogener Daten und den

tenschutz beschrieben sind, die in allen Mitgliedstaaten der Europäischen Union durch nationale Gesetze sichergestellt werden sollen. Die Richtlinie 95/46/EG bildet zusammen mit der Konvention 108, der EU-Grundrechtecharta sowie der EMRK ein gemeinsames und umfassendes europäisches Datenschutzrecht.[87]

D. Freiheit vs. Sicherheit

Unter diesen veränderten gesellschaftlichen Bedingungen scheinen sowohl der Einzelne als auch die Gesellschaft in permanente Verunsicherung versetzt worden zu sein und zu Gunsten der Sicherheit willentlich seine bzw. ihre Freiheiten aufzugeben. Neue Bedrohungen wie Terroranschläge begünstigen die Tendenz, die Sicherheit *durch* den Staat gegenüber der Sicherheit *vor* dem Staat vorzuziehen. Im Zuge dieser Entwicklung wurden und werden weiterhin verschiedene neue technikgestützte Mittel sozialer Kontrolle eingeführt. Diese neuartigen Kontrollmittel sind deshalb fragwürdig, weil sie Eingriffe in die Grundrechte des Einzelnen, genauer gesagt, in seine Freiheit darstellen. Die gesellschaftlichen Veränderungen und die damit einhergehende zunehmend präventive Ausrichtung der staatlichen Sicherheitsvorsorge stellen das Verhältnis von Freiheit und Sicherheit vor neue Fragen. Der Staat muss auf der einen Seite die Grundrechte des Einzelnen berücksichtigen, ist auf der anderen Seite jedoch auch dazu verpflichtet, die notwendigen Maßnahmen zu ergreifen, um Sicherheit als eine Voraussetzung für Freiheit zu gewährleisten. Es handelt sich also um eine Kollision von Freiheit und Sicherheit, sodass sich zwei konfligierende Interessenkreise gegenüberstehen. Zu den Aufgaben des Gesetzgebers gehört es, zwischen diesen beiden Interessenkreisen einen Interessenausgleich herzustellen.

Freiheit und Sicherheit werden häufig als ein Gegensatzpaar begriffen. Sie stehen jedoch nicht in einem gegensätzlichen Verhältnis zueinander, sondern bedingen einander vielmehr wechselseitig.[88] Die Sicherheit soll grundsätzlich der Freiheit dienen. Der Staat übernimmt die doppelte Aufgabe der Gewährleistung von Freiheit und Sicherheit. Fraglich ist

---

Schutz der Privatsphäre in der elektronischen Kommunikation (RL 2002/58/EG, Abl. EG 2002, L201, 37).

87 *Genz*, Datenschutz in Europa und den USA, S. 19.

88 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 12.

dabei, ob die politischen Entscheidungen, die mit dem Slogan „Sicherheit vor Freiheit" bezeichnet werden können, verfassungskonform sind. Entscheidend ist demzufolge, wie der Staat diese doppelte Aufgabe verfassungskonform und optimal erfüllen kann. Als sich die Diskussion um das Folterverbot ausweitete, waren die deutschen Rechtswissenschaftler äußerst überrascht. Gleichwohl nimmt zurzeit die Tendenz zu, Freiheit für Sicherheit zu opfern. Die Notwendigkeit neuer Sozialkontrollmittel ist zu vergleichen mit der Notwendigkeit der Folter für die Rettung des Lebens. Beispielsweise werden bei der Vorratsdatenspeicherung als einer Art der oben beschriebenen neuen technikgestützten staatlichen Maßnahmen Telekommunikationsdaten durch einen Telekommunikationsdienstanbieter anlassunabhängig für einen bestimmten Zeitraum für Strafverfolgungs- und Gefahrenabwehrzwecke gespeichert. Damit wird die Möglichkeit eines staatlichen Zugriffs auf diese Daten zu einem späteren Zeitpunkt abgesichert. Dies kann insofern als ein beträchtlicher Angriff auf die Menschenwürde und als ein intensiver Eingriff in die Freiheit des Einzelnen betrachtet werden, als bei der Vorratsdatenspeicherung alle Bürger als potenzielle Täter gelten. Durch die Kombination verschiedener Daten können Persönlichkeitsprofile hergestellt und die Privatsphäre teilweise oder vollständig überwacht werden, und zwar im Namen der Sicherheitsgewährleistung für die Gesellschaft. Dies verursacht das Problem einer strategischen Abwägung zwischen Strafverfolgungseffizienz, Sicherheit und dem Schutz des Privaten. Somit sollte nach einem Modell gesucht werden, bei dem das gesellschaftliche Bedürfnis nach Sicherheit befriedigt und zugleich die Privatsphäre des Einzelnen geschützt werden können.

Im Zusammenhang damit behauptet *Isensee*, dass das Problem des Konflikts zwischen der Gewährleistung von Freiheit und Sicherheit mit einem „Grundrecht auf Sicherheit" gelöst werden soll.[89] Nach seiner Ansicht verpflichtet sich der Staat nicht nur dazu, die Grundrechte im Sinne des *status negativus* zu achten, sondern auch dazu, sie positiv zu schützen. Entgegen dem eindeutigen Wortlaut des Grundgesetzes konstruiert Isensee im Zusammenhang mit der Sicherheitsgewährleistung als der Grundlage von Freiheit ein Grundrecht auf Sicherheit als *status positivus* und definiert dieses als die Gesamtheit der Schutzpflichten des Staates.[90] Nach dieser Auffassung kommt diesem Grundrecht der Charakter eines

89 *Isensee*, Das Grundrecht auf Sicherheit, 1983.

90 *Comans*, Ein „modernes" europäisches Datenschutzrecht – Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, S. 57.

Leistungsanspruchsrechts zu. Jedoch kann diese Konstruktion nicht dem Zweck dienen, dem Einzelnen einen Anspruch auf eine staatliche Leistung zuteilwerden zu lassen, sondern es geht darum, Eingriffe in das Freiheitsrecht, beispielsweise in das Recht auf informationelle Selbstbestimmung, zu legitimieren.[91] Angesichts des eigentlichen Charakters der Grundrechte als Abwehrrechte gegen den Staat ist es jedoch unhaltbar, aus den Grundrechten ein Grundrecht abzuleiten, das eine positive Handlung vom Staat fordert. Darüber hinaus droht die Gefahr, mit diesem Grundrecht staatliche Einschränkungen des Freiheitsrechts des Einzelnen ohne gewichtigen Grund zu legitimieren.

Angesichts des Umgangs mit den beträchtlichen Datenmengen, die bei der modernen Datenverarbeitung elektronisch gespeichert werden, können sich aus der Perspektive des Datenschutzes besondere Herausforderungen ergeben. Um unter diesem Gesichtspunkt betrachtet einem optimalen Interessenausgleich zwischen Freiheit und Sicherheit zu dienen, sollte zuerst geklärt werden, wie das Verfassungsrecht einer jeweiligen Gesellschaft Freiheit konstituiert und wie die Privatsphäre sowie die personenbezogenen Daten durch das Verfassungsrecht geschützt werden. Danach ist es erforderlich, konkrete Sicherheitsvorkehrungen zu analysieren, die zu diesem Schutz bei den einzelnen Maßnahmen, die zur Strafverfolgungseffizienz im modernen Staat klassisch oder neuartig eingesetzt werden, bereits zur Verfügung stehen. Aus diesem Grund soll im Folgenden auf die verfassungsrechtliche Grundlage in Bezug auf den Privatsphären- sowie Datenschutz eingegangen werden. Außerdem sollen drei neuartige Maßnahmen vorgestellt werden, aufgrund derer personenbezogene Daten verwertet werden dürfen. Durch die Analyse des Problems des Datenschutzes in diesen drei Bereichen soll das Kollisionsproblem zwischen Freiheit und Sicherheit bei der staatlichen Verwertung personenbezogener Daten hervorgehoben werden und es soll die Notwendigkeit des Ausgleichs zwischen Strafverfolgungseffizienz und Freiheitsgewährleistung durch Datenschutz betont werden.

Gegenwärtig steht die Gewährleistung von Freiheit und Sicherheit durch den Wandel gesellschaftlicher Bedingungen vor neuen Herausforderungen. Wie garantiert die Verfassung konkret den Schutz personenbezogener Daten? Welche Sicherheitsvorrichtungen verlangt die Verfassung für staatliche Maßnahmen, die personenbezogene Daten verwenden? Wie setzt die Verfassung dem Interesse der Ermittlungsbehörden, zu Sicherheitszwe-

91 *Kutscha*, in: *Roggan/Aden* (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, S. 31 m. w. N.

cken möglichst viele personenbezogene Daten der Bürger zu sammeln und zu verwenden, Grenzen? Wie sind diese Grenzen bei konkreten staatlichen Maßnahmen, die personenbezogene Daten verwenden, realisiert? Sind die bestehenden Grenzen hinreichend, um die Privatsphäre und die Daten zu schützen? Befinden sich der verfassungsrechtliche Schutz der Privatsphäre und der personenbezogenen Daten auf der einen und die Sicherheitsgewährleistung durch strafrechtliche Maßnahmen auf der anderen Seite im Zustand eines angemessenen Interessenausgleichs?

Um diese Fragen zu beantworten, ist es erforderlich, den verfassungsrechtlichen Schutz der Privatsphäre[92] und personenbezogener Daten konkret zu analysieren. Es geht darum, wie verfassungsrechtliche Vorgaben bei Sachverhalten konkretisiert sind. Anschließend sollen einige konkrete Maßnahmen als Beispiele für das Kollisionsverhältnis zwischen Freiheit und Sicherheit untersucht werden. Hierbei handelt es sich um das Strafregister, die Rasterfahndung und die Vorratsdatenspeicherung. Es soll untersucht werden, wie diese drei Maßnahmen gesetzlich ausgestaltet sind, inwiefern sie erfolgsversprechend sind – also ob sie für die Sicherheitsgewährleistung tatsächlich hilfreich sind – und welche Vorkehrungen getroffen wurden, um einen unbefugten oder unverhältnismäßigen Zugriff auf die im Strafverfahren verwendeten personenbezogenen Daten zu verhindern. Damit soll untersucht werden, ob die staatlichen Überwachungsmaßnahmen zu Sicherheitszwecken eine Gefährdung der verfassungsrechtlich garantierten Freiheiten darstellen und in welchem Umfang die Sicherheitspolitik in Freiheitsrechte eingreifen darf. Die hier durchgeführte rechtsvergleichende Untersuchung zu diesen Fragestellungen soll es ermöglichen, die Bedeutung, die der moderne Rechtsstaat der Privatsphäre und den personenbezogenen Daten beimisst, und damit das Schutzniveau der Privatsphäre und der personenbezogenen Daten zu erfassen. Aus den Ergebnissen dieser Untersuchung sollen Hinweise für einen angemessenen Interessenausgleich zwischen Freiheit und Sicherheit herausgearbeitet werden.

92 Der Begriff des Privatlebens ist ein auf Umstände bezogener Begriff, der sich mit Zeit, Ort und den sozialen und psychologischen Faktoren ändert. Er ist aber auch ein Mehrzweckkonzept, das in verschiedenen Umgebungen eine unterschiedliche Bedeutung hat. Es ist daher schwierig, den Begriff einheitlich zu definieren. In Deutschland ist unter der privaten Sphäre der Bereich einer Person zu verstehen, der nicht öffentlich ist, also der nur die eigene Person angeht. Durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist die Privatsphäre in besonderem Maße geschützt. Dieses Verständnis zeigt bereits die verschiedenen Auslegungsmöglichkeiten, die abhängig von zeitlichen oder örtlichen Verhältnissen bestehen.